

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.lg. 30 giugno 2003, n. 196)

Indice

Sezione I Documento programmatico sulla sicurezza	5
1 Revisione.....	5
2 Scopo	6
3 Campo di applicazione.....	7
4 Riferimenti normativi.....	8
5 Definizioni.....	9
Trattamento	9
Dato personale	9
Dati sensibili	9
Dati giudiziari	9
Titolare	9
Responsabile	9
Incaricati	9
Interessato	9
Comunicazione	10
Diffusione	10
Dato anonimo	10
Blocco	10
Banca dati	10
Comunicazione elettronica.....	10
Misure minime	10
Strumenti elettronici.....	10
Autenticazione informatica.....	10
Credenziali di autenticazione.....	11
Parola chiave	11
Profilo di autorizzazione.....	11
Sistema di autorizzazione.....	11
6 Elenco degli allegati e modelli utilizzati.....	12
Sezione II Ruoli, compiti e nomina delle figure previste per la sicurezza dei dati personali	13
1 Titolare del trattamento dei dati personali.....	13

Compiti del titolare del trattamento dei dati personali	13
2 Responsabile della sicurezza dei dati personali.....	15
Compiti del responsabile della sicurezza dei dati personali.....	15
Nomina del responsabile della sicurezza dei dati personali.....	15
3 Responsabile di specifico trattamento dei dati personali.....	17
Compiti del responsabile di uno specifico trattamento di dati personali.....	17
Nomina dei responsabili di uno specifico trattamento di dati personali.....	17
4 Incaricati della gestione e della manutenzione degli strumenti elettronici	19
Compiti degli incaricati della gestione e della manutenzione degli strumenti elettronici	19
Nomina degli incaricati della gestione e della manutenzione degli strumenti elettronici	20
5 Incaricato della custodia delle copie delle credenziali.....	21
Compiti degli incaricati della custodia delle copie delle credenziali.....	21
Nomina degli incaricati della custodia delle copie delle credenziali.....	22
6 Incaricato delle copie di sicurezza delle banche dati.....	23
Compiti degli incaricati delle copie di sicurezza delle banche dati.....	23
Nomina degli incaricati delle copie di sicurezza delle banche dati.....	24
7 Incaricato della custodia delle aree e dei locali.....	25
Compiti degli incaricati della custodia delle aree e dei locali.....	25
Nomina degli incaricati della custodia delle aree e dei locali.....	25
8 Incaricato del trattamento dei dati personali.....	26
Compiti degli incaricati del trattamento dei dati personali.....	26
Nomina degli incaricati del trattamento dei dati personali.....	27

Sezione III Trattamenti con l'ausilio di strumenti elettronici 29

1 Sistema di autenticazione informatica	29
Procedura di identificazione.....	29
Identificazione dell'incaricato.....	29
Cautele per assicurare la segretezza della componente riservata della credenziale	29
Caratteristiche della parola chiave	30
Modalità di richiesta delle credenziali di autenticazione.....	30
Istruzioni per non lasciare incustodito e accessibile lo strumento elettronico.....	31
Accesso straordinario.....	31
2 Sistema di autorizzazione.....	32

3	Altre misure di sicurezza.....	33
4	Periodicità di revisione del documento programmatico sulla sicurezza.....	34
5	Elenco dei trattamenti di dati personali.....	35
	Elenco delle sedi e degli uffici in cui vengono trattati i dati.....	35
	Elenco degli archivi dei dati oggetto del trattamento.....	35
	Elenco dei sistemi di elaborazione per il trattamento.....	35
6	Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati.....	36
	Elenco dei soggetti autorizzati al trattamento dei dati.....	36
	Verifiche periodiche delle condizioni per il mantenimento delle autorizzazioni.....	36
	Distribuzione dei compiti e delle responsabilità.....	36
7	Analisi dei rischi.....	37
	Analisi dei rischi hardware.....	37
	Analisi dei rischi sui sistemi operativi e sui software installati.....	37
	Analisi degli altri rischi nel trattamento dei dati.....	38
8	Misure da adottare per garantire l'integrità e la disponibilità dei dati.....	39
9	Misure da adottare per la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità.....	40
	Misure generali.....	40
	Procedure per controllare l'accesso ai locali in cui vengono trattati i dati.....	40
10	Formazione degli incaricati del trattamento.....	41
	Piano di formazione.....	41
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.....	42
	Trattamenti di dati personali affidati all'esterno della struttura del titolare.....	42
	Criteri per la scelta degli enti terzi per il trattamento di dati personali affidati all'esterno della struttura del titolare.....	42
	Nomina del responsabile del trattamento in Out-sourcing.....	43
	Nomina del titolare autonomo del trattamento in Out-sourcing.....	43
12	Ulteriori misure in caso di trattamento di dati sensibili o giudiziari.....	45
	Protezione contro l'accesso abusivo.....	45
	Istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili.....	45
	Riutilizzo dei supporti rimovibili.....	46
	Ripristino dell'accesso ai dati in caso di danneggiamento.....	46

13 Trattamenti effettuati da organismi sanitari e esercenti le professioni sanitarie.....	48
Cifatura dei dati o separazione dei dati identificativi.....	48
Tabella dei trattamenti di dati personali idonei a rivelare lo stato di salute e la vita sessuale.....	48
14 Misure di tutela e garanzia.....	51
Descrizione degli interventi effettuati da soggetti esterni.....	51
Relazione del bilancio d'esercizio.....	51
 Sezione IV Trattamenti senza l'ausilio di strumenti elettronici	 52
1 Nomina e istruzioni agli incaricati.....	52
2 Norme di sicurezza per gli incaricati del trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici.....	53
3 Copie degli atti e dei documenti.....	54
4 Controllo degli accessi.....	55
 Sezione V Diritti dell'interessato	 56
1 Diritto di accesso ai dati personali.....	56
2 Esercizio dei diritti.....	57
3 Modalità di esercizio.....	58
4 Riscontro all'interessato.....	59
 Sezione VI Allegati	 60
1 DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA (Artt. da 33 a 36 del codice).....	60

