Genova Palazzo Ducale Fondazione per la Cultura

# Manuale della Privacy

Redatto ai sensi del DLgs 196/2003 e del relativo disciplinare tecnico

Data: 30/03/2012

Versione: 5 - Revisione: 0

Genova Palazzo Ducale Fondazione per la Cultura
Piazza Matteotti 9
16123 Genova, Ge
Partita IVA: 03137910109
Telefono: 0105574000
Fax: 0105574001
Email: palazzoducale@palazzoducale.genova.it
Website: www.palazzoducale.genova.it

6 agosto 2013

# Dati generali

Manuale della Privacy e Documento Programmatico sulla Sicurezza redatti da:

**Denominazione/Ragione sociale** Genova Palazzo Ducale Fondazione per la Cultura
**Tipologia** Soggetto privato - Fondazione
**Partita IVA** 03137910109
**Codice Fiscale** 03288320157

Indirizzo Piazza Matteotti 9 Comune 16123 Genova, Ge
Recapiti telefonici 0105574000
Fax 0105574001

Indirizzo Sito Web www.palazzoducale.genova.it
Indirizzo Email palazzoducale@palazzoducale.genova.it

Tipologia titolare dei trattamenti Persona giuridica
Titolare dei trattamenti Genova Palazzo Ducale Fondazione per la Cultura

# Manuale della Privacy
# SOMMARIO

## Capitolo 4. DOCUMENTO PROGRAMMATICO SULLA SICUREZZA



## Capitolo 5. DIRITTI DELL'INTERESSATO

## Appendice. DISCIPLINARE TECNICO

## ALLEGATI

Lettere di nomina

Responsabili dei trattamenti di dati personali Incaricati dei
Trattamenti di dati personali Responsabili dei trattamenti esterni
Amministratori di sistema
Custodi delle credenziali

Responsabili della manutenzione degli strumenti elettronici Responsabili della
custodia delle aree e dei locali Responsabili backup e prove di ripristino
Richiesta impresa pulizie

Documento Programmatico sulla Sicurezza (DPS) Elenco dei trattamenti dei dati personali (Regola 19.1)

Distribuzione dei compiti e delle responsabilità (Regola 19.2) Analisi dei rischi che
incombono sui dati(Regola 19.3) Misure in essere e da adottare (regola 19.4)
Criteri e modalità di ripristino della disponibilità dei dati (regola 19.5) Pianificazione degli
interventi formativi previsti (regola 19.6) Trattamenti affidati all'esterno (Regola 19.7)
Cifratura dei dati o separazione dei dati identificativi (regola 19.8)

Diritti dell'interessato

Procedura per la gestione delle richieste degli interessati Modello per l'esercizio
dei diritti da parte dell'interessato Modello per informativa agli interessati
Modello per la richiesta del consenso al trattamento

Atri modelli

Richiesta azioni correttive

Registro carico/scarico documentazione sensibile

# Capitolo 1. PRESENTAZIONE DEL MANUALE

## 1.1. Oggetto e finalità

Il Manuale descrive e definisce le responsabilità e le istruzioni impartite ai soggetti preposti al Trattamento (responsabili e incaricati del trattamento).

Il Manuale si occupa di definire le azioni per la gestione dei rischi e per l'adozione delle misure di sicurezza. Definisce, inoltre, gli adempimenti necessari, sia a rilevanza interna che esterna, e individua le procedure per la tutela della riservatezza dei dati personali.

Vengono definiti i criteri e le modalità operative adottate dall'Azienda per l'adozione del documento programmatico sulla sicurezza. In particolare vengono individuati, descritti e valutati i rischi e le conseguenti misure di sicurezza adeguate alla protezione della sicurezza delle aree, dei dati e delle trasmissioni, al fine di ridurre al minimo i rischi stessi.

## 1.2. Definizioni

Si ritiene utile riportare, per favorire una migliore comprensione del manuale, le principali definizioni di ordine generale previste dal DLgs 196/2003.

- trattamento: qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;
- dato personale: qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- dati identificativi: i dati personali che permettono l'identificazione diretta dell'interessato;
- dati sensibili: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
- dati giudiziari: i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;
- titolare: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
- responsabile: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati

personali;

- amministratore di sistema: la persona fisica in grado di conoscere tutte le informazioni dell'azienda custodite negli elaboratori elettronici o da essi trasmessi, in grado di vagliare il traffico di informazioni da e verso la Rete (e-mail, navigazione in Internet, attachment inviati e ricevuti, software scaricati, ect.);
- custode delle credenziali: la persona fisica cui è conferito l'incarico di custodire le credenziali di autenticazione per l'accesso ai computer da parte degli incaricati;
- incaricati: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- interessato: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
- comunicazione: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- diffusione: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- dato anonimo: il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
- blocco: la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
- banca di dati: qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;
- Garante: l'autorità di cui all'articolo 153, istituita dalla legge 31.12.1996 n. 675.

Valgono inoltre le seguenti definizioni:

- comunicazione elettronica: ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;
- chiamata: la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale;
- reti di comunicazione elettronica: i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;
- rete pubblica di comunicazioni: una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;
- servizio di comunicazione elettronica: i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche,

compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettere c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002; - abbonato: qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate;

- utente: qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;
- dati relativi al traffico: qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;
- dati relativi all'ubicazione: ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;
- servizio a valore aggiunto: il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione;
- posta elettronica: messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

Ai fini del codice sulla privacy si richiamano le ulteriori seguenti definizioni relative alle misure minime di sicurezza in materia di privacy, previste nel disciplinare tecnico allegato al DLgs 196/2003.

- 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'art. 31;
- strumenti elettronici: gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;
- autenticazione informatica: l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;
- credenziali di autenticazione: i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l' autenticazione informatica;
- parola chiave: componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;
- profilo di autorizzazione: l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;
- sistema di autorizzazione: l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

Si intende, infine, per:

- scopi storici: le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato;
- scopi statistici: le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici;
- scopi scientifici: le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore.

## 1.3. Ambito di applicazione

L'ambito di applicazione riguarda qualsiasi trattamento di dati personali che venga effettuato da chiunque sia 'stabilito' nel territorio dello Stato, anche se i dati vengano detenuti all'estero. Con il termine 'stabilito' il legislatore fa riferimento alla presenza di una stabile organizzazione economica anche se si tratta di una succursale, una filiale o un ufficio. Per quel che riguarda i trattamenti eseguiti al di fuori della UE, ma che impiegano strumenti (anche non elettronici) situati in Italia, è necessario che il Titolare designi un rappresentante stabilito in Italia, a meno che non si tratti di modalità di puro transito.

## 1.4. Riferimenti normativi

D.Lgs. n.196/2003

Parte I Disposizioni generali – Titolo I Principi generali

Art. 4 (Definizioni)

Art. 5 (Oggetto ed ambito di applicazione)
Art. 6 (Disciplina del trattamento)

Parte I Disposizioni generali – Titolo II Diritti dell'interessato

Art. 7 (Diritto di accesso ai dati personali ed altri diritti)

Art. 8 (Esercizio dei diritti)
Art. 9 (Modalita di esercizio)

Art. 10 (Riscontro all'interessato)

Parte I Disposizioni generali – Titolo III Regole generali per il trattamento dei dati

Capo I Regole per tutti i trattamenti - Artt. 11-17

Capo III Regole ulteriori per privati ed enti pubblici economici - Artt. 23-27

Parte I Disposizioni generali – Titolo IV Soggetti che effettuano il trattamento

Art. 28 (Titolare del trattamento)

Art. 29 (Responsabile del trattamento)
Art. 30 (Incaricati del trattamento)

Parte I Disposizioni generali – Titolo V Sicurezza dei dati e dei sistemi

Capo I Misure di sicurezza – Art. 31 (Obblighi di sicurezza)
Capo II Misure minime di sicurezza – Artt. 33-36

Parte III Tutela dell'interessato e sanzioni – Titolo III Sanzioni

Capo I Violazioni amministrative – Artt. 161-166
Capo II Illeciti penali – Artt. 167-172

Allegato B Disciplinare tecnico in materia di misure minime di sicurezza

## 1.5. Revisione del Documento

Il manuale deve essere aggiornato ogni anno e sottoposto a revisione entro e non oltre ogni 31 marzo.

Inoltre deve essere tempestivamente modificato dal Titolare e dal Responsabile del Trattamento qualora, nel corso delle attività svolte, dovessero presentarsi anomalie applicative delle misure di sicurezza adottate o dovessero presentarsi ulteriori nuovi rischi tali da dover intervenire con nuove misure di sicurezza.

# Capitolo 2. FIGURE PREVISTE PER LA SICUREZZA DEI DATI

## 2.1. Titolare del Trattamento dei dati personali

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 è responsabile dell'analisi e della valutazione dei rischi ai fini dell'adozione delle misure di sicurezza, sia idonee, sia minime. La predisposizione della presente modulistica spetta al Titolare.

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

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.

Spetta al titolare del trattamento, coadiuvato dai Responsabili dei trattamenti designati, valutare la congruità tecnico-economica delle misure proposte e quindi disporre l'adozione delle stesse. Il documento programmatico sulla sicurezza è approvato dal titolare, su proposta dei soggetti coinvolti a diverso titolo nelle operazioni di trattamento.

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.

## 2.2. Responsabile della Sicurezza dei dati personali

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, degli uffici e dei locali in genere in cui vengono trattati i dati, nonchè delle banche dati oggetto di trattamento dei dati.

- Se il trattamento è effettuato con mezzi informatici, redigere ed aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione;
- Nominare, per ciascun ufficio o locale 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 acceso 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, della custodia delle copie delle credenziali e delle copie di sicurezza delle banche dati.

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

La nomina di ciascun Responsabile della sicurezza dei 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 che deve essere controfirmata dall'interessato per accettazione (A.01). Copia della lettera di nomina accettata deve essere conservata a cura del Titolare del trattamento in luogo sicuro. La mancata accettazione di tale Responsabilità comporta la preclusione a ricoprire l'incarico.

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.

La nomina del Responsabile del Trattamento può riguardare anche soggetti esterni operanti in nome e per conto del Titolare. Questi soggetti agiscono per finalità definite dal titolare e non hanno poteri decisionali autonomi. Per la loro nomina deve essere utilizzato l'apposito modulo predisposto (A.03), previa l'esibizione da parte di tali soggetti dell'intera documentazione comprovante l'osservanza dei precetti imposti dalla Legge sulla Privacy.

La nomina spetta sempre al Titolare del Trattamento, che dovrà prevederla negli atti di

conferimento di incarichi (convenzioni, protocolli), o comunque dovrà essere prevista, per poi essere formalizzata con successivo atto nei contratti stipulati dall'azienda.

La nomina di un soggetto esterno come Responsabile del Trattamento comporta che il trasferimento di dati personali dall'azienda al soggetto esterno non sia qualificabile tecnicamente come una comunicazione di informazioni. Nominare il soggetto privato come Responsabile del Trattamento fa sì che venga meno il rapporto di terzietà di quest'ultimo rispetto al legame Titolare dell'azienda - interessato al Trattamento; quindi la conoscenza dei dati di quest'ultimo, da parte del soggetto esterno, non è configurabile tecnicamente come una comunicazione.

Per ciò che concerne la nomina dei Responsabili esterni, questa deve essere espressamente accettata dal legale rappresentante pro-tempore del soggetto giuridico nominato o dal soggetto che assumerà tale qualifica. Anche a tali Responsabili esterni deve essere consegnata la lettera di incarico con la specificazione analitica dei compiti assegnati e delle istruzioni relative.

## 2.3. Amministratore di sistema

Ove il Titolare ritenga di nominare un Amministratore di sistema, dovrà formalizzare tale nomina utilizzando una delle figure previste dalla legge, ossia quella di Responsabile o di Incaricato. La prima risulta essere più idonea allo scopo, in quanto consente l'attribuzione di poteri e facoltà adeguatamente ampi. Oltre ai poteri, dovranno essere affiancati compiti e funzioni, facoltà decisionali, anche di spesa, con le relative responsabilità.

La nomina deve essere effettuata dal Titolare del trattamento con una lettera di incarico in cui sono specificate le responsabilità che gli sono affidate e che deve essere controfirmata dall'interessato per accettazione (A.04). Copia della lettera di nomina accettata deve essere conservata a cura del Titolare del trattamento in luogo sicuro. La mancata accettazione di tale Responsabilità comporta la preclusione a ricoprire l'incarico.

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

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

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

G.U. 10 marzo 2007, n. 58) o, in alternativa, mediante altri strumenti di comunicazione interna (ad es., intranet aziendale, ordini di servizio a circolazione interna o bollettini). Ciò, salvi i casi in cui tali forme di pubblicità o di conoscibilità siano incompatibili con diverse previsioni dell'ordinamento che disciplinino uno specifico settore.

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

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

Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

## 2.4. Incaricato del Trattamento dei dati personali

L'individuazione degli incaricati è effettuata a cura del Titolare o del Responsabile del Trattamento, quando nominato, mediante la modulistica predisposta. La designazione è effettuata per iscritto e individua puntualmente l'ambito di trattamento consentito.

Ad ogni soggetto incaricato deve essere consegnata la lettera di incarico redatta in duplice copia di cui una deve essere restituita al Responsabile, opportunamente firmata per ricevuta e da conservarsi agli atti (A.02).

Gli Incaricati del Trattamento sono i soggetti che quotidianamente sono chiamati a rendere effettive le prescrizione del DLgs 196/2003. L'importanza di fornire istruzioni scritte, sia ai Responsabili che agli Incaricati del Trattamento, risiede nell'esigenza di sviluppare la consapevolezza e responsabilizzazione dei soggetti coinvolti affinché operino con le cautele necessarie per un legittimo Trattamento dei dati personali.

Poiché maggiore è il numero di soggetti che hanno accesso ai dati, maggiori sono i rischi di identificazione dell'interessato e quindi le violazioni potenziali della riservatezza del medesimo, l'accesso alle diverse tipologie di dati è consentito ai soli incaricati del Trattamento sotto la diretta autorità del Titolare o del Responsabile. Questa disposizione prevede che non solo si debba procedere necessariamente alla individuazione degli incaricati, ma che questa nomina avvenga differenziando il profilo di ognuno nell'ambito delle finalità proprie del trattamento.

L'autorizzazione deve essere comunque limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di Trattamento. Le autorizzazioni all'accesso sono

rilasciate e revocate dal Titolare e/o dal Responsabile che periodicamente, e comunque almeno una volta l'anno, deve verificare gli incarichi afferenti i dati sensibili in termini sia di legittimità del Trattamento che della sussistenza delle cautele poste in essere per la conservazione dei medesimi dati.

## 2.5. Incaricato della gestione e manutenzione degli strumenti elettronici

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.

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

Ad ogni soggetto incaricato deve essere consegnata la lettera di incarico redatta in duplice copia di cui una deve essere restituita al Responsabile, opportunamente firmata per ricevuta e da conservarsi agli atti (A.06).

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.

## 2.6. Incaricato della custodia delle copie delle credenziali

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.

Ad ogni soggetto incaricato deve essere consegnata la lettera di incarico redatta in duplice copia di cui una deve essere restituita al Responsabile, opportunamente firmata per ricevuta e da conservarsi agli atti (A.05).

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 riservate 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).

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.

## 2.7. Incaricato 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.

Ad ogni soggetto incaricato deve essere consegnata la lettera di incarico redatta in duplice copia di cui una deve essere restituita al Responsabile, opportunamente firmata per ricevuta e da conservarsi agli atti (A.08).

L'Incaricato delle copie di sicurezza delle banche dati è la persona fisica che ha il compito di sovrintendere alla esecuzione periodica delle copie di sicurezza delle Banche 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 backup;
- Il numero di copie di backup effettuate ogni volta;
- Se i supporti utilizzati per le copie di backup sono riutilizzati e in questo caso con quale periodicità;
- Se per effettuare le copie di backup si utilizzano procedure automatizzate e programmate;
- Le modalità di controllo delle copie di backup;
- 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 backup;
- Le istruzioni e i comandi necessari per effettuare le copie di backup.

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;
- Assicurarsi della qualità delle copie di sicurezza dei dati e della loro conservazione in luogo adatto e sicuro;
- Assicurarsi della conservazione delle copie di sicurezza in luogo adatto e sicuro e ad accesso controllato;
- 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;

- Segnalare tempestivamente all'Incaricato della gestione e della manutenzione degli strumenti elettronici, ogni eventuale problema che 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.

## 2.8. Incaricato 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.

Ad ogni soggetto incaricato deve essere consegnata la lettera di incarico redatta in duplice copia di cui una deve essere restituita al Responsabile, opportunamente firmata per ricevuta e da conservarsi agli atti (A.07).

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 di lavoro.

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.

# Capitolo 3. SICUREZZA DEI DATI E DEI SISTEMI

Il DLgs 196/2003 sancisce l'obbligo, per i soggetti coinvolti nelle operazioni di trattamento di dati personali, di adottare le idonee e preventive misure di sicurezza al fine di ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato, trattamento non consentito di dati personali. La custodia e il controllo dei dati personali va adeguato alla natura dei dati e alle specifiche caratteristiche del trattamento, nonché alle conoscenze acquisite in base al progresso tecnologico.

## 3.1. Trattamenti con l'ausilio di strumenti elettronici

Per 'strumenti elettronici' il legislatore intende gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato.

### 3.1.1. Sistema di autenticazione

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 sia 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. Procedura di identificazione

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. Sicurezza PC e supporti rimovibili

Sui computer devono essere installati solo software autorizzati, software valutati ed adottati per i loro aspetti di funzionalità e sicurezza. I PC portatili di proprietà dell'azienda o società non devono essere usati per scopi diversi da quelli aziendali. Tutti i PC, compresi gli 'stand alone' e i portatili, devono essere dotati della versione più aggiornata del software antivirus adottato.

Devono essere disponibili copie pulite di backup dei pacchetti software originali per la reinstallazione in caso di virus.

Gli utilizzatori non devono trasferire sui loro PC dati o programmi provenienti da floppy, o altre unità di immagazzinamento dati, non preventivamente monitorate dall'antivirus.

L'utilizzatore che ritenga che il suo PC sia stato infettato da virus deve immediatamente avvisare il responsabile della sicurezza dei dati personali. Il PC potrà essere utilizzato soltanto dopo la rimozione dei virus.

I supporti rimovibili contenenti dati sensibili o giudiziari devono essere custoditi ed utilizzati in maniera tale da non poter essere accessibili da persone non autorizzate. Una volta cessato lo scopo di conservazione dei dati, i supporti devono essere resi inintelligibili in modo tale da non poter ricostruire i dati in essi contenuti, ossia si deve, se necessario, distruggere il supporto.

Anche per i supporti contenenti dati personali di qualsiasi natura, anche comuni, si raccomanda di seguire le prescrizioni valide per i dati sensibili.

Non deve essere possibile eseguire copie non autorizzate dei dati su supporti rimovibili (floppy, chiavi USB, ecc.) da parte di incaricati.

Un'eventuale copia di dati sensibili o giudiziari su supporto rimovibile, indispensabile per lo svolgimento dell'attività assegnata all'incaricato, potrà essere effettuate solo seguendo le seguenti istruzioni:

- il supporto che dovrà contenere la copia dei dati dovrà essere formattato inizialmente;
- attivare la protezione per ulteriori scritture una volta eseguita la prima;
- apporre una chiara etichetta sul supporto in modo tale da contraddistinguerlo da altri ed identificarne il contenuto;
- il supporto contenente la copia dovrà essere custodito esclusivamente dall'incaricato che lo ha realizzato;
- in caso di spedizione assicurarsi che l'incaricato di destinazione abbia lo stesso profilo di autorizzazione dell'incaricato mittente e che la busta contenente il supporto sia adeguatamente sigillata;
- concordare con l'incaricato destinatario i tempi e le modalità di spedizione della copia prima di effettuarla;
- procedere alla formattazione del supporto qualora i dati contenuti in esso non abbiano più ragione di essere;
- non lasciare mai incustodito sulla scrivania o in altri posti il supporto contenente i dati, bensì assicurarsi che sia conservato sempre in custodia sicura, quando non utilizzato.

### 3.1.4. Gestione password

L'Amministratore di sistema individua le password di almeno 8 caratteri di ciascun utente e le fornisce ai preposti, appositamente nominati.

Tali password devono essere adeguatamente custodite come per gli stessi dati personali.

L'Amministratore di sistema deve fornire le giuste indicazioni agli utilizzatori dei PC nella scelta delle password e nel loro utilizzo.

In tal caso, per evitare accessi non autorizzati, si consiglia nella scelta delle password:

- di non utilizzare come password il nome di login o un codice di identificazione personale in qualunque forma;
- di non scegliere il nome e cognome, comunque modificato;
- di non utilizzare informazioni personali che possono essere recuperate (data di nascita, targa auto, codice fiscale);
- di scegliere una parola chiave con più di 8 caratteri alfanumerici;
- di non usare cifre tutte in ordine crescente o decrescente;

La password deve essere:

- semplice da ricordare;
- possibilmente di senso compiuto;
- composta da caratteri minuscoli e maiuscoli e/o da segni di interpunzione.

La password deve essere modificata almeno ogni 6 mesi (3 se si tratta di dati sensibili).

### 3.1.5. Sicurezza elettronica degli elaboratori in rete

Per gli elaboratore collegati in rete occorre fornire un codice identificativo personale per ogni incaricato del trattamento che dovrà essere univoco e non potrà essere quindi assegnato a persone diverse.

Dovrà essere inoltre prevista la disattivazione di detti codici in caso di mancato utilizzo per un periodo di tempo superiore ai 6 mesi.

Tutti gli elaboratori collegati in rete dovranno essere muniti di software antivirus aggiornato. Per i server di rete dovrà essere previsto un sistema di backup automatico che dovrà assicurare il recupero dei dati in caso di malfunzionamento del sistema. In particolare per ogni server dovrà essere previsto un ciclo di backup.

Le copie di backup dovranno essere custodite in armadi chiusi a chiave presso la sede della società o azienda o anche presso un centro di sicurezza informatica posto all'esterno dell'azienda.

### 3.1.6. Sicurezza elettronica degli elaboratori in Rete Pubblica

La connessione di un PC ad una rete pubblica dovrà essere autorizzata dall'amministratore di sistema.

Tali connessioni con l'esterno dovranno essere protette da adeguati sistemi firewall, ossia dispositivi software o hardware disposti nei punti di interconnessione tra reti distinte, ad esempio tra una rete intranet e la rete esterna Internet, in grado automaticamente di controllare gli accessi ed eventualmente bloccare quelli indesiderati, il tutto in base a parametri definiti dalle politiche di sicurezza adottate.

#### 3.1.7. Protezione locali server

I server dovranno essere posizionati in locali adeguatamente protetti. L'alimentazione elettrica dovrà essere a norma di legge e dovranno essere installati idonei controlli per permettere l'accesso alle sole persone autorizzate.

Per la sicurezza passiva dovranno essere installati dispositivi come rilevatori di fumo o calore, sirena di allarme antincendio, estintore, uscita di sicurezza.

La protezione dei dati contenuti nei dispositivi di immagazzinamento dati dei server (dischi, nastri, cassette, ecc..) dovrà essere garantita dall'amministratore di sistema e dai responsabili dei trattamenti.

## 3.2. Trattamenti senza l'ausilio di strumenti elettronici

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 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 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 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, 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 nei locali individuati per la loro conservazione;
- I documenti contenenti dati personali 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;

- Per evitare il rischio di diffusione dei dati personali 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;
- L'incaricato del trattamento deve evitare che un soggetto terzo non autorizzato al trattamento possa esaminare anche solo la copertina del documento in questione;
- Si raccomanda di non parlare mai ad alta voce, trattando dati personali per telefono, soprattutto utilizzando apparati cellulari, in presenza di terzi non autorizzati. Queste precauzioni diventano particolarmente importanti, quando il telefono è utilizzato in luogo pubblico od aperto al pubblico.

Inoltre 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.

### 3.2.1. Sicurezza archivi cartacei

L'accesso agli archivi cartacei da parte degli incaricati deve essere limitata ai soli dati la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati.

Le procedure di accesso agli archivi possono essere le seguenti:

- fornire la chiave degli archivi ai soli soggetti autorizzati;
- fornire un badge identificativo posto fuori dal locale archivio;
- permettere il prelievo di documenti solo previa registrazione su apposito registro accessi;

Nel caso di dati sensibili devono, inoltre, essere osservate le seguenti procedure:

- le cartelle o fascicoli o supporti cartacei di vario genere devono essere conservati in armadi muniti di serratura con chiave che devono essere chiusi al termine della giornata di lavoro dagli incaricati al trattamento;
- i documenti o atti contenenti dati, affidati agli incaricati del trattamento, qualora non vengano utilizzati ai fini del trattamento stesso, devono essere conservati in contenitori chiusi a chiave fino al loro rientro nell'archivio;
- l'accesso all'archivio deve essere controllato mediante dispositivi di identificazione (badge) anche dopo l'orario di chiusura, e gli eventuali accessi in questi orari devono essere registrati.
- devono essere previsti dispositivi di sicurezza passiva (rilevatori di fumo e calore, campanelli di allarme, estintori).

### 3.2.2. Sicurezza nella cancellazione dei dati

La cancellazione dei dati può essere effettuata quando la conservazione non è più necessaria per gli scopi per i quali gli stessi sono stati raccolti e successivamente trattati.

I dati possono essere cancellati anche su richiesta da parte dell'interessato, sempre che la conservazione non sia necessaria per legge.

La distruzione dei dati deve avvenire con sistemi meccanici o automatizzati in modo da evitare ogni possibile recupero.

## 3.3. Comunicazioni telefoniche o telematiche

La richiesta di dati via telefono può avvenire solo dopo l'accertamento che il richiedente abbia titolo idoneo alla richiesta. In caso di dati sensibili o in circostanze particolari, devono essere utilizzati mezzi di comunicazione dei dati più sicuri.

Prima dell'invio di fax contenenti dati personali è necessario accertarsi della identificazione del destinatario e che gli stessi dati, una volta giunti a destinazione, siano prelevati e non lasciati incustoditi presso il fax ricevente e visibili a terze persone.

# Capitolo 4. DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

## 4.1. Premessa

Obbiettivo principale del Documento Programmatico sulla Sicurezza (DPS) è di fornire un resoconto dettagliato delle misure di sicurezza adottate dall'Azienda o Società titolare di trattamenti di dati personali per evitare, o ridurre al minimo, il verificarsi di qualsiasi tipo di evento dannoso o pericoloso (Rischio) a carico degli stessi dati personali.

Vengono definiti i criteri e le modalità operative adottate dall'Azienda per l'adozione del documento programmatico sulla sicurezza. In particolare vengono individuati, descritti e valutati i rischi e le conseguenti misure di sicurezza adeguate alla protezione della sicurezza delle aree, dei dati e delle trasmissioni, al fine di ridurre al minimo i rischi stessi.

## 4.2. Elenco dei trattamenti dei dati personali (Regola 19.1)

In questa sezione sono individuati i trattamenti effettuati dal titolare, direttamente o attraverso collaborazioni esterne, con l'indicazione della natura dei dati e della struttura (ufficio, funzione, ecc.) interna o esterna operativamente preposta, nonché degli strumenti impiegati.

Nell'allegato DPS.01 è riportato l'elenco dei trattamenti svolti dall'Azienda con tutte le seguenti informazioni:

- Nome del trattamento: è il nome assegnato al trattamento per una più immediata identificazione;
- Descrizione sintetica: contiene la descrizione del trattamento attraverso l'indicazione della finalità perseguita o dell'attività svolta (es. fornitura di beni e servizi, gestione del personale, ecc.) e delle categorie di persone cui i dati si riferiscono (clienti e utenti, dipendenti e/o collaboratori, fornitori, ecc.);
- Tipologia dei dati trattati: specifica se si tratta di dati comuni, sensibili o giudiziari;
- Fonte normativa: eventuali riferimenti a norme e leggi che autorizzano al trattamento dei dati;
- Rilevanti finalità di interesse pubblico: elenco delle eventuali finalità di interesse pubblico, se presenti;
- Descrizione: fornisce la descrizione dettagliata del trattamento;
- Obbligatorietà del consenso: specifica se è necessario, per il trattamento in oggetto, fornire il consenso;
- Conseguenze in caso di rifiuto del consenso: descrive le conseguenze derivanti dal rifiuto a fornire il consenso al trattamento dei dati;
- Struttura di riferimento: indica la struttura (o reparto, funzione, ufficio, ecc.) all'interno della quale viene realizzato il trattamento. Il livello di sintesi utilizzato è stabilito dal titolare. Ad esempio, in caso di strutture complesse, è possibile indicare la macro-struttura (direzione del personale) oppure uffici specifici (ufficio paghe, ufficio sviluppo risorse, ufficio controversie sindacali, ecc.). Per i trattamenti affidati all'esterno sono riportati i dati identificativi del soggetto delegato con l'indicazione dei riferimenti contrattuali;

- Altre strutture coinvolte nel trattamento: sono elencate le altre strutture aziendali che eventualmente concorrono allo svolgimento delle operazioni di trattamento dei dati personali.
- Parametri trattamento: sono elencate dettagliatamente le caratteristiche del trattamento con riferimento alla natura dei dati trattati, comunicazione e diffusione dei dati, categorie interessate, finalità del trattamento, modalità di trattamento;
- Contitolari del trattamento: elenca i soggetti esterni che, eventualