

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, 196)

| | |
|--|----|
| 1. Documento programmatico sulla sicurezza | 4 |
| 1.1. Revisione | 4 |
| 1.2. Scopo del documento e linee guida per la sua composizione | 4 |
| 1.3. Campo di applicazione | 6 |
| 1.4. Riferimenti normativi | 6 |
| 1.5. Definizioni | 6 |
| 1.5.1. Trattamento | 6 |
| 1.5.2. Dato personale | 6 |
| 1.5.3. Dati sensibili | 6 |
| 1.5.4. Dati giudiziari | 7 |
| 1.5.5. Titolare | 7 |
| 1.5.6. Responsabile | 7 |
| 1.5.7. Incaricati | 7 |
| 1.5.8. Interessato | 7 |
| 1.5.9. Comunicazione | 7 |
| 1.5.10. Diffusione | 7 |
| 1.5.11. Dato anonimo | 7 |
| 1.5.12. Blocco | 7 |
| 1.5.13. Banca dati | 7 |
| 1.5.14. Comunicazione elettronica | 7 |
| 1.5.15. Misure minime | 7 |
| 1.5.16. Strumenti elettronici | 8 |
| 1.5.17. Autenticazione informatica | 8 |
| 1.5.18. Credenziali di autenticazione | 8 |
| 1.5.19. Parola chiave | 8 |
| 1.5.20. Profilo di autorizzazione | 8 |
| 1.5.21. Sistema di autorizzazione | 8 |
| 2. Ruoli, compiti e nomina delle figure previste per la sicurezza dei dati personali | 9 |
| 2.1. Titolare del trattamento dei dati personali | 9 |
| 2.1.1. Compiti del titolare del trattamento dei dati personali | 9 |
| 2.2. Coordinamento ed indirizzo ai fini della sicurezza dei dati personali (INFOSEC) | 9 |
| 2.2.1. Compiti del responsabile della sicurezza dei dati personali | 9 |
| 2.2.2. Nomina dei componenti del Gruppo di Coordinamento ed indirizzo ai fini della sicurezza dei dati personali | 10 |
| 2.3. Responsabile di specifico trattamento dei dati personali | 10 |
| 2.3.1. Compiti del responsabile di uno specifico trattamento di dati personali | 10 |
| 2.3.2. Nomina dei responsabili di uno specifico trattamento di dati personali | 10 |
| 2.4. Incaricati della gestione e della manutenzione degli strumenti elettronici | 11 |
| 2.4.1. Compiti degli incaricati della gestione e della manutenzione degli strumenti elettronici contenenti dati | 11 |
| 2.4.2. Nomina degli incaricati della gestione e della manutenzione degli strumenti elettronici contenenti dati | 11 |
| 2.5. Incaricato della custodia delle copie delle Credenziali | 11 |
| 2.5.1. Compiti degli incaricati della custodia delle copie delle Credenziali | 11 |
| 2.5.2. Nomina degli incaricati della custodia delle copie delle Credenziali | 13 |
| 2.6. Incaricato delle copie di sicurezza delle banche dati | 13 |
| 2.6.1. Compiti degli incaricati delle copie di sicurezza delle banche dati | 13 |
| 2.6.2. Nomina degli incaricati delle copie di sicurezza delle banche dati | 14 |
| 2.7. Incaricato della custodia delle aree e dei locali | 14 |
| 2.7.1. Compiti degli incaricati della custodia delle aree e dei locali | 14 |
| 2.7.2. Nomina degli incaricati della custodia delle aree e dei locali | 15 |
| 2.8. Incaricato del trattamento dei dati personali | 15 |
| 2.8.1. Compiti degli incaricati del trattamento dei dati personali | 15 |
| 2.8.2. Nomina degli incaricati del trattamento dei dati personali | 16 |
| 2.9. Amministratore di sistema | 17 |
| 2.9.1. Compiti dell'Amministratore di sistema | 17 |
| 2.9.2. Nomina dell'Amministratore di Sistema | 17 |
| 3. Trattamenti con l'ausilio di strumenti elettronici | 19 |
| 3.1. Sistema di autenticazione informatica | 19 |
| 3.1.1. Procedura di identificazione | 19 |
| 3.1.2. Identificazione dell'incaricato | 19 |
| 3.1.3. Cautele per assicurare la segretezza della componente riservata della credenziale | 19 |
| 3.1.4. Caratteristiche della parola chiave | 19 |
| 3.1.5. Modalità di richiesta delle Credenziali di autenticazione | 19 |

| | |
|--|----|
| 3.1.6. Istruzioni per non lasciare incustodito e accessibile lo strumento elettronico | 20 |
| 3.1.7. Accesso straordinario | 20 |
| 3.2. Sistema di autorizzazione | 21 |
| 3.3. Altre misure di sicurezza | 21 |
| 3.4. Periodicità di revisione del documento programmatico sulla sicurezza | 21 |
| 3.5. Elenco dei trattamenti di dati personali | 22 |
| 3.5.1. Elenco delle sedi e degli uffici in cui vengono trattati i dati | 22 |
| 3.5.2. Elenco degli archivi dei dati oggetto del trattamento | 22 |
| 3.5.3. Elenco dei sistemi di elaborazione per il trattamento | 22 |
| 3.6. Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati | 22 |
| 3.6.1. Elenco dei soggetti autorizzati al trattamento dei dati | 22 |
| 3.6.2. Verifiche periodiche delle condizioni per il mantenimento delle autorizzazioni | 23 |
| 3.6.3. Distribuzione dei compiti e delle responsabilità | 23 |
| 3.7. Analisi dei rischi | 23 |
| 3.7.1. Analisi dei rischi hardware | 23 |
| 3.7.2. Analisi dei rischi sui sistemi operativi e sui software installati | 23 |
| 3.7.3. Analisi degli altri rischi nel trattamento dei dati | 24 |
| 3.8. Misure da adottare per garantire l'integrità e la disponibilità dei dati | 24 |
| 3.9. Misure da adottare per la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità | 24 |
| 3.9.1. Misure generali | 24 |
| 3.9.2. Procedure per controllare l'accesso ai locali in cui vengono trattati i dati | 24 |
| 3.10. Formazione degli incaricati del trattamento | 24 |
| 3.10.1. Piano di formazione | 24 |
| 3.11. Criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati all'esterno della struttura del titolare | 25 |
| 3.11.1. Trattamenti di dati personali affidati all'esterno della struttura del titolare | 25 |
| 3.11.2. Criteri per la scelta di soggetti terzi per il trattamento di dati personali affidati all'esterno della struttura del titolare | 26 |
| 3.11.3. Nomina del responsabile del trattamento per soggetti esterni alla struttura del Titolare in Out-sourcing | 26 |
| 3.11.4. Nomina del titolare autonomo del trattamento in Out-sourcing | 27 |
| 3.12. Ulteriori misure in caso di trattamento di dati sensibili o giudiziari | 27 |
| 3.12.1. Protezione contro l'accesso abusivo | 27 |
| 3.12.2. Istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili | 28 |
| 3.12.3. Riutilizzo dei supporti rimovibili | 28 |
| 3.12.4. Ripristino dell'accesso ai dati in caso di danneggiamento | 28 |
| 3.13. Trattamenti effettuati da organismi sanitari e esercenti le professioni sanitarie | 28 |
| 3.13.1. Cifratura dei dati o separazione dei dati identificativi | 28 |
| 3.13.2. Tabella dei trattamenti di dati personali idonei a rivelare lo stato di salute e la vita sessuale | 28 |
| 3.14. Misure di tutela e garanzia | 28 |
| 3.14.1. Descrizione degli interventi effettuati da soggetti esterni | 28 |
| 4. Trattamenti senza l'ausilio di strumenti elettronici | 29 |
| 4.1. Nomina e istruzioni agli incaricati | 29 |
| 4.2. Norme di sicurezza per gli incaricati del trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici | 29 |
| 4.3. Copie degli atti e dei documenti | 30 |
| 4.4. Controllo degli accessi | 30 |
| 5. Diritti dell'interessato | 31 |
| 5.1. Diritto di accesso ai dati personali | 31 |
| 5.2. Esercizio dei diritti | 31 |
| 5.3. Modalità di esercizio | 32 |
| 5.4. Riscontro all'interessato | 32 |
| 6. Allegati | 34 |
| 6.1. DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA (Artt. da 33 a 36 del codice) | 34 |

1. Documento programmatico sulla sicurezza

1.1. Revisione

Indice delle revisioni

| Rev | Data | Descrizione | Aggiornamenti |
|-----|------------|----------------------------------|----------------|
| 05 | 31/03/2011 | Revisione Ruoli e Responsabilità | Capitolo 2 e 3 |
| | | | |
| | | | |
| | | | |

1.2. Scopo del documento e linee guida per la sua composizione

Il presente Documento Programmatico Sulla Sicurezza (di seguito indicato anche come DPS) è redatto per fornire linee guida sulla soddisfazione delle misure minime di sicurezza che debbono essere adottate da questo Ente nel trattamento di dati personali, conformemente a quanto previsto dal Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003).

Inoltre costituisce, assieme agli allegati indicati, un valido strumento per l'adozione delle misure previste dall'Art. 31, dall'Art. 34 e dall'Art. 35 dello stesso 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 del Dlgs. n.196 del 30 giugno 2003).

Scopo del presente documento è quello di fornire informazioni che consentano di comprendere come questo Ente si adoperi per ridurre al minimo 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, intendendosi per misure di sicurezza il complesso degli accorgimenti tecnici, informatici, organizzativi, logistici e procedurali di sicurezza.

Nell'ambito del presente documento, sono adottate le seguenti linee guida, che costituiscono gli obiettivi che l'Ente persegue per eseguire una corretta e coerente politica di sicurezza:

Classificazione dei trattamenti

I trattamenti di dati personali devono essere classificati secondo i seguenti principi generali: l'Ente deve riporre assoluta attenzione affinché venga garantita una adeguata protezione ai dati personali e deve individuare le specifiche modalità di trattamento dei dati e i relativi flussi e processi. Si deve procedere, conseguentemente, ad una classificazione, ai fini della sicurezza, rispettando i livelli di protezione dei dati sensibili e strategici in relazione alla operatività del Sistema Informativo.

Classificazione dei dati

I criteri generali di classificazione dei dati dell'Ente ai fini della sicurezza devono valere in linea generale, quindi sia che essi siano originati direttamente, sia che essi siano derivati da terzi. Questo elemento è da considerare attività di primaria importanza in quanto costituisce la "base di conoscenza" su cui si fonda il corretto e sicuro trattamento dei dati.

Criteri di attribuzione di ruoli e responsabilità

I criteri generali di attribuzione di ruoli e responsabilità ai fini della sicurezza devono, in linea generale: individuare i ruoli all'interno dell'Ente ai fini della sicurezza per consentire di fissare le "necessità" di trattamento per ciascun soggetto, determinandone i compiti ed i poteri, in relazione alle diverse tipologie di dati e modalità di trattamento in cui esso è coinvolto, che saranno esercitati previo il controllo di accesso attraverso l'identificazione mediante utente e password.

Sicurezza Fisica

I criteri tecnico-organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza nonché le procedure per il controllo dell'accesso fisico delle persone nei locali interessati devono, in linea generale: riguardare tutti i dispositivi per il trattamento dei dati, siano essi elettronici che tradizionali, nonché i dati personali, indipendentemente dal supporto su cui essi sono conservati, al fine di essere custoditi in ambienti sicuri. Gli ambienti, sotto il profilo della protezione fisica, saranno distinti in aree a protezione diversificata a seconda delle necessità di protezione dei dati in essere trattati.

Controlli di accesso a dati e processi

I criteri tecnico-organizzativi per il controllo di accesso logico a dati e processi di trattamento dei dati devono, in linea generale: consentire l'abbinamento password - utente per controllare gli accessi alle informazioni, alle applicazioni ed alle attrezzature.

Conseguentemente, in tutte le situazioni di trattamento dei dati personali gli incaricati devono essere forniti di identificativo utente e password da utilizzare in combinazione al fine di consentire l'identificazione. Gli incaricati devono essere responsabilizzati per la custodia della password e dell'identificativo utente affidatagli.

Gestione delle password

I criteri tecnico-organizzativi per la gestione delle password di accesso devono, in linea generale: fornire ad ogni operatore che agisce su personal computer sia collegato in rete che non una password, fornita dal Responsabile del Sistema Informativo come codice univoco, per l'identificazione dello stesso. Tale codice deve essere conosciuto e custodito dall'operatore a cui è affidato.

Continuità operativa

I criteri tecnico-organizzativi per garantire il ripristino della disponibilità dei dati personali a seguito di distruzione o danneggiamento dei dati stessi o degli strumenti elettronici di trattamento: devono fare riferimento alle analisi dei rischi adottate, in cui sono definiti i criteri generali di massima per la sicurezza dei dati in modo che siano disponibili anche in seguito ad eventi che li distruggano o danneggino.

Outsourcing

I criteri tecnico-organizzativi per garantire l'adozione delle misure minime di sicurezza in caso di trattamento di dati personali affidati all'esterno della propria struttura (outsourcing-telelavoro): devono, in base ai vari processi, prevedere eventuali deleghe dall'Ente a organizzazioni esterne. Per tali dati devono essere richieste le giuste assicurazioni affinché i dati in loro possesso vengano trattati adottando adeguate misure di sicurezza.

Cifratura e segregazione di taluni dati sensibili

I criteri tecnico-organizzativi per la cifratura o per la separazione di alcune categorie di dati personali sensibili, dagli altri dati personali dell'Interessato: devono attivarsi indipendentemente dai criteri di archiviazioni e dai formati. Per tutti i dati sensibili suddetti si deve altresì operare separando i processi che riguardano tali dati e cifrando gli stessi dopo la loro elaborazione.

Protezione da programmi maliziosi

I criteri tecnico-organizzativi per la protezione dei dati e dei processi di trattamento da programmi maliziosi (malware) devono, in linea generale: prevedere adeguate protezioni a causa del progresso tecnologico che comporta il progressivo aumento di nuove vulnerabilità e minacce per il sistema informativo; ne consegue che dinamicamente, il sistema informativo deve essere protetto mediante idonei programmi antivirus ed antintrusione con aggiornamento possibilmente automatico.

Riutilizzo dei supporti di memorizzazione

I criteri tecnico-organizzativi per il riutilizzo dei supporti di memorizzazione dei dati (sia per il mantenimento che per il backup) devono, in linea generale: garantire che tutti i supporti che contengono dati sensibili al termine del trattamento devono essere distrutti in modo che non sia consentito il recupero delle informazioni ivi contenute. Nel caso che tali supporti debbano essere riutilizzati preventivamente si deve procedere alla cancellazione in modo permanente ed irrecuperabile delle informazioni ivi contenute. E' da evitare l'uso dei dispositivi di memorizzazione rimovibili per lo scambio di dati all'interno dell'Ente: deve essere utilizzato in maniera idonea il sistema informatico e le possibilità di operare in rete.

Criteri e procedure per l'integrità dei dati

I criteri generali per garantire l'integrità dei dati trattati dall'Ente devono, in linea generale: verificare che siano protetti dai rischi, anche accidentali, di distruzione, perdita o modifica non consentita tutti i dati. A tal fine, oltre alle misure di sicurezza preventive, deve essere predisposto un sistema di copiatura al fine di consentire il recupero dei dati. Le copie devono essere le più aggiornate possibile, devono avere la medesima efficacia giuridica degli originali e devono essere trattate e protette con le medesime misure previste per gli originali.

Criteri e procedure per la sicurezza delle trasmissioni dati

I criteri generali per garantire l'integrità e la sicurezza delle trasmissioni dei dati da e verso entità esterne devono, in linea generale: provvedere alla massima protezione delle trasmissioni dati in tutti i casi in cui i dati devono essere trasferiti, sia per via elettronica che tradizionale, anche all'interno dell'Ente; devono essere altresì osservate idonee misure di sicurezza al fine di ridurre i rischi di perdita o distruzione, anche accidentale, di intercettazione dei dati, di trattamento comunque non conforme alle finalità di raccolta.

Piano di formazione degli incaricati

Al fine di rendere edotti gli incaricati del trattamento dei rischi individuati, dei modi per prevenire i danni, delle regolamentazioni in materia di sicurezza operanti nell'Ente, deve essere definito un apposito piano di formazione che in termini generali preveda che: l'efficacia delle misure predisposte, poichè subordinata alla collaborazione ed alla effettiva applicazione da parte degli incaricati, deve, con cadenza periodica e, comunque, ogni qualvolta vi siano rilevanti modifiche del piano di sicurezza, prevedere che gli incaricati ed i responsabili siano edotti sulle misure che devono essere adottate e dei rischi che sono stati individuati. L'attività di formazione viene svolta in considerazione delle effettive necessità operative e di conoscenza di ciascun incaricato, responsabile o gruppo.

Revisione della sicurezza

L'efficacia delle misure di sicurezza come specificate nel presente documento, ed in tutta la documentazione che l'Ente dovrà produrre sia in osservanza di obblighi di legge sia per specifiche scelte interne, deve essere verificata periodicamente e comunque almeno una volta l'anno. L'Ente deve perseguire una politica dinamica di gestione della sicurezza e, ne consegue che, ove si manifestasse l'esigenza, il Documento Programmatico della Sicurezza e tutta la documentazione a corredo deve essere sottoposta periodicamente a revisione.

Auditing (verifiche ispettive) della sicurezza

L'efficacia delle misure di sicurezza deve essere verificata periodicamente e comunque almeno una volta l'anno, individuando apposito personale responsabile (interno o esterno all'Ente), con le modalità minime di controllo indicate dall'Allegato B della normativa, ovvero modalità idonee al reale stato di applicazione.

1.3. Campo di applicazione

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

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

- Sensibili
- Giudiziari
- Comuni

Si veda il paragrafo 1.5 per le definizioni di dettaglio.

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 (ed esempio: Cartacei, Audio, Visivi e Audiovisivi, ecc..)

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

1.4. Riferimenti normativi

1. CODICE IN MATERIA DI DATI PERSONALI (Dlgs. n.196 del 30 giugno 2003)
2. DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA (Allegato B al Dlgs. n.196 del 30 giugno 2003)
3. REGOLAMENTO SUL TRATTAMENTO DEI DATI SENSIBILI E GIUDIZIARI

1.5. Definizioni

1.5.1. 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.

1.5.2. 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.

1.5.3. 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.

1.5.4. 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.

1.5.5. 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.

1.5.6. 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.

1.5.7. Incaricati

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

1.5.8. Interessato

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

1.5.9. 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.

1.5.10. Diffusione

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

1.5.11. Dato anonimo

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

1.5.12. Blocco

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

1.5.13. Banca dati

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

1.5.14. 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.

1.5.15. 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.

1.5.16. Strumenti elettronici

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

1.5.17. Autenticazione informatica

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

1.5.18. 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.

1.5.19. 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.

1.5.20. 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.

1.5.21. 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.

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

2.1. Titolare del trattamento dei dati personali

Titolare del trattamento dei dati è il Comune di Città di Castello, rappresentato allo scopo dal Sindaco pro tempore.

2.1.1. 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, previa idonee istruzioni fornite per iscritto.

Il Titolare del trattamento può decidere di affidare il trattamento dei dati in parte all'esterno della struttura, nei modi previsti dagli incarichi specifici che emana direttamente o per tramite dei Responsabili del trattamento dei dati.

Avvalendosi della possibilità prevista dall'Art. 29 del Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003), il Titolare del trattamento, per esigenze organizzative, designa più soggetti Responsabili del trattamento dati mediante suddivisione di compiti, i quali sono individuati tra i Dirigenti dei Settori poiché questi soggetti, per esperienza, capacità ed affidabilità, forniscono 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 dati sono analiticamente specificati per iscritto dal Titolare del trattamento. I Responsabili del trattamento effettuano il trattamento attenendosi alle istruzioni impartite dal Titolare del trattamento, con specifici dettagli descritti al paragrafo 2.3.

Per esigenze organizzative, il Titolare individua uno o più soggetti come Gruppo di Coordinamento ed Indirizzo ai fini della tutela dei dati personali (INFOSEC) composto da soggetti interni all'Ente, cui è affidato il ruolo di coordinamento ed indirizzo della sicurezza dei dati personali.

2.2. Coordinamento ed indirizzo ai fini della sicurezza dei dati personali (INFOSEC)

2.2.1. Compiti di INFOSEC

Ad INFOSEC spettano i seguenti compiti:

- Dare supporto ai Responsabili del Trattamento affinché tutte le misure in materia di sicurezza riguardanti i dati personali siano applicate
- Dare supporto ai Responsabili del Trattamento affinché siano aggiornati ad ogni variazione l'elenco delle sedi e degli uffici in cui vengono trattati i dati
- Dare supporto ai Responsabili del Trattamento affinché siano aggiornati ad ogni variazione l'elenco delle banche dati oggetto di trattamento
- Se il trattamento è effettuato con mezzi informatici, dare supporto ai Responsabili del Trattamento e all'Amministratore di Sistema affinché siano aggiornati ad ogni variazione l'elenco dei sistemi di elaborazione
- Dare supporto ai Responsabili del Trattamento affinché siano definite e verificate periodicamente le modalità di accesso ai locali e le misure da adottare per la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità
- Qualora il trattamento dei dati sia stato affidato in tutto o in parte all'esterno della struttura del titolare, dare supporto ai Responsabili del Trattamento affinché siano controllate e garantite le applicazioni di tutte le misure di sicurezza riguardanti i dati personali
- Dare supporto ai Responsabili del Trattamento affinché siano individuate tutte le figure previste dal Codice in materia di protezione dei dati personali.

2.2.2. Nomina dei componenti singoli o di gruppo di INFOSEC (Coordinamento ed indirizzo ai fini della sicurezza dei dati personali)

La nomina al Gruppo di Coordinamento della sicurezza dei dati personali è effettuata dal Titolare del trattamento con lettera di incarico in cui sono specificate le responsabilità affidate.

Il Titolare del trattamento può, in qualunque momento, affidare i compiti previsti dai componenti di INFOSEC ad altro soggetto.

2.3. Responsabile di specifico trattamento dei dati personali

I Responsabili del trattamento dei dati personali sono i garanti dei trattamenti dei dati personali eseguiti nell'ambito di funzioni omogenee dell'Ente. Possono essere nominati dal Titolare del trattamento dati con atto proprio. Laddove nominati, hanno i compiti definiti nel paragrafo che segue.

2.3.1. Compiti del responsabile di uno specifico trattamento di dati personali

I Responsabili di uno specifico trattamento di dati personali hanno il compito di:

- Nominare gli Incaricati del trattamento dei dati personali (interni ed esterni) limitatamente ai Trattamenti di cui sono responsabili, nelle forme previste all'interno del presente documento
- Sorvegliare che il trattamento sia effettuato nei termini e nei modi stabiliti 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)
- 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.

2.3.2. Nomina dei responsabili di uno specifico trattamento di dati personali

La nomina di ciascun Responsabile di uno specifico trattamento di dati personali è effettuata dal Titolare del trattamento con lettera di incarico in cui sono specificate le responsabilità che gli sono affidate, controfirmata dall'Interessato per accettazione.

Nella lettera di nomina debbono essere indicati i Trattamenti di cui è responsabile per quanto attiene alla sicurezza e a quanto stabilito dal 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).

Copia della lettera di nomina accettata deve essere conservata a cura di INFOSEC in luogo sicuro.

Il Titolare del trattamento ha informato 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).

Il Titolare del trattamento rende disponibile a ciascun Responsabile di uno specifico trattamento di dati personali una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina, unitamente al presente documento, agli allegati descritti e ogni altra documentazione tecnica e/o organizzativa che riterrà utile.

La nomina del Responsabile di uno specifico trattamento di dati personali è a tempo indeterminato, e decade per revoca data dal Titolare del trattamento ovvero per dimissioni o designazione ad altra mansione del Responsabile di uno specifico trattamento di dati personali.

La nomina del Responsabile di uno specifico trattamento di dati personali può essere pertanto affidata dal Titolare del trattamento dati ad altro soggetto in qualunque momento.

2.4. Incaricati della gestione e della manutenzione degli strumenti elettronici

2.4.1. Compiti degli incaricati della gestione e della manutenzione degli strumenti elettronici contenenti dati

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) il Responsabile di specifico trattamento dei dati personali, in relazione all'attività svolta, ha individuato, nominato e incaricato per iscritto più Incaricati della gestione e della manutenzione degli strumenti elettronici contenenti dati.

Ogni Incaricato della gestione e della manutenzione degli strumenti elettronici è persona fisica o giuridica che sovrintende alle risorse messe a disposizione dell'Ente che contengono, in qualunque forma, una o più Banche di dati.

E' compito degli Incaricati della gestione e della manutenzione degli strumenti elettronici:

- Attivare per tutti i trattamenti di manutenzione le autorizzazioni di accesso a locali e informazioni, su indicazione del Responsabile di uno specifico trattamento di dati personali.
- Definire l'attivazione di idonei strumenti per la protezione contro il rischio di accesso abusivo ai dati, danneggiamento anche accidentale degli stessi, ovvero l'interruzione, totale o parziale, o l'alterazione del funzionamento. Questi strumenti debbono essere verificati con cadenza almeno semestrale.
- Informare il Titolare e il Responsabile dello specifico trattamento dei dati di competenza nella eventualità che si siano rilevati dei rischi relativamente alle misure di sicurezza riguardanti i dati personali contenuti negli strumenti oggetto della manutenzione.

2.4.2. Nomina degli incaricati della gestione e della manutenzione degli strumenti elettronici contenenti dati

Il Responsabile di specifico trattamento dei dati personali nomina uno o più soggetti Incaricati della gestione e della manutenzione degli strumenti elettronici a cui è stato conferito il compito di sovrintendere al buon funzionamento degli strumenti elettronici contenenti dati.

Il Responsabile dello specifico trattamento dati di competenza informa 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), dal Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003) ed ogni altro documento o disciplinare o policy tecnica approvata dal Responsabile dello specifico trattamento dati di competenza.

La nomina di uno o più Incaricati della gestione e della manutenzione degli strumenti elettronici è effettuata con una lettera di incarico del Responsabile di specifico trattamento dei dati personali ed è controfirmata per accettazione; copia della lettera di nomina accettata deve essere conservata a cura del Responsabile di specifico trattamento dei dati personali o dall'Incaricato in luogo sicuro.

Il Responsabile dello specifico trattamento dati di competenza rende disponibile 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, unitamente al presente documento, agli allegati descritti e ogni altra documentazione tecnica e/o organizzativa riterrà utile.

La nomina dell'Incaricato della gestione e della manutenzione degli strumenti elettronici è a tempo indeterminato, e decade per revoca data dal Titolare del trattamento ovvero dal Responsabile di specifico trattamento dei dati personali ovvero per dimissioni o designazione ad altra mansione dell'Incaricato medesimo.

Copia della lettera di nomina accettata deve essere conservata a cura di INFOSEC in luogo sicuro.

La nomina del Responsabile di uno specifico trattamento di dati personali può essere pertanto affidata ad altro soggetto in qualunque momento.

2.5. Incaricato della custodia delle copie delle Credenziali

2.5.1. Compiti degli incaricati della custodia delle copie 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), sono impartite idonee e preventive disposizioni scritte volte ad individuare chiaramente le modalità con le quali il Responsabile di specifico trattamento dei dati personali 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.

Il Responsabile di specifico trattamento dei dati personali, in relazione all'attività svolta, individua, nomina e incarica per iscritto, uno o più Incaricati della custodia delle copie delle Credenziali.

E' compito dell'Incaricato 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 eventualmente 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 riservato delle componenti delle Credenziali di autenticazione, e sulle caratteristiche che debbono 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/o di sicurezza del sistema, l'Incaricato della custodia delle copie delle Credenziali, in accordo con il Responsabile dello specifico trattamento di dati personali, assicura la disponibilità di dati o strumenti elettronici operando secondo le seguenti istruzioni:

1. Utilizzando i diritti di amministratore di sistema, modifica 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 al Responsabile dello specifico trattamento di dati personali il quale potrà utilizzarla o farla utilizzare ad un altro Incaricato del trattamento dei dati personali designato, solo temporaneamente e per il tempo strettamente indispensabile alle attività di operatività e/o di sicurezza del sistema.
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 al primo accesso utile al sistema.

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

1. Utilizzando i diritti di amministratore di sistema, modifica in modo forzoso la componente riservata delle Credenziali di autenticazione del Responsabile dello specifico trattamento di dati personali assente o impedito ad effettuare il trattamento.
2. Comunica la componente riservata delle Credenziali di autenticazione così modificata al Segretario Generale il quale potrà utilizzarla o farla utilizzare ad un altro Incaricato del trattamento dei dati personali designato, solo temporaneamente e per il tempo strettamente indispensabile alle attività di operatività e/o di sicurezza del sistema.
3. Terminata l'assenza o l'impedimento del Responsabile dello specifico trattamento di dati personali 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 al primo accesso utile al sistema.

Qualora si adottino criteri automatici di gestione delle attività appena descritte, il ruolo dell'Incaricato della custodia delle copie delle Credenziali potrà essere assegnato all'Amministratore di Sistema.

2.5.2. Nomina degli incaricati della custodia delle copie 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), il Responsabile dello specifico trattamento dei dati di competenza nomina un soggetto Incaricato 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 dell'Incaricato della custodia delle copie delle Credenziali è effettuata con una lettera di incarico ed è controfirmata per accettazione; copia della lettera di nomina accettata è conservata a cura di INFOSEC in luogo sicuro.

Il Responsabile dello specifico Trattamento dei dati informa l'Incaricato della custodia delle copie delle Credenziali della responsabilità che gli è 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).

Il Responsabile dello specifico Trattamento dei dati rende disponibile 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, unitamente al presente documento, agli allegati descritti e ogni altra documentazione tecnica e/o organizzativa riterrà utile.

La nomina dell'Incaricato della custodia delle copie delle Credenziali è a tempo indeterminato, e decade per revoca data dal Titolare del trattamento ovvero dal Responsabile di specifico trattamento dei dati personali ovvero per dimissioni o designazione ad altra mansione dell'Incaricato medesimo.

La nomina dell'Incaricato della custodia delle copie delle Credenziali può essere pertanto affidata ad altro soggetto in qualunque momento.

2.6. Incaricato delle copie di sicurezza delle banche dati

2.6.1. 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) il Responsabile di specifico trattamento dei dati personali del trattamento dati, in relazione all'attività svolta, individua, nomina e incarica per iscritto uno o più Incaricati delle copie di sicurezza delle banche dati.

L'Incaricato delle copie di sicurezza delle banche dati è la persona fisica che ha il compito di sovrintendere alla esecuzione periodica delle copie di sicurezza delle Banche dati personali gestite direttamente presso la struttura dell'Ente. Per questo, ove non diversamente specificato, per Incaricato delle copie di sicurezza delle banche dati si intende un incaricato interno all'Ente.

Le Banche dati gestite esternamente all'Ente, in modalità di outsourcing da persona fisica o giuridica (soggetti denominati outsourcer), sono gestite da Incaricati esterni alle copie di sicurezza delle banche dati individuati ed incaricati, in forma scritta, dal Responsabile dello specifico trattamento dati che ha competenza di governare sull'operato degli outsourcer suddetti. Tali attività non rientrano, pertanto, tra i compiti specifici dell'Incaricato delle copie di sicurezza delle banche dati qui descritti. Le politiche di gestione delle copie di sicurezza delle banche dati eseguite da Incaricati esterni possono, tuttavia, essere pienamente conformate a quelle descritte per gli Incaricati interni alle copie di sicurezza dei dati; in ogni caso sono approvate dal Responsabile dello specifico trattamento dati cui compete il controllo delle attività dell'outsourcer, il quale può chiedere parere favorevole all'Incaricato delle copie di sicurezza delle banche dati e/o al Responsabile per la sicurezza dei dati personali.

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, il Responsabile di specifico trattamento dei dati personali di competenza stabilisce, con il supporto tecnico eventuale dell'Incaricato della gestione e della manutenzione degli strumenti elettronici, la periodicità con cui debbono essere effettuate le copie di sicurezza delle Banche di dati trattate.

I criteri possono 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 debbono essere effettuate le copie dei dati personali non deve superare in nessun caso i 7 (sette) giorni dall'ultima copia di sicurezza eseguita.

In particolare, esiste una politica formale di copia delle Banche di dati nella quale sono 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 dell'Incaricato 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 dal Responsabile di specifico trattamento dei dati personali di competenza.
- 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 si adottino criteri automatici di gestione delle attività appena descritte, il ruolo dell'Incaricato delle copie di sicurezza può essere assegnato all'Amministratore di Sistema.

2.6.2. 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) il Responsabile di specifico trattamento dei dati personali, in relazione all'attività svolta, individua, nomina e incarica per iscritto un Incaricato 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 direttamente dall'Ente, specificando gli elaboratori o le banche dati che è chiamato a sovrintendere. Per questo, ove non diversamente specificato, per Incaricato delle copie di sicurezza delle banche dati si intende l'incaricato interno all'Ente.

Il Responsabile di specifico trattamento dei dati personali di competenza informa 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 è effettuata con una lettera di incarico ed è controfirmata.

Copia della lettera di nomina accettata è conservata a cura di INFOSEC in luogo sicuro.

Il Responsabile di specifico trattamento dei dati personali di competenza rende disponibile 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, unitamente al presente documento, agli allegati descritti e ogni altra documentazione tecnica e/o organizzativa riterrà utile.

2.7. Incaricato della custodia delle aree e dei locali

2.7.1. Compiti degli incaricati della custodia delle aree e dei locali

In conformità a quanto disposto dal punto 19.4 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) il Responsabile di specifico trattamento dei dati personali del trattamento, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più Incaricati della custodia delle aree e dei locali in cui sono effettuati i trattamenti di dati personali o in cui vengono conservati documenti contenenti dati personali.

Gli Incaricati della custodia delle aree e dei locali debbono:

- Consentire l'accesso alle aree e ai locali di cui debbono assicurare il controllo solo agli Incaricati del trattamento autorizzati.
- Identificare e registrare le persone ammesse, a qualunque titolo, dopo l'orario di chiusura.
- Informare tempestivamente il Titolare e il Responsabile di specifico trattamento dei dati personali di competenza nel caso in cui si siano riscontrate situazioni anomale.
- Controllare la chiusura dei locali al termine dell'orario.

Qualora il Titolare non ritenga di nominare alcun Incaricato della custodia delle aree e dei locali, il Responsabile di specifico trattamento dei dati personali di competenza ne assumerà tutte le responsabilità e funzioni.

2.7.2. Nomina degli incaricati della custodia delle aree e dei locali

In conformità a quanto disposto dal punto 19.4 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) il Titolare, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più Incaricati della custodia delle aree e dei locali in cui sono effettuati i trattamenti di dati personali o in cui vengono conservati documenti contenenti dati personali.

Il Responsabile di specifico trattamento dei dati personali di competenza deve informare ciascun Incaricato della custodia delle aree e dei locali 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 custodia delle aree e dei locali deve essere effettuata con una lettera di incarico e deve essere controfirmata.

Copia della lettera di nomina accettata deve essere conservata a cura di INFOSEC in luogo sicuro.

La nomina dell'Incaricato della custodia delle aree e dei locali può essere revocata in qualsiasi momento dal soggetto che gli ha affidato l'incarico, senza preavviso, ed eventualmente può essere affidata ad altro soggetto.

2.8. Incaricato del trattamento dei dati personali

2.8.1. Compiti degli incaricati del trattamento dei dati personali

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, interni all'Ente o esterni, che operano sotto la diretta autorità del Responsabile di uno specifico trattamento di dati personali cui gli Incaricati fanno riferimento per competenza e mansione, 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, che può essere comunicato all'atto della designazione lavorativa (contratto di assunzione, ordine di servizio, disposizioni, ecc.) ovvero con lettera di incarico al trattamento dati specifica, con la conseguente possibilità di accesso ed utilizzo della documentazione cartacea e degli strumenti informatici, elettronici e telematici e delle banche dati 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 ed 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.
- E' inoltre tassativamente proibito utilizzare copie fotostatiche di documenti (anche se non perfettamente riuscite) all'esterno del posto di lavoro, né tantomeno si possono utilizzare come carta per appunti.
- 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.

2.8.2. Nomina degli incaricati del trattamento dei dati personali

La nomina degli Incaricati del trattamento dei dati personali è effettuata dal Responsabile di uno specifico trattamento di dati personali cui gli Incaricati fanno riferimento per competenza e mansione, con una lettera di incarico in cui sono specificati i compiti che sono stati affidati.

La lettera di incarico può essere indirizzata ad un singolo dipendente o ad un gruppo di dipendenti qualora alcuni trattamenti di dati siano condivisi tra più soggetti.

Il Responsabile di uno specifico trattamento di dati personali informa 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), dal Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003) ed ogni altro documenti di indirizzo o politica di gestione formale in merito di tutela del dato personale.

Il Responsabile della sicurezza dei dati personali rende disponibile 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, unitamente al presente documento, agli allegati descritti e ogni altra documentazione tecnica e/o organizzativa riterrà utile.

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

Agli Incaricati del trattamento dei dati personali è 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 data dal Titolare del trattamento (o dal Responsabile dello specifico trattamento di dati personali che gli ha affidato l'incarico) ovvero per dimissioni o designazione ad altra mansione dell'Incaricato medesimo.

Copia della lettera di nomina accettata deve essere conservata a cura di INFOSEC in luogo sicuro.

La nomina dell'Incaricato può essere pertanto affidata in qualunque momento ad altro soggetto.

2.9. Amministratore di sistema

2.9.1. Compiti dell' Amministratore di sistema

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) e dal Provv. Gen. Garante Privacy sulla figura dell'Amministratore di Sistema e s.m.i. il Titolare, individua, nomina e incarica per iscritto, uno o più Amministratore di Sistema, cui è conferito il compito di sovrintendere alle risorse del sistema e di consentirne l'utilizzazione, secondo le seguenti disposizioni, oltre a quelle previste nella lettera di incarico e nel Provv. Gen. Garante Privacy citato:

- Verificare la rispondenza del sistema informatico rispetto alle norme sulla sicurezza emanate dal Garante della Privacy, ed in base alle risultanze provvedere agli adempimenti necessari in relazione alle disposizioni di legge in materia di sicurezza del trattamento dei dati.
- Gestire il sistema informatico, nel quale risiedono le banche dati, in base alle disposizioni del D. Lgs. n. 196/2003, del relativo Allegato B e dei successivi disciplinari tecnici, attenendosi alle disposizioni in esse contenute.
- Collaborare con il Titolare, il Responsabile della sicurezza dei dati personali ed i Responsabili degli specifici trattamenti di dati personali al fine di esercitare un doveroso controllo sulle attività effettuate dagli incaricati al trattamento, affinché le azioni svolte siano rispondenti alle norme vigenti.
- Sovrintendere alle attività di salvaguardia degli archivi, individuare eventualmente un preposto alla custodia delle Credenziali di autenticazione e provvedere, in collaborazione con il preposto eventualmente individuato alla custodia, affinché siano assegnate le parole chiave di accesso al sistema agli utilizzatori che ne abbiano facoltà.
- Provvedere ad attivare un sistema efficace di gestione giornaliera delle copie di sicurezza degli archivi di dati.
- Predisporre, mediante adeguati strumenti, tutte le misure idonee a limitare danni conseguenti a guasti tecnici, violazione del sistema, virus informatici e quanto altro possa mettere a rischio i dati.
- Curare l'aggiornamento periodico dei programmi antivirus in conformità al disposto dell'Allegato B del D. Lgs. n. 196/2003.
- Verificare la situazione del software installato, sia per una maggiore tutela nei confronti di programmi che potrebbero danneggiare il sistema, sia per dare attuazione al rispetto delle norme sulla tutela dei diritti d'autore. Potrà pertanto proporre, di concerto con il Responsabile della sicurezza dei dati, eventuali Regolamenti tecnici specifici (denominati policy) nei quali si stabiliscano le norme di comportamento per l'utilizzo dei sistemi (strumenti e programmi), ponendo particolare attenzione ad evitare l'installazione di software non autorizzato (anche se gratuito).
- Assegnare agli utilizzatori dei terminali i codici di autenticazione (codice utente e Password associata) e gestire gli stessi in base ai disposti dell'Allegato B del D. Lgs. n. 196/2003.
- Predisporre ed aggiornare, in collaborazione con il Titolare o il Responsabile dei dati personali o i Responsabili degli specifici trattamenti dei dati personali, il sistema di sicurezza in base alle disposizioni degli Artt. 31, 33 e 34 D. Lgs. n. 196/2003.
- Relazionare almeno annualmente al Titolare del Trattamento dati sullo stato del sistema informatico e sulle iniziative avvenute per la miglioria del medesimo

2.9.2. Nomina dell'Amministratore di Sistema

La nomina dell'Amministratore di Sistema è effettuata dal Titolare, con una lettera di incarico in cui sono specificati i compiti che gli sono stati affidati e che è controfirmata dall'Interessato per presa visione.

Copia della lettera di nomina firmata è conservata a cura del Titolare o di INFOSEC in luogo sicuro.

Il Titolare informa l'Amministratore di Sistema 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) e dal Provv. Gen. Garante Privacy in materia di Amministratore di Sistema e s.m.i.

Il Titolare o INFOSEC se delegato rende disponibile all'Amministratore di Sistema una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina, unitamente al presente documento, agli allegati descritti e ogni altra documentazione tecnica e/o organizzativa riterrà utile.

La nomina dell'Amministratore di Sistema è a tempo indeterminato, ma è soggetta a revisione e conferma almeno annuale da parte del Titolare, con i criteri previsti dal Provv. Gen. Garante Privacy di riferimento; decade per revoca data dal Titolare che gli ha affidato l'incarico ovvero per dimissioni o designazione ad altra mansione dell'Amministratore di Sistema.

La nomina dell'Amministratore di Sistema può essere pertanto affidata ad altro soggetto, interno all'Ente o esterno a questo, sia a persona fisica che persona giuridica.

Copia della lettera di nomina accettata deve essere conservata a cura di INFOSEC in luogo sicuro.

3. Trattamenti con l'ausilio di strumenti elettronici

3.1. Sistema di autenticazione informatica

3.1.1. Procedura di identificazione

In conformità a quanto disposto dal punto 1 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003), poichè il trattamento di dati personali è effettuato con strumenti elettronici, il Responsabile della sicurezza dei dati personali si assicura che il trattamento sia consentito solamente agli Incaricati del trattamento dei dati personali dotati di Credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti e di autorizzazione relativa.

3.1.2. Identificazione dell'incaricato

In conformità a quanto disposto dal punto 2 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) il Responsabile della sicurezza dei dati personali, avvalendosi della collaborazione dell'Incaricato della custodia delle copie delle Credenziali e dell'Incaricato della gestione e della manutenzione degli strumenti elettronici (se necessario) si assicura che il trattamento di dati personali, effettuato con strumenti elettronici, sia consentito solamente agli Incaricati del trattamento dotati di una Credenziale di autenticazione, costituita da un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo.

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) ad ogni Incaricato del trattamento possono essere assegnate o associate individualmente una o più Credenziali per l'autenticazione.

3.1.3. Cautele per assicurare la segretezza della componente riservata della credenziale

In conformità a quanto disposto dal punto 4 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) gli Incaricati devono adottare le necessarie cautele per assicurare la segretezza della parola chiave e custodire diligentemente ogni altro dispositivo che gli è stato affidato per i sistemi di autenticazione informatica (badge magnetici, tessere magnetiche, ecc..).

Inoltre ogni Incaricato del trattamento è informato e reso edotto che le Credenziali di autenticazione:

- Sono personali
- Devono essere memorizzate
- Non devono essere comunicate a nessuno
- Non devono essere trascritte

3.1.4. Caratteristiche della parola chiave

In conformità a quanto disposto dal punto 5 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) la Componente riservata delle Credenziali di autenticazione (parola chiave o password) rispetta i seguenti criteri:

- Non deve contenere nomi comuni
- Non deve contenere nomi di persona
- Deve contenere sia lettere che numeri
- Deve comprendere maiuscole e minuscole
- Deve essere diversa dallo User-Id
- Deve essere lunga almeno 8 caratteri fino al massimo consentito dal sistema di autenticazione
- Non deve essere riconducibile all'incaricato

Possono essere assegnati criteri di caratteristiche della parola chiave in maniera maggiormente restrittiva, qualora il Titolare del Trattamento o l'Amministratore di Sistema ritengano di applicare tali canoni per ragioni di idonee misure di sicurezza.

3.1.5. Modalità di richiesta delle Credenziali di autenticazione

L'assegnazione delle Credenziali di autenticazione avviene dietro specifica richiesta del Responsabile di uno specifico trattamento.

La richiesta viene inoltrata all'Amministratore di Sistema in forma scritta (nell'ordine) dal Responsabile di specifico trattamento dei dati ovvero dalla figura apicale di riferimento dell'Incaricato al trattamento al quale si intende fornire Credenziali di autenticazione.

L'Amministratore di Sistema provvede:

- A comunicare all'Incaricato del trattamento dei dati personali, nonché a colui che ha eseguito formale richiesta scritta, al momento dell'attivazione, la sua Credenziale di autenticazione.
- A comunicare all'Incaricato del trattamento dei dati personali al momento dell'attivazione la sua Componente riservata delle Credenziali di autenticazione (parola chiave o password) temporanea, che sarà modificata al primo accesso.
- Alla abilitazione dei permessi che consentano all'Incaricato del trattamento dei dati personali di accedere al trattamento che gli è stato affidato.
- Ad effettuare le verifiche di corretto accesso.
- A conservare copia della richiesta.

Il Responsabile di uno specifico trattamento informa i propri Incaricati del trattamento dei criteri e delle regole che devono essere osservate per assicurare la segretezza della Componente riservata delle Credenziali di autenticazione (parola chiave o password).

Il Responsabile di uno specifico trattamento che ha effettuato la richiesta fornisce idonee informazioni, anche in forma strutturata, con le quali sono specificati i criteri che devono essere rispettati per la Componente riservata delle Credenziali di autenticazione (parola chiave o password), secondo quanto riportato dal "Regolamento sull'accesso e l'uso delle risorse informatiche e telematiche con riguardo alla disciplina della tutela dei dati personali per il sistema informativo comunale".

Al primo accesso l'Incaricato del trattamento dovrà modificare la Componente riservata delle Credenziali di autenticazione (parola chiave o password) rispettando le regole descritte nel "Regolamento sull'accesso e l'uso delle risorse informatiche e telematiche con riguardo alla disciplina della tutela dei dati personali per il sistema informativo comunale".

È compito dell'Amministratore di Sistema approntare, direttamente o per mezzo di deleghe di compiti specifici, gli strumenti ed i controlli mediante cui verificare il corretto uso delle Credenziali di autenticazione e monitorare e vigilare sui tentativi di accesso non autorizzato.

I tentativi di accesso non autorizzati al sistema saranno registrati e dovrà essere data tempestiva comunicazione al Responsabile dello specifico trattamento dei dati di competenza da parte dell'Amministratore di Sistema.

In caso di smarrimento della Componente riservata delle Credenziali di autenticazione (parola chiave o password) il Responsabile dello specifico trattamento dell'incaricato dovrà richiedere all'Amministratore di Sistema una nuova assegnazione.

Le Credenziali di autenticazione che non sono utilizzate per più di 6 mesi dovranno essere disabilitate d'autorità dall'Amministratore di Sistema.

I Responsabili di uno specifico trattamento devono dare informazione dall'Amministratore di Sistema circa le dimissioni del personale o lo spostamento di mansione per annullare le Credenziali di autenticazione dell'Incaricato del trattamento.

3.1.6. Istruzioni per non lasciare incustodito e accessibile lo strumento elettronico

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) gli Incaricati del trattamento hanno l'obbligo di:

- Non lasciare incustodito il proprio posto di lavoro.
- Di chiudere tutte le applicazioni aperte o meglio ancora di spegnere il sistema informatico in caso di assenza prolungata.
- Di bloccare l'uso della postazione di lavoro, mediante funzionalità specifica del sistema operativo, in caso di breve assenza dal posto di lavoro, attivata manualmente o in forma automatica.

3.1.7. Accesso straordinario

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) gli Incaricati della custodia delle copie delle Credenziali, hanno il compito di assicurare la disponibilità dei dati e degli 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.

Il Responsabile del trattamento specifico dei dati di competenza richiede, con atto scritto e motivato, dall'Amministratore di Sistema di accedere con le proprie credenziali di amministratore di sistema e provvedere all'annullamento della password dell'incaricato assente ed assegna una credenziale di autenticazione temporanea allo scopo.

L'incaricato assente, nel momento di ripresa delle attività sulla propria postazione di lavoro, avuta notizia dell'annullamento della credenziale di autenticazione precedente in forma scritta, dovrà provvedere alla richiesta di una nuova credenziale di autenticazione.

In conformità a quanto disposto dal punto 11 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

3.2. Sistema di autorizzazione

Ogni Responsabile di uno specifico trattamento di dati personali individua gli Incaricati del trattamento per ogni tipologia di banca di dati personali trattata.

In conformità a quanto disposto dal punto 12 e dal punto 13 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) il tipo di trattamento effettuato da ogni singolo Incaricato del trattamento risulta essere differenziato.

In particolare il Responsabile di uno specifico trattamento di dati personali autorizza le operazioni di trattamento consentite ad ogni Incaricato del trattamento tra le seguenti:

- Inserire nuove informazioni nella banca di dati personali.
- Accedere alle informazioni in visualizzazione e stampa.
- Modificare le informazioni esistenti nella banca di dati personali.
- Cancellare le informazioni esistenti nella banca di dati personali.

In conformità a quanto disposto dal punto 15 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) almeno una volta l'anno e comunque entro il 31 marzo, ogni Responsabile di uno specifico trattamento di dati personali aggiorna l'Elenco dei permessi di accesso che sono stati assegnati agli Incaricati del trattamento per ogni tipologia di banca di dati.

In conformità a quanto disposto dal punto 19.2 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. 196 del 30 giugno 2003), tale Elenco si evince dalle schede compilate a cura del Responsabile di uno specifico trattamento di dati personali. Il dettaglio sui profili di autorizzazione di ogni utente è desumibile dalle policy specifiche assegnate a livello di sistema informativo comunale.

3.3. Altre misure di sicurezza

In considerazione di quanto disposto 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), oltre all'applicazione di altre norme specifiche, è fatto divieto a chiunque di:

- Effettuare copie su supporti magnetici o trasmissioni telematiche non autorizzate formalmente dal Responsabile di uno specifico trattamento di dati personali di dati oggetto del trattamento, ed in ogni caso non strettamente riferibili alle attività lavorative ed istituzionali dell'Ente.
- Effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate formalmente dal Responsabile di uno specifico trattamento di dati personali, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento, ed in ogni caso non strettamente riferibili alle attività lavorative ed istituzionali dell'Ente.
- Sottrarre, cancellare, distruggere senza l'autorizzazione formale del Responsabile di uno specifico trattamento di dati personali, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.
- Consegnare a persone non autorizzate formalmente dal Responsabile di uno specifico trattamento di dati personali, stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

3.4. Periodicità di revisione del documento programmatico sulla sicurezza

Entro il 31 marzo di ogni anno, il Titolare del trattamento di dati sensibili o di dati giudiziari verifica ed aggiorna il Documento Programmatico sulla Sicurezza contenente idonee informazioni riguardo ai punti 19.1, 19.2, 19.3, 19.4, 19.5, 19.6, 19.7, 19.8 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).

3.5. Elenco dei trattamenti di dati personali

3.5.1. Elenco delle sedi e degli uffici in cui vengono trattati i dati

Al Responsabile della sicurezza dei dati personali è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco delle sedi in cui viene effettuato il trattamento dei dati.

In conformità a quanto disposto dal punto 19.1 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) l'elenco delle sedi si evince dalle schede compilate a cura del Responsabile di uno specifico trattamento di dati personali. Le sedi presso cui vengono trattati i dati sono quelle istituzionali dell'Ente.

3.5.2. Elenco degli archivi dei dati oggetto del trattamento

Al Responsabile dello specifico trattamento di dati personali è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco delle tipologie di trattamenti effettuati.

Ogni banca di dati o archivio deve essere classificato in relazione alle informazioni contenute indicando se si tratta di:

- Dati personali comuni
- Dati personali sensibili
- Dati personali giudiziari

In conformità a quanto disposto dal punto 19.1 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) l'individuazione degli archivi dei dati oggetto del trattamento si evince dalle schede compilate a cura del Responsabile di uno specifico trattamento di dati personali. Il modello della scheda è allegato (Allegato 1) al presente Documento Programmatico sulla Sicurezza.

3.5.3. Elenco dei sistemi di elaborazione per il trattamento

All'Amministratore di Sistema è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione con cui viene effettuato il trattamento dei dati.

Per ogni sistema deve essere specificato:

- Il nome dell'Incaricato della gestione e della manutenzione.
- Il nome dell'incaricato o degli incaricati che lo utilizzano.
- Il nome di uno o più Incaricati della custodia delle copie delle Credenziali.

In conformità a quanto disposto dal punto 19.1 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) i sistemi si evincono dalle schede compilate a cura del Responsabile di uno specifico trattamento di dati personali. L'elenco dei sistemi e dei profili utente è mantenuto mediante procedure informatizzate.

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

3.6.1. Elenco dei soggetti autorizzati al trattamento dei dati

Ogni Responsabile di uno specifico trattamento di dati personali ha il compito di:

- Nominare gli Incaricati del trattamento dei dati personali (siano essi interni o esterni) limitatamente alle Banche di dati di cui sono responsabili
- Richiedere e comunicare le Credenziali di autenticazione
- Informare l'Amministratore di Sistema delle variazioni intervenute nella struttura organizzativa.

Ogni Responsabile di uno specifico trattamento di dati personali tiene aggiornato ad ogni variazione l'Elenco del personale autorizzato al trattamento dei dati per quanto attiene alle competenze e mansioni specifiche della propria sfera di responsabilità.

Ogni elenco del personale autorizzato al trattamento dei dati deve essere redatto dal Responsabile di uno specifico trattamento di dati personali.

3.6.2. Verifiche periodiche delle condizioni per il mantenimento delle autorizzazioni

I Responsabili degli specifici trattamenti di dati personali hanno il compito di verificare ogni anno, entro il 31 marzo, le Credenziali di autenticazione assegnate agli incaricati che afferiscono allo loro sfera di competenza e mansione.

Ogni Responsabile degli specifici trattamenti di dati personali tiene pertanto aggiornato costantemente ogni variazione dell'Elenco del personale autorizzato al trattamento dei dati che afferisce al Responsabile in questione.

Ogni Elenco del personale autorizzato al trattamento dei dati si evince dalle Schede di rilevazione del trattamento dati compilate a cura del Responsabile di uno specifico trattamento di dati personali.

3.6.3. Distribuzione dei compiti e delle responsabilità

In conformità a quanto disposto dal punto 19.2 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. 196 del 30 giugno 2003), il Responsabile dello specifico trattamento dei dati di competenza autorizza la struttura di riferimento, assegna i compiti e le relative responsabilità, in relazione ai trattamenti effettuati.

3.7. Analisi dei rischi

3.7.1. Analisi dei rischi hardware

Il Responsabile della sicurezza dei dati personali, anche avvalendosi di consulenti interni o esterni e/o della collaborazione dall'Amministratore di Sistema, deve verificare ogni anno:

- La situazione delle apparecchiature hardware installate con cui vengono trattati i dati.
- La situazione delle apparecchiature periferiche.
- La situazione dei dispositivi di collegamento con le reti pubbliche.

La verifica ha lo scopo di controllare l'affidabilità del sistema tenendo conto anche dell'evoluzione tecnologica, per quanto riguarda:

- La sicurezza dei dati trattati.
- Il rischio di distruzione o di perdita.
- Il rischio di accesso non autorizzato o non consentito

L'Amministratore di Sistema aggiorna il Report annuale dei rischi hardware.

In conformità a quanto disposto dal punto 19.3 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) l'analisi dei rischi viene redatta in base ai dati rilevati.

Gli Incaricati della gestione e della manutenzione degli strumenti elettronici nel caso in cui esistano rischi evidenti informano tempestivamente il Titolare o l'Amministratore di Sistema dei dati personali affinché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

3.7.2. Analisi dei rischi sui sistemi operativi e sui software installati

Al Responsabile della sicurezza dei dati personali, anche avvalendosi di consulenti interni o esterni e/o della collaborazione dall'Amministratore di Sistema, è affidato il compito di verificare ogni anno, la situazione dei Sistemi Operativi e delle applicazioni software installate sulle apparecchiature con cui vengono trattati i dati.

La verifica ha lo scopo di controllare l'affidabilità dei Sistemi Operativi e delle applicazioni software, per quanto riguarda:

- La sicurezza dei dati trattati.
- Il rischio di distruzione o di perdita.
- Il rischio di accesso non autorizzato o non consentito.

Tenendo conto in particolare di:

- Disponibilità di nuove versioni migliorative dei software utilizzati.
- Segnalazioni di Patch, Fix o System-Pack per la rimozione di errori o malfunzionamenti.
- Segnalazioni di Patch, Fix o System-Pack per l'introduzione di maggiori sicurezze contro i rischi di intrusione o di danneggiamento dei dati.

L'Amministratore di Sistema aggiorna il Report annuale dei rischi sui software installati.

In conformità a quanto disposto dal punto 19.3 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003), tale analisi dei rischi viene redatta in base ai dati rilevati.

Gli Incaricati della gestione e della manutenzione degli strumenti elettronici, nel caso in cui esistano rischi evidenti, informano tempestivamente il Titolare o l'Amministratore di Sistema affinché siano presi gli opportuni provvedimenti per assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

3.7.3. Analisi degli altri rischi nel trattamento dei dati

Ad INFOSEC, anche avvalendosi di consulenti interni o esterni, ed in collaborazione con i Responsabili degli specifici trattamenti di dati personali, è affidato il compito di analizzare eventuali altri rischi connessi al trattamento dei dati tenendo conto in particolare di:

- Rischi connessi al comportamento degli operatori.
- Rischi connessi al contesto fisico ed ambientale.

INFOSEC aggiorna il Report annuale degli altri rischi.

In conformità a quanto disposto dal punto 19.3 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) l'analisi dei rischi suddetta viene redatta in base ai dati rilevati.

INFOSEC, nel caso in cui esistano rischi evidenti, informano tempestivamente il Titolare o il Responsabile dello specifico trattamento dei dati di competenza affinché siano presi gli opportuni provvedimenti per assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

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

L'Amministratore di Sistema, anche avvalendosi di altre figure a supporto, interni o esterni, al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, stabilisce la periodicità con cui debbono essere effettuate le procedure che consentano di garantire l'integrità e la disponibilità dei dati trattati. I criteri sono definiti in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

Possono inoltre essere impartite precise istruzioni contenute in documenti di varia natura da portare a conoscenza dei Responsabili di uno specifico trattamento e degli Incaricati.

3.9. Misure da adottare per la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità

3.9.1. Misure generali

In considerazione di quanto disposto 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), è fatto divieto a chiunque di eseguire le attività elencate di cui al punto 3.3.

3.9.2. Procedure per controllare l'accesso ai locali in cui vengono trattati i dati

Possono inoltre essere impartite precise istruzioni contenute in documenti di varia natura da portare a conoscenza dei Responsabili di uno specifico trattamento e degli Incaricati.

3.10. Formazione degli incaricati del trattamento

3.10.1. Piano di formazione

In conformità a quanto disposto dal punto 19.6 del Disciplinare tecnico in materia di misure minime di sicurezza (Dlgs. n.196 del 30 giugno 2003) INFOSEC, in collaborazione con i Responsabili degli specifici trattamenti di dati personali, valuta per ogni incaricato a cui è stato affidato il trattamento, sulla base dell'esperienza, delle sue conoscenze, ed in funzione anche di eventuali opportunità offerte dall'evoluzione tecnologica, se è necessario pianificare interventi di formazione.

La formazione è programmata già al momento dell'ingresso in servizio di nuovi incaricati del trattamento, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.

INFOSEC, in collaborazione con i Responsabili degli specifici trattamenti di dati personali, redige ogni anno, entro il 31 marzo, il Piano di Formazione del personale limitatamente alle competenze in materia di privacy, specificando le necessità di ulteriore formazione del personale.

Il Piano di formazione del personale è predisposto per:

- Rendere edotti gli incaricati del trattamento sui rischi che incombono sui dati.
- Rendere edotti gli incaricati del trattamento sulle misure disponibili per prevenire eventi dannosi.
- Rendere edotti gli incaricati del trattamento sui profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività.
- Rendere edotti gli incaricati del trattamento sulle responsabilità che ne derivano.
- Rendere edotti gli incaricati del trattamento sulle modalità per aggiornarsi sulle misure minime adottate dal Titolare.

In conformità a quanto disposto dal punto 19.6 del Disciplinare tecnico in materia di misure minime di sicurezza (Dlgs. n.196 del 30 giugno 2003) si terranno eventi formativi rivolti a tutte le figure previste dal presente documento.

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

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

Il Titolare del trattamento dati ha facoltà di decidere di affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare, eventualmente sentito il parere di uno o più Responsabili di uno specifico trattamento di dati personali e/o dall'Amministratore di Sistema. Tali soggetti esterni possono essere persone fisiche o giuridiche (o comunque altre forme organizzative) che diano garanzia di affidabilità nella gestione di tali trattamenti esterni.

In caso in cui questo avvenga, il Responsabile della specifico trattamento dei dati di competenza, redige ed aggiorna 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 indica per ognuno di essi il tipo di trattamento effettuato, specificando:

- I soggetti interessati.
- I luoghi dove fisicamente avviene il trattamento dei dati stessi.
- I/Il responsabili/e del trattamento di dati personali di riferimento per l'Ente.
- La forma documentale che il soggetto esterno alla struttura dell'Ente mette a disposizione per le attività di controllo del proprio operato (a titolo di esempio e non esaustivo, Dichiarazioni di Conformità ai sensi del D.Lgs 196/03, Piano di sicurezza delle informazioni, Documento programmatico sulla sicurezza e simili).

L'inventario dei soggetti a cui affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare, si evince dalle schede compilate a cura del Responsabile di uno specifico trattamento di dati personali.

Nel caso in cui, per i trattamenti dei dati affidati in tutto o in parte all'esterno della struttura del titolare, sia possibile nominare responsabili del trattamento soggetti controllabili dal Titolare del trattamento stesso (relativamente alle modalità e alle misure minime di sicurezza da adottare nel trattamento stesso), gli stessi sono indicati quali Responsabili del trattamento in Out-sourcing.

Nel caso in cui sia stato nominato uno o più Responsabili del trattamento in Out-sourcing, in conformità a quanto disposto dal punto 19.7 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) saranno incaricati tramite opportuno modulo.

Nel caso in cui, per i trattamenti dei dati affidati in tutto o in parte all'esterno della struttura del titolare, non sia possibile nominare i responsabili del trattamento, in quanto soggetti autonomi non controllabili dal titolare del trattamento stesso (relativamente alle modalità e alle misure minime di sicurezza da adottare nel trattamento stesso), sono individuati i Titolari autonomi del trattamento in Out-sourcing, per il quale trattamento, ai sensi dell'art. 28 del Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003), si intendono autonomi titolari del trattamento e quindi soggetti ai corrispettivi obblighi, e pertanto rispondono direttamente ed in via esclusiva per le eventuali violazioni alla legge.

Nel caso in cui sia stato nominato uno o più Titolari autonomi del trattamento in Out-sourcing, in conformità a quanto disposto dal punto 19.7 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) saranno incaricati tramite opportuno modulo.

3.11.2. Criteri per la scelta di soggetti terzi per il trattamento di dati personali affidati all'esterno della struttura del titolare

Il Titolare, può affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare a quei soggetti terzi che abbiano i requisiti di esperienza, capacità ed affidabilità individuati all'art. 29 del Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003).

Il Titolare a cui è stato affidato il trattamento dei dati all'esterno rilascia una dichiarazione scritta da cui risulti che sono state adottate le misure idonee di sicurezza per il trattamento 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), c.d. Dichiarazione di Conformità, unitamente a rendere sempre disponibile copia del piano della sicurezza delle informazioni e/o copia del Documento programmatico sullo stato della sicurezza.

Nei casi in cui i trattamenti di dati personali vengano affidati, in conformità a quanto previsto dal Dlgs 196/2003, all'esterno della struttura del Titolare, si adottano i seguenti criteri, atti a garantire che il soggetto destinatario adotti misure di sicurezza conformi a quelle minime, previste dagli articoli da 33 a 35 Dlgs 196/2003 e dal disciplinare tecnico.

Per la generalità dei casi, in cui il trattamento di dati personali, di qualsiasi natura, venga affidato all'esterno della struttura del titolare, sono impartite istruzioni per iscritto al terzo destinatario, di rispettare quanto prescritto per il trattamento dei dati personali:

- ♦ dal Dlgs 196/2003, se il terzo destinatario è italiano
- ♦ dalla direttiva 95/46/CE, se il terzo destinatario non è italiano ma risiede in un paese comunitario

e comunque, in ogni caso, solamente in base alle finalità istituzionali dell'Ente oppure in base a specifica Autorizzazione al Trattamento da parte del Garante.

Se il trattamento concerne dati di natura sensibile, l'Ente fa riferimento alle disposizioni integrative previste dal D.Lgs. 11 maggio 1999 n. 135, pubblicato nella Gazzetta Ufficiale n. 113 del 17 maggio 1999.

Non sono previsti ambiti all'interno dei quali sia attuabile il trasferimento verso soggetti residenti in Paesi extra-Ue.

3.11.3. Nomina del responsabile del trattamento per soggetti esterni alla struttura del Titolare in Out-sourcing

Per ogni trattamento affidato ad un soggetto esterno alla struttura del titolare, il Responsabile della sicurezza dei dati personali si assicura che siano rispettate le norme di sicurezza di un livello almeno non inferiore a quanto stabilito per il trattamento interno.

Il Responsabile del trattamento in Out-sourcing accetta la nomina in forma scritta.

La nomina del Responsabile del trattamento in Out-sourcing è controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura di INFOSEC.

Il Responsabile della sicurezza dei dati personali informa il Responsabile del trattamento in Out-sourcing, dei compiti che gli sono assegnati 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).

Al momento dell'affidamento dell'incarico il Responsabile del trattamento in Out-sourcing, dichiara di accettare per iscritto almeno le seguenti prescrizioni operative:

- Di essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali sono soggetti all'applicazione del codice per la protezione dei dati personali.
- Di ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali.
- Di adottare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o di integrarle nelle procedure già in essere.
- Di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate e di allertare immediatamente il proprio committente in caso di situazioni anomale o di emergenze.
- Di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate, anche senza preavviso.

3.11.4. Nomina del titolare autonomo del trattamento in Out-sourcing

Per ogni trattamento affidato ad un soggetto esterno alla struttura del titolare, il Titolare o Responsabile dello specifico trattamento si assicura che siano rispettate le norme di sicurezza di un livello almeno non inferiore a quanto stabilito per il trattamento interno.

Il Titolare autonomo del trattamento in Out-sourcing accetta la nomina, secondo il modello di riferimento.

La nomina del Titolare autonomo del trattamento in Out-sourcing viene controfirmata per accettazione e copia della lettera di nomina accettata è conservata a cura di INFOSEC in luogo sicuro.

Il Responsabile dello specifico trattamento dei dati informa il Titolare autonomo del trattamento in Out-sourcing, dei compiti che gli sono assegnati 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), dal Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003) e da ogni altro documento adottato in materia di sicurezza delle informazioni.

Al momento dell'affidamento dell'incarico il Titolare autonomo del trattamento in Out-sourcing, dichiara di accettare per iscritto almeno le seguenti prescrizioni operative:

- Di essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali sono soggetti all'applicazione del codice per la protezione dei dati personali.
- Di ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali.
- Di adottare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o di integrarle nelle procedure già in essere.
- Di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate e di allertare immediatamente il proprio committente in caso di situazioni anomale o di emergenze.
- Di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate, anche senza preavviso

In conformità a quanto disposto dal punto 19.7 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. 196 del 30 giugno 2003) le informazioni si evincono dalle schede compilate a cura del Responsabile di uno specifico trattamento di dati personali.

3.12. Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

3.12.1. Protezione contro l'accesso abusivo

In conformità a quanto disposto dal 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) al fine di garantire la sicurezza dei dati sensibili o giudiziari contro l'accesso abusivo, il Responsabile della sicurezza dei dati personali, stabilisce, con l'eventuale supporto dell'Amministratore di Sistema e dei Responsabili di specifico trattamento dei dati personali le misure tecniche da adottare in rapporto ad eventuali rischi.

I criteri sono definiti dall'Amministratore di Sistema in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata. Sono considerate anche dati informato elettronico contenenti dati sensibili e/o giuridici quelle afferenti ai trattamenti riportati nel Regolamento sul Trattamento dei dati sensibili e giudiziari.

In particolare, per ogni Sistema interessato sono definite le seguenti specifiche:

- 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) individua idonei strumenti per la protezione degli strumenti elettronici 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.
- 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) stabilire la frequenza con cui aggiornare i programmi per elaboratore per prevenire la vulnerabilità degli strumenti elettronici e correggerne difetti.
- 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) individuare come proteggere, mediante l'utilizzo di idonei strumenti elettronici, i dati sensibili o giudiziari contro l'accesso abusivo da parte di chiunque abusivamente si introduce nel sistema informatico o telematico.

In conformità a quanto disposto dal punto 19.3 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003) le informazioni si evincono dalle schede compilate a cura del Responsabile di uno specifico trattamento di dati personali.

3.12.2. Istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili

Possono inoltre essere impartite precise istruzioni contenute in documenti di varia natura da portare a conoscenza dei Responsabili di uno specifico trattamento e degli Incaricati.

3.12.3. Riutilizzo dei supporti rimovibili

Possono inoltre essere impartite precise istruzioni contenute in documenti di varia natura da portare a conoscenza dei Responsabili di uno specifico trattamento e degli Incaricati.

3.12.4. Ripristino dell'accesso ai dati in caso di danneggiamento

Possono inoltre essere impartite precise istruzioni contenute in documenti di varia natura da portare a conoscenza dei Responsabili di uno specifico trattamento e degli Incaricati.

3.13. Trattamenti effettuati da organismi sanitari e esercenti le professioni sanitarie

3.13.1. Cifratura dei dati o separazione dei dati identificativi

NON APPLICABILE

3.13.2. Tabella dei trattamenti di dati personali idonei a rivelare lo stato di salute e la vita sessuale

NON APPLICABILE

3.14. Misure di tutela e garanzia

3.14.1. Descrizione degli interventi effettuati da soggetti esterni

Nel caso in cui ci si avvalga di soggetti esterni alla propria struttura, per provvedere al controllo del buon funzionamento infrastrutturale, hardware e/o software, degli strumenti elettronici contenenti dati, per eventuale riparazione, aggiornamento o sostituzione, nonché per trattamenti di dati completamente esternalizzati o erogati in outsourcing (da qualunque persona fisica, giuridica ovvero organizzazione), il Responsabile dello specifico trattamento dei dati competente per il controllo di tali attività (ovvero il Responsabile della sicurezza dei dati personali qualora lo preveda espressamente), deve farsi consegnare puntualmente dal personale che ha effettuato l'intervento tecnico, una dichiarazione scritta con la descrizione dettagliata delle operazioni eseguite che attesti la conformità a quanto stabilito dal Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003). Tale dichiarazione è integrata complessivamente da Dichiarazione di Conformità ai sensi del Disciplinare Tecnico previsto dall'Allegato B della normativa suddetta, e dalla messa a disposizione di copia del Piano di sicurezza delle informazioni.

4. Trattamenti senza l'ausilio di strumenti elettronici

4.1. Nomina e istruzioni agli incaricati

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.

Il Responsabile di uno specifico trattamento di dati personali deve predisporre per ogni archivio di cui è responsabile l'elenco degli Incaricati del trattamento autorizzati ad accedervi e impartire istruzioni tese a garantire un controllo costante per l'accesso agli archivi.

In base a quanto stabilito dal punto 28 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003), i documenti che contengono dati sensibili o giudiziari debbono essere custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

Oltre alle indicazioni generali contenute nel presente capitolo, possono essere impartite precise istruzioni contenute in documenti di varia natura.

4.2. Norme di sicurezza per gli incaricati del trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici

In base a quanto stabilito dal punto 27 e dal punto 28 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003), per i trattamenti di dati personali effettuati senza l'ausilio di strumenti elettronici vengono stabilite le seguenti regole che gli Incaricati del trattamento debbono osservare:

- 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.
- E' inoltre tassativamente proibito utilizzare copie fotostatiche di documenti (anche se non perfettamente riuscite) all'esterno del posto di lavoro, né tantomeno si possono utilizzare come carta per appunti.
- 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.

4.3. Copie degli atti e dei documenti

In base a 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), è fatto divieto a chiunque di:

- Effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal Responsabile di uno specifico trattamento di dati personali, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento, ed in ogni caso non strettamente riferibili alle attività lavorative ed istituzionali dell'Ente.
- Sottrarre, cancellare, distruggere senza l'autorizzazione del Responsabile di uno specifico trattamento di dati personali, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento, ed in ogni caso non strettamente riferibili alle attività lavorative ed istituzionali dell'Ente.
- Consegnare a persone non autorizzate dal Responsabile di uno specifico trattamento di dati personali, stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento, ed in ogni caso non strettamente riferibili alle attività lavorative ed istituzionali dell'Ente.

4.4. Controllo degli accessi

In base a quanto stabilito dal punto 29 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003), l'accesso agli archivi contenenti dati sensibili o giudiziari deve essere controllato dai soggetti Incaricati della custodia delle aree e dei locali ed è consentito, solo agli Incaricati del trattamento autorizzati dal Responsabile dello specifico trattamento.

Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, debbono essere identificate e registrate.

L'accesso agli archivi cartacei avviene con apposite modalità formali descritte nel Manuale di Gestione del protocollo informatico e dei flussi documentali in adozione.

5. Diritti dell'interessato

5.1. 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 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.

5.2. 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.

5.3. 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.

5.4. 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 di competenza 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.

6. Allegati

6.1. DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA (Artt. da 33 a 36 del codice)

Trattamenti con strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica

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

2. Le Credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.

3. Ad ogni incaricato sono assegnate o associate individualmente una o più Credenziali per l'autenticazione.

4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.

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

7. Le Credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

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

9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle Credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

Sistema di autorizzazione

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.

13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

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

Altre misure di sicurezza

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Documento programmatico sulla sicurezza

19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

19.1. l'elenco dei trattamenti di dati personali;

19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

19.3. l'analisi dei rischi che incombono sui dati;

19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;

19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;

19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;

19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'Interessato.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all' art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.

21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.

22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

Misure di tutela e garanzia

25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.

26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

Trattamenti senza l'ausilio di strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

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