1 Documento programmatico sulla sicurezza

1.1 Revisione

Indice delle revisioni

Rev	Data	Descrizione	Redatto	Verificato	Approvato

1.2 Scopo

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

Inoltre costituisce un valido strumento per la adozione delle misure previste **dall'Art. 31, dall'Art. 34 e dall'Art. 35** dello stesso **Codice in materia di protezione dei dati personali (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 programmatico sulla sicurezza è quello di 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.

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

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 deve essere 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)

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.

1.6 Elenco degli allegati e modelli utilizzati

Codice	Tipo di documento	Descrizione
LI_ADS	Lettera di incarico	Incaricato gestione e manutenzione strumenti elettronici
LI_BKP	Lettera di incarico	Incaricato delle copie di sicurezza delle banche dati
LI_CDP	Lettera di incarico	Custode delle copie delle credenziali
LI_IDT	Lettera di incarico	Incaricato del trattamento dei dati personali
LI_RAL	Lettera di incarico	Incaricato della custodia delle aree e dei locali
LI_RDT	Lettera di incarico	Responsabile della sicurezza dei dati personali
LI_RST	Lettera di incarico	Responsabile di specifici trattamenti di dati personali
DTEC_W	Lettera di incarico	Responsabile del trattamento dei dati in Out-Sourcing
DTEC_W2	Lettera di incarico	Indicazione di Titolare autonomo
DTEC_A	Modello	Elenco degli archivi dei dati oggetto del trattamento
DTEC_B	Modello	Elenco delle sedi/uffici in cui vengono trattati i dati
DTEC_D	Modello	Sistemi di elaborazione per il trattamento dei dati
DTEC_E	Modello	Soggetti terzi a cui è affidato il trattamento dei dati in out-sourcing
DTEC_F	Modello	Personale autorizzato al trattamento dei dati
DTEC_G	Modello	Permessi di accesso ai dati
DTEC_H	Modello	Piano di formazione del personale autorizzato al trattamento dei dati
DTEC_J	Modello	Distribuzione dei compiti e delle responsabilità
DTEC_M	Modello	Criteri e procedure per garantire l'integrità dei dati
DTEC_N	Modello	Piano di formazione degli incaricati del back-up
DTEC_Q	Modello	Report dei virus informatici rilevati
DTEC_Q2	Modello	Report dei virus informatici rilevati da eliminare
DTEC_R	Modello	Report dei contagi da Virus Informatici
DTEC_R2	Modello	Report dei contagi da Virus Informatici Ripuliti
DTEC_S	Modello	Criteri di assegnazione delle credenziali di accesso
DTEC_T	Modello	Report annuale dei rischi hardware
DTEC_U	Modello	Report annuale dei rischi sui software installati
DTEC_Z	Modello	Report annuale altri rischi

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

2.1 Titolare del trattamento dei dati personali

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

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

I **Responsabili del trattamento** sono individuati tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

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

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

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

del trattamento dei dati personali.

- Qualora il **Titolare del trattamento** ritenga di non nominare alcun **Responsabile di specifici trattamenti**, ne assumerà tutte le responsabilità e funzioni.

2.2 Responsabile della sicurezza dei dati personali

2.2.1 Compiti del responsabile della sicurezza dei dati personali

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

Il **Responsabile della sicurezza dei dati personali** è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo a cui da parte del **Titolare del trattamento**, sono affidate le seguenti responsabilità e compiti:

- Garantire che tutte le misure di sicurezza riguardanti i dati personali siano applicate.
- Redigere ed aggiornare ad ogni variazione l'elenco delle sedi in cui vengono trattati i dati.
- Redigere ed aggiornare ad ogni variazione l'elenco degli uffici in cui vengono trattati i dati.
- Redigere ed aggiornare ad ogni variazione l'elenco delle banche dati oggetto di trattamento.
- Se il trattamento è effettuato con mezzi informatici, redigere ed aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione.
- Redigere e di aggiornare ad ogni variazione l'elenco delle sedi e degli uffici in cui viene effettuato il trattamento dei dati.
- Nominare per ciascun ufficio in cui viene effettuato il trattamento dei dati, un **incaricato** con il compito di controllare i sistemi, le apparecchiature, e se previsti, i registri di accesso ai locali allo scopo di impedire intrusioni o danneggiamenti.
- Definire e verificare 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 controllare e garantire che tutte le misure di sicurezza riguardanti i dati personali siano applicate.
- Se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più **Incaricati della gestione e della manutenzione degli strumenti elettronici**.
- Se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più **Incaricati della custodia delle copie delle credenziali** qualora vi sia più di un incaricato del trattamento.
- Se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più **Incaricati delle copie di sicurezza delle banche dati**.
- Custodire e conservare i supporti utilizzati per le copie dei dati.

Qualora il **Titolare del trattamento** ritenga di non nominare alcun **Responsabile della sicurezza dei dati personali**, ne assumerà tutte le responsabilità e funzioni.

2.2.2 Nomina del responsabile della sicurezza dei dati personali

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

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

Il **Titolare del trattamento** deve informare ciascun **Responsabile della sicurezza dei dati personali** delle responsabilità che gli sono affidate in conformità a quanto disposto dalle normative in

vigore, ed in particolare di quanto stabilito dal **Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003)** e del **Disciplinare tecnico in materia di misure minime di sicurezza (allegato B al Dlgs. n.196 del 30 giugno 2003)**.

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

La nomina del **Responsabile della sicurezza dei dati personali** è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.

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

2.3 Responsabile di specifico trattamento dei dati personali

2.3.1 Compiti del responsabile di uno specifico trattamento di dati personali

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

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

I **Responsabili di uno specifico trattamento di dati personali** sono individuati tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

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

- Nominare gli **Incaricati del trattamento dei dati personali** limitatamente alle **Banche di dati** di cui sono responsabili.
- Sorvegliare che il trattamento sia effettuato nei termini e nei modi stabiliti dal **Codice in materia di protezione dei dati personali (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**.

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

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** deve essere effettuata dal **Titolare del trattamento** con una lettera di incarico in cui sono specificate le responsabilità che gli sono affidate e deve essere controfirmata dall'interessato per accettazione.

Nella lettera di nomina debbono essere indicate le **Banche dati** di cui è responsabile per quanto attiene alla sicurezza e a quanto stabilito dal **Codice in materia di protezione dei dati personali (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 (LI_RST) accettata deve essere conservata a cura del **Titolare del trattamento** in luogo sicuro.

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

minime di sicurezza (Allegato B al Dlgs. n.196 del 30 giugno 2003).

Il **Titolare del trattamento** deve consegnare 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.

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

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

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

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 della sicurezza dei dati personali**, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più **Incaricati della gestione e della manutenzione degli strumenti elettronici**.

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

E' onere del **Responsabile della sicurezza dei dati personali**, in relazione all'attività svolta, individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più **Incaricati della gestione e della manutenzione degli strumenti elettronici**.

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

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

Qualora il **Responsabile della sicurezza dei dati personali** ritenga di non nominare alcun **Incaricato della gestione e della manutenzione degli strumenti elettronici**, ne assumerà tutte le responsabilità e funzioni.

2.4.2 Nomina degli incaricati della gestione e della manutenzione degli strumenti elettronici

Il **Responsabile della sicurezza dei dati personali** nomina uno o più soggetti **Incaricati della gestione e della manutenzione degli strumenti elettronici** a cui è conferito il compito di sovrintendere al buon funzionamento delle risorse del sistema informativo e degli accessi alle **Banche di dati**.

Anche se non espressamente previsto dalla norma, è opportuno che il **Responsabile della sicurezza dei dati personali** nomini uno o più **Incaricati della gestione e della manutenzione degli strumenti elettronici**, specificando gli elaboratori o le banche dati che è chiamato a sovrintendere.

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

La nomina di uno o più **Incaricati della gestione e della manutenzione degli strumenti elettronici** deve essere effettuata con una lettera di incarico (LI_ADS) e deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del **Responsabile della sicurezza dei dati personali** in luogo sicuro.

Il **Responsabile della sicurezza dei dati personali** deve consegnare a ciascun **Incaricato della gestione e della manutenzione degli strumenti elettronici** una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

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

La nomina degli **Incaricati della gestione e della manutenzione degli strumenti elettronici** può essere revocata in qualsiasi momento dal **Responsabile della sicurezza dei dati personali** senza preavviso, ed eventualmente affidata ad altro soggetto.

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)** debbono essere impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il **Titolare del trattamento** può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema.

E' onere del **Titolare del trattamento** o, se designato, del **Responsabile della sicurezza dei dati personali**, in relazione all'attività svolta, individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più **Incaricati della custodia delle copie delle credenziali**.

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

- Autorizzare l'assegnazione e la gestione delle **Credenziali di autenticazione** per l'accesso ai dati personali degli **Incaricati del trattamento**, su richiesta del **Responsabile dello specifico trattamento**, avvalendosi del supporto tecnico dell'**incaricato della gestione e della manutenzione degli strumenti elettronici**, in conformità a quanto disposto dal **punto 3 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n.196 del 30 giugno 2003)**.
- Istruire gli incaricati del trattamento sull'uso delle **componenti riservata delle credenziali di autenticazione**, e sulle caratteristiche che 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 di sicurezza del sistema, l'**Incaricato della custodia delle copie delle credenziali**, in accordo con il **Responsabile dello specifico trattamento di dati personali** può assicurare la disponibilità di dati o strumenti elettronici operando secondo le seguenti istruzioni:

1. Utilizzando i diritti di "amministratore di sistema", può modificare in modo forzoso la **componente riservata delle credenziali di autenticazione** dell'**Incaricato del trattamento dei dati personali** assente o impedito ad effettuare il trattamento.

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

Qualora il **Responsabile della sicurezza dei dati personali** ritenga di non nominare alcun **Incaricato della custodia delle copie delle credenziali**, ne assumerà tutte le responsabilità e funzioni.

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 della sicurezza dei dati personali** nomina uno o più soggetti **Incaricati della custodia delle copie delle credenziali** a cui è conferito il compito di autorizzare l'assegnazione e la gestione delle **Credenziali di autenticazione** per l'accesso ai dati gestiti con strumenti elettronici.

La nomina di uno o più **Incaricati della custodia delle copie delle credenziali** deve essere effettuata con una lettera di incarico (LI_CDP), deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del **Responsabile della sicurezza dei dati personali** in luogo sicuro.

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

Il **Responsabile della sicurezza dei dati personali** deve consegnare a ciascun **Incaricato della custodia delle copie delle credenziali**, una copia di tutte le norme che riguardano la Sicurezza del trattamento dei dati in vigore al momento della nomina.

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

La nomina di uno o più **Incaricati della custodia delle copie delle credenziali** può essere revocata in qualsiasi momento dal **Responsabile della sicurezza dei dati personali** senza preavviso, ed essere affidata ad altro soggetto.

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 della sicurezza dei dati personali**, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più **Incaricati delle copie di sicurezza delle banche dati**.

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

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, il **Responsabile della sicurezza dei dati personali** stabilisce, con il supporto tecnico 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 debbono 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.

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

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

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

- Prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di sicurezza secondo i criteri stabiliti dal **Responsabile della sicurezza dei dati personali**.
- Assicurarli della qualità delle copie di sicurezza dei dati e della loro conservazione in luogo adatto e sicuro.
- Assicurarli 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 il **Responsabile della sicurezza dei dati personali** ritenga di non nominare alcun **Incaricato delle copie di sicurezza delle banche dati**, ne assumerà tutte le responsabilità e funzioni.

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 della sicurezza dei dati personali**, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più **Incaricati delle copie di sicurezza delle banche dati** a cui è conferito il compito di effettuare periodicamente le copie di sicurezza delle Banche di dati gestite specificando gli elaboratori o le banche dati che è chiamato a sovrintendere.

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

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

Copia della lettera di nomina accettata deve essere conservata a cura del **Responsabile della sicurezza dei dati personali** in luogo sicuro.

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

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 della sicurezza dei dati personali**, 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 **Responsabile della sicurezza dei dati personali** nel caso in cui si siano riscontrate situazioni anomale.
- Controllare la chiusura dei locali al termine dell'orario.

Qualora il **Responsabile della sicurezza dei dati personali** ritenga di non nominare alcun **Incaricato della custodia delle aree e dei locali**, 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 **Responsabile della sicurezza dei dati personali**, 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 della sicurezza dei dati personali** 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 (LI_RAL) e deve essere controfirmata.

Copia della lettera di nomina accettata deve essere conservata a cura del **Responsabile della sicurezza dei dati personali** in luogo sicuro.

La nomina dell'**Incaricato della custodia delle aree e dei locali** può essere revocata in qualsiasi momento dal **Responsabile della sicurezza dei dati personali** 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** che operano sotto la diretta autorità del **Titolare del trattamento** o, se designato, del **Responsabile di uno specifico trattamento di dati personali**, attenendosi alle istruzioni impartite.

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

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

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

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

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

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

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

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

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

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

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

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)** nel caso in cui il trattamento di dati personali è effettuato con strumenti elettronici, il **Responsabile della sicurezza dei dati personali** deve assicurarsi 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.

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** deve assicurare che il trattamento di dati personali, effettuato con strumenti elettronici, sia consentito solamente agli **Incaricati del trattamento** dotati di una o più **Credenziali di autenticazione** tra le seguenti:

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

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 debbono 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** deve essere 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) deve rispettare i seguenti criteri:

- Non deve contenere nomi comuni
- Non deve contenere nomi di persona
- Deve contenere sia lettere che numeri
- Deve comprendere almeno 3 caratteri alfabetici
- Deve comprendere almeno 2 caratteri numerici
- Deve essere diversa dallo User-Id
- Deve essere lunga 8 caratteri o massimo consentito dal sistema di autenticazione
- Non deve essere riconducibile all'incaricato

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 deve essere inoltrata al **Responsabile della gestione e della manutenzione degli strumenti elettronici** in forma scritta utilizzando una copia del modulo DTEC_s.

Il **Responsabile della gestione e della manutenzione degli strumenti elettronici** provvederà:

- A comunicare all'**Incaricato del trattamento dei dati personali** 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) provvisoria
- 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** deve informare i propri **Incaricati del trattamento** dei criteri e delle regole che debbono 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 deve fare firmare ad ogni **Incaricato del trattamento** per presa visione una copia del modulo DTEC_s in cui sono specificati i criteri che debbono essere rispettati per la **Componente riservata delle credenziali di autenticazione** (parola chiave o password), che deve essere allegata al presente Documento Programmatico sulla Sicurezza.

Al primo accesso l'**Incaricato del trattamento** dovrà modificare la **Componente riservata delle credenziali di autenticazione** (parola chiave o password) rispettando le regole definite nella lettera di assegnazione delle **Credenziali di autenticazione**.

È compito del **Responsabile della sicurezza dei dati personali** approntare 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 saranno registrati e dovrà essere data tempestiva comunicazione al **Titolare del trattamento**.

In caso di smarrimento della **Componente riservata delle credenziali di autenticazione** (parola chiave o password) il **Responsabile dello specifico trattamento** dell'incaricato dovrà richiedere al **Responsabile della gestione e della manutenzione degli strumenti elettronici** una nuova assegnazione.

Il **Responsabile della gestione e della manutenzione degli strumenti elettronici** provvederà ad annullare la **Componente riservata delle credenziali di autenticazione** (parola chiave o password) precedente e ad assegnarne una nuova provvisoria.

Le **Credenziali di autenticazione** che non sono utilizzate per più di 6 mesi dovranno essere disabilitate d'autorità dal **Responsabile della gestione e della manutenzione degli strumenti elettronici**.

I **Responsabili di uno specifico trattamento** devono dare informazione al **Responsabile della sicurezza dei dati personali** 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.

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.

La custodia delle copie delle **Credenziali di autorizzazione** è organizzata garantendo la relativa segretezza.

Gli **Incaricati della custodia delle copie delle credenziali** devono informare tempestivamente l'**Incaricato del trattamento** ogni qualvolta sia stato effettuato un tale tipo di intervento.

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

Il **Responsabile di uno specifico trattamento di dati personali** ha il compito di individuare 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** può essere differenziato.

In particolare il **Responsabile di uno specifico trattamento di dati personali** può decidere quali operazioni di trattamento siano 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** deve aggiornare l'**Elenco dei permessi di accesso** che sono stati assegnati agli **Incaricati del trattamento** per ogni tipologia di banca di dati utilizzando il modulo DTEC_g.

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 modulo DTEC_g, deve essere allegato al presente Documento Programmatico sulla Sicurezza.

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)**, è fatto divieto a chiunque di:

- Effettuare copie su supporti magnetici o trasmissioni non autorizzate dal **Responsabile della sicurezza dei dati personali** di dati oggetto del trattamento.
- Effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal **Responsabile della sicurezza dei dati personali**, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.
- Sottrarre, cancellare, distruggere senza l'autorizzazione del **Responsabile della sicurezza dei dati personali**, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.
- Consegnare a persone non autorizzate dal **Responsabile della sicurezza dei 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 deve verificare ed aggiornare 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)** per redigere l' Elenco delle sedi in cui vengono trattati i dati deve essere utilizzato il modulo DTEC_b, che deve essere allegato al presente Documento Programmatico sulla Sicurezza, e deve essere aggiornato e conservato in luogo sicuro a cura del **Responsabile della sicurezza dei dati personali**.

3.5.2 Elenco degli archivi dei dati oggetto del trattamento

Al **Responsabile della sicurezza dei 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)** per l'individuazione degli archivi dei dati oggetto del trattamento deve essere utilizzato il modulo DTEC_a, che deve essere allegato al presente Documento Programmatico sulla Sicurezza.

3.5.3 Elenco dei sistemi di elaborazione per il trattamento

Al **Responsabile della sicurezza dei dati personali** 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)** per ogni sistema deve essere utilizzato il modulo DTEC_d, che deve essere allegato al presente Documento Programmatico sulla Sicurezza, e deve essere conservato a cura del **Responsabile della sicurezza dei dati personali** in luogo sicuro e deve essere trasmesso in copia controllata all'**Incaricato della gestione e della manutenzione degli strumenti elettronici** di competenza.

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** limitatamente alle **Banche di dati** di cui sono responsabili
- Assegnare le **Credenziali di autenticazione**
- Informare il **Responsabile della sicurezza dei dati personali** delle variazioni intervenute nell'assegnazione delle **Credenziali di autorizzazione**.

Il **Responsabile della sicurezza dei dati personali** deve tenere aggiornato ad ogni variazione l'**Elenco del personale autorizzato al trattamento dei dati**.

L'**Elenco del personale autorizzato al trattamento dei dati** deve essere redatto dal **Responsabile della sicurezza dei dati personali**, utilizzando il modulo DTEC_f., che deve essere allegato al presente Documento Programmatico sulla Sicurezza, e deve essere conservato a cura del **Responsabile della sicurezza dei dati personali**, in luogo sicuro.

Una copia dell'**Elenco del personale autorizzato al trattamento dei dati** deve essere consegnata all'**Incaricato della custodia delle copie delle credenziali**.

3.6.2 Verifiche periodiche delle condizioni per il mantenimento delle autorizzazioni

Il **Responsabile della sicurezza dei dati personali** eventualmente in collaborazione con i **Responsabili degli specifici trattamenti di dati personali** ha il compito di verificare ogni anno, entro il **31 marzo**, le **Credenziali di autenticazione**.

Il **Responsabile della sicurezza dei dati personali** deve tenere aggiornato ad ogni variazione l'**Elenco del personale autorizzato al trattamento dei dati**.

L'**Elenco del personale autorizzato al trattamento dei dati** deve essere redatto dal **Responsabile della sicurezza dei dati personali**, utilizzando il modulo DTEC_f., che deve essere allegato al presente Documento Programmatico sulla Sicurezza, e deve essere conservato a cura del **Responsabile della sicurezza dei dati personali**, in luogo sicuro.

Una copia dell'**Elenco del personale autorizzato al trattamento dei dati** deve essere consegnata all'**Incaricato della custodia delle copie delle credenziali**.

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 **Titolare del trattamento** una volta stabilita la struttura di riferimento, i compiti e le relative responsabilità, in relazione ai trattamenti effettuati, deve predisporre il modulo DTEC_J, che deve essere allegato al presente Documento Programmatico sulla Sicurezza.

3.7 Analisi dei rischi

3.7.1 Analisi dei rischi hardware

Il **Responsabile della sicurezza dei dati personali** in collaborazione con gli **Incaricati della gestione e della manutenzione degli strumenti elettronici**, anche avvalendosi di consulenti interni o esterni, 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

Gli **Incaricati della gestione e della manutenzione degli strumenti elettronici** debbono aggiornare il **Report annuale dei rischi hardware** conformemente al modulo DTEC_t.

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)** il modulo DTEC_t, deve essere allegato al presente Documento Programmatico sulla Sicurezza.

Gli **Incaricati della gestione e della manutenzione degli strumenti elettronici** nel caso in cui esistano rischi evidenti debbono informare tempestivamente il **Responsabile della sicurezza 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** in collaborazione con gli **Incaricati della gestione e della manutenzione degli strumenti elettronici**, 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.

Il **Responsabile della sicurezza dei dati personali** in collaborazione con gli **Incaricati della gestione e della manutenzione degli strumenti elettronici**, deve aggiornare il **Report annuale dei rischi sui software installati** conformemente al modulo DTEC_u.

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)** il modulo DTEC_u, deve essere allegato al presente Documento Programmatico sulla Sicurezza.

Gli **Incaricati della gestione e della manutenzione degli strumenti elettronici**, nel caso in cui esistano rischi evidenti, debbono informare tempestivamente il **Responsabile della sicurezza dei dati personali** 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

Al **Responsabile della sicurezza dei dati personali** 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

Il **Responsabile della sicurezza dei dati personali** deve aggiornare il **Report annuale degli altri rischi** conformemente al modulo DTEC_z.

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)** il modulo DTEC_z, deve essere allegato al presente Documento Programmatico sulla Sicurezza.

I **Responsabili degli specifici trattamenti di dati personali**, nel caso in cui esistano rischi evidenti, debbono informare tempestivamente il **Responsabile della sicurezza dei dati personali** 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

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

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

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

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

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

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

- Una copia del "**Documento con le istruzioni di copia**" deve essere conservata a cura del **Responsabile della sicurezza dei dati personali** in luogo sicuro.
- Una copia del "**Documento con le istruzioni di copia**" deve essere consegnata a ciascun **Incaricato delle copie di sicurezza delle banche dati**.

Al **Responsabile della sicurezza dei dati personali**, in collaborazione con gli **Incaricati della gestione e della manutenzione degli strumenti elettronici**, e con gli **Incaricati delle copie di sicurezza delle banche dati** è affidato il compito di verificare ogni anno, **entro il 31 marzo**, le necessità di formazione del personale incaricato di effettuare periodicamente le Copie di sicurezza delle banca di dati trattate, in funzione anche di eventuali opportunità offerte dall'evoluzione tecnologica, utilizzando il modulo DTEC_n.

In conformità a quanto disposto dal **punto 19.6 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003)** il modulo DTEC_n, deve essere allegato al presente Documento Programmatico sulla Sicurezza.

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:

- Effettuare copie su supporti magnetici o trasmissioni non autorizzate dal **Responsabile della sicurezza dei dati personali** o dal **Responsabile dello specifico trattamento di dati personali** oggetto del trattamento.
- Effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal **Responsabile della sicurezza dei dati personali** o dal **Responsabile dello specifico trattamento di dati personali**, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.
- Sottrarre, cancellare, distruggere senza l'autorizzazione del **Responsabile della sicurezza dei dati personali** o dal **Responsabile dello specifico trattamento di dati personali**, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.
- Consegnare a persone non autorizzate dal **Responsabile della sicurezza dei dati personali** o dal **Responsabile dello specifico trattamento di dati personali**, stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

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

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)** al **Responsabile della sicurezza dei dati personali** è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco degli uffici in cui viene effettuato il trattamento dei dati, e di nominare per ciascun ufficio un **Incaricato della custodia delle aree e dei locali** con il compito di controllare direttamente i sistemi, le apparecchiature, o i registri di accesso ai locali allo scopo di impedire intrusioni o danneggiamenti.

Il **Responsabile della sicurezza dei dati personali** deve definire le modalità di accesso agli uffici in cui sono presenti sistemi o apparecchiature di accesso ai dati trattati.

Il **Responsabile della sicurezza dei dati personali** deve incaricare per iscritto con una lettera di nomina ogni incaricato del controllo di accesso ai locali dei compiti che gli sono stati affidati utilizzando il modello L_RAL.

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)** i moduli L_RAL, debbono essere allegati al presente Documento Programmatico sulla Sicurezza.

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)** il **Responsabile della sicurezza dei dati personali**, 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.

Il **Responsabile della sicurezza dei dati personali**, in collaborazione con i **Responsabili degli specifici trattamenti di dati personali**, deve redigere ogni anno, **entro il 31 marzo**, il **Piano di Formazione del personale** utilizzando il modulo DTEC_h, specificando le necessità di ulteriore formazione del personale.

Il Piano di formazione del personale deve essere 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)** il modulo DTEC_h, deve essere allegato al presente Documento Programmatico sulla Sicurezza.

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 **Responsabile della sicurezza dei dati personali**, può decidere di affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare.

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

- I soggetti interessati
- I luoghi dove fisicamente avviene il trattamento dei dati stessi
- I responsabili del trattamento di dati personali

Per l'inventario dei soggetti a cui affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare, deve essere utilizzato il modulo DTEC_e, che deve essere allegato al presente Documento Programmatico sulla Sicurezza, e deve essere conservato a cura del **Responsabile della sicurezza dei dati personali**, in luogo sicuro.

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), è possibile indicare gli stessi **Responsabili del trattamento in Out-sourcing**, mediante il modello DTEC_w.

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)** il modulo DTEC_w, deve essere allegato al presente Documento Programmatico sulla Sicurezza.

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), è possibile indicare i **Titolari autonomi del trattamento in Out-sourcing**, mediante il modello DTEC_w2, 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)**, devono intendersi 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)** il modulo DTEC_w2, deve essere allegato al presente Documento Programmatico sulla Sicurezza.

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

Il **Responsabile della sicurezza dei dati personali**, 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 deve rilasciare 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).

3.11.3 Nomina del responsabile del trattamento in Out-sourcing

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

Il **Responsabile del trattamento in Out-sourcing** deve accettare la nomina, secondo il modello DTEC_w.

La nomina del **Responsabile del trattamento in Out-sourcing** deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del **Responsabile della sicurezza dei dati personali** in luogo sicuro.

Il **Responsabile della sicurezza dei dati personali** deve informare 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**, deve dichiarare per iscritto:

- *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.*

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) il modulo DTEC_w, deve essere allegato al presente Documento Programmatico sulla Sicurezza.

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 **Responsabile della sicurezza dei dati personali** deve assicurarsi che siano rispettate le norme di sicurezza di un livello non inferiore a quanto stabilito per il trattamento interno.

Il **Titolare autonomo del trattamento in Out-sourcing** deve accettare la nomina, secondo il modello DTEC_w2.

La nomina del **Titolare autonomo del trattamento in Out-sourcing** deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del **Responsabile della sicurezza dei dati personali** in luogo sicuro.

Il **Responsabile della sicurezza dei dati personali** deve informare 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)** 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 **Titolare autonomo del trattamento in Out-sourcing** , deve dichiarare per iscritto:

- *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.*

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) il modulo DTEC_w2, deve essere allegato al presente Documento Programmatico sulla Sicurezza.

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**, deve stabilire, con il supporto tecnico degli **Incaricati della gestione e della manutenzione degli strumenti elettronici**, le misure tecniche da adottare in rapporto ad eventuali rischi.

I criteri debbono essere definiti dal **Responsabile della sicurezza dei dati personali** in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

In particolare per ogni Sistema interessato debbono essere 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)** individuare gli 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.

Per ogni sistema deve essere utilizzato il modulo DTEC_d, e deve essere conservato a cura del **Responsabile della sicurezza dei dati personali** in luogo sicuro e deve essere trasmesso in copia controllata all'**Incaricato della gestione e della manutenzione degli strumenti elettronici** di competenza.

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)** il modulo DTEC_d, deve essere allegato al presente Documento Programmatico sulla Sicurezza.

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

In conformità a quanto disposto dal **punto 21 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003)** per ogni **supporto utilizzato per le operazioni di copia** deve essere individuato il luogo di conservazione in modo che sia convenientemente protetto dai potenziali rischi di:

- Agenti chimici
- Fonti di calore
- Campi magnetici

- Intrusioni e atti vandalici
- Incendio
- Allagamento
- Furto
- Accesso non autorizzato
- Trattamento non consentito

L'accesso ai supporti utilizzati per le copie dei dati è limitato per ogni banca di dati a:

- **Incaricati delle copie di sicurezza delle banche dati**
- **Responsabile della sicurezza dei dati personali**

Il **Responsabile della sicurezza dei dati personali** è responsabile della custodia e della conservazione dei supporti utilizzati per le copie dei dati e deve indicare, utilizzando il modulo DTEC_m, il luogo di conservazione dei supporti utilizzati per le copie dei dati.

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)** i moduli DTEC_m, debbono essere allegati al presente Documento Programmatico sulla Sicurezza.

3.12.3 Riutilizzo dei supporti rimovibili

In conformità a quanto disposto dal **punto 22 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003)** se il **Responsabile della sicurezza dei dati personali** decide che i supporti magnetici contenenti dati sensibili o giudiziari non siano più utilizzabili per gli scopi per i quali erano stati destinati, deve provvedere a farne cancellare il contenuto annullando e rendendo intelligibili e tecnicamente in alcun modo ricostruibili le informazioni in esso contenute.

E' compito del **Responsabile della sicurezza dei dati personali** controllare e assicurarsi che in nessun caso vengano lasciate copie di **Banche di dati** contenenti dati sensibili o giudiziari, non più utilizzate, senza che ne venga cancellato il contenuto ed annullate e rese intelligibili e tecnicamente in alcun modo ricostruibili le informazioni in esso registrate.

3.12.4 Ripristino dell'accesso ai dati in caso di danneggiamento

In conformità a quanto disposto dal **punto 23 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003)** la decisione di ripristinare la disponibilità dei dati in seguito a distruzione o danneggiamento è compito esclusivo del **Responsabile della sicurezza dei dati personali**.

La decisione di ripristinare la disponibilità dei dati deve essere presa rapidamente e in ogni caso la disponibilità dei dati deve essere ripristinata al massimo entro 7 (sette) giorni.

Una volta valutata la assoluta necessità di ripristinare la disponibilità dei dati in seguito a distruzione o danneggiamento il **Responsabile della sicurezza dei dati personali** deve provvedere col la collaborazione dell'**Incaricato delle copie di sicurezza delle banche dati** e dell'**Incaricato della gestione e della manutenzione degli strumenti elettronici** all'operazione di ripristino dei dati.

La decisione di ripristinare la funzionalità degli elaboratori elettronici guasti, è compito esclusivo del **Responsabile della sicurezza dei dati personali** che si può avvalere del parere dell'**Incaricato della gestione e della manutenzione degli strumenti elettronici**.

La decisione di ripristinare la funzionalità degli elaboratori elettronici guasti deve essere presa

rapidamente e in ogni caso la funzionalità deve essere ripristinata al massimo entro 7 (sette) giorni.

3.13 Trattamenti effettuati da organismi sanitari e esercenti le professioni sanitarie

3.13.1 Cifratura dei dati o separazione dei dati identificativi

(Questa parte del Documento programmatico sulla sicurezza riguarda solamente gli Organismi sanitari e gli esercenti professioni sanitarie)

Il Responsabile della sicurezza dei dati personali per i trattamenti di dati personali idonei a rivelare lo stato di salute e la vita sessuale elencati ha stabilito di adottare le seguenti misure di sicurezza come specificato nella tabella che segue in conformità a quanto disposto dal **punto 19.8 del Disciplinare tecnico in materia di misure minime di sicurezza (Allegato B del Dlgs. n.196 del 30 giugno 2003)**.

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

(Questa parte del Documento programmatico sulla sicurezza riguarda solamente gli Organismi sanitari e gli esercenti professioni sanitarie)

Descrizione del tipo di trattamento	Tipo di protezione	Tecniche adottate
	<input type="checkbox"/> CF <input type="checkbox"/> SP	<input type="checkbox"/> A <input type="checkbox"/> B <input type="checkbox"/> C <input type="checkbox"/> D
	<input type="checkbox"/> CF <input type="checkbox"/> SP	<input type="checkbox"/> A <input type="checkbox"/> B <input type="checkbox"/> C <input type="checkbox"/> D
	<input type="checkbox"/> CF <input type="checkbox"/> SP	<input type="checkbox"/> A <input type="checkbox"/> B <input type="checkbox"/> C <input type="checkbox"/> D
	<input type="checkbox"/> CF <input type="checkbox"/> SP	<input type="checkbox"/> A <input type="checkbox"/> B <input type="checkbox"/> C <input type="checkbox"/> D
	<input type="checkbox"/> CF <input type="checkbox"/> SP	<input type="checkbox"/> A <input type="checkbox"/> B <input type="checkbox"/> C <input type="checkbox"/> D
	<input type="checkbox"/> CF <input type="checkbox"/> SP	<input type="checkbox"/> A <input type="checkbox"/> B <input type="checkbox"/> C <input type="checkbox"/> D
	<input type="checkbox"/> CF <input type="checkbox"/> SP	<input type="checkbox"/> A <input type="checkbox"/> B <input type="checkbox"/> C <input type="checkbox"/> D
	<input type="checkbox"/> CF <input type="checkbox"/> SP	<input type="checkbox"/> A <input type="checkbox"/> B <input type="checkbox"/> C <input type="checkbox"/> D
	<input type="checkbox"/> CF <input type="checkbox"/> SP	<input type="checkbox"/> A <input type="checkbox"/> B <input type="checkbox"/> C <input type="checkbox"/> D
	<input type="checkbox"/> CF <input type="checkbox"/> SP	<input type="checkbox"/> A <input type="checkbox"/> B <input type="checkbox"/> C <input type="checkbox"/> D
	<input type="checkbox"/> CF <input type="checkbox"/> SP	<input type="checkbox"/> A <input type="checkbox"/> B <input type="checkbox"/> C <input type="checkbox"/> D
	<input type="checkbox"/> CF <input type="checkbox"/> SP	<input type="checkbox"/> A <input type="checkbox"/> B <input type="checkbox"/> C <input type="checkbox"/> D
	<input type="checkbox"/> CF <input type="checkbox"/> SP	<input type="checkbox"/> A <input type="checkbox"/> B <input type="checkbox"/> C <input type="checkbox"/> D
	<input type="checkbox"/> CF <input type="checkbox"/> SP	<input type="checkbox"/> A <input type="checkbox"/> B <input type="checkbox"/> C <input type="checkbox"/> D
	<input type="checkbox"/> CF <input type="checkbox"/> SP	<input type="checkbox"/> A <input type="checkbox"/> B <input type="checkbox"/> C <input type="checkbox"/> D

Legenda del tipo di protezione adottato:

- CF** Cifratura. Tutti i servizi tramite Internet il sistema di sicurezza sono basati su un protocollo TCP/IP con crittografia Secure Socket Layer (SSL) a 128 bit strong encryption emesso da Verisign Certification Authority per dare la massima garanzia che le informazioni che transitano sulla rete siano visibili unicamente dall'utente interessato. L'utilizzo di una chiave di cifratura a 128 bit garantisce il massimo livello di sicurezza a protezione del mutuo scambio di informazioni con l'utente interessato. Il tempo necessario per decodificare tale chiave è infatti virtualmente infinito (circa $3 \cdot 10^{30}$ possibili combinazioni).
- SP** Separazione architetturale tra le macchine contenenti i dati personali idonei a rivelare lo stato di salute e la vita sessuale e i server collegati ad Internet

Legenda delle tecniche di sicurezza adottate:

- A** E' garantita in ogni momento l'impossibilità dell'accesso non autorizzato all'infrastruttura ed ai supporti di dati.
- B** E' escluso l'accesso di persone non autorizzate a dati personali utilizzando un sistema di controllo delle credenziali di autenticazione.
- C** Le informazioni, trasmesse sono cifrate e che la cifratura rispetta un livello tecnico adeguato all'attuale stato dell'arte.
- D** L'identificazione dell'utente interessato che ha il diritto di ricevere i dati è garantita in modo univoco.

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 hardware e/o software degli strumenti elettronici e alla eventuale riparazione, aggiornamento o sostituzione, il **Responsabile della sicurezza dei dati personali**, 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)**.

3.14.2 Relazione del bilancio d'esercizio

Nel caso in cui è previsto che debba essere redatta la **Relazione accompagnatoria al Bilancio d'esercizio il Titolare del trattamento** deve riferire della avvenuta redazione o dell'avvenuto aggiornamento del Documento programmatico sulla sicurezza nei termini previsti e ne attesti la conformità 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)**.

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.

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 della sicurezza dei dati personali**, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.
- Sottrarre, cancellare, distruggere senza l'autorizzazione del **Responsabile della sicurezza dei dati personali**, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.
- Consegnare a persone non autorizzate dal **Responsabile della sicurezza dei dati personali**, stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

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.

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 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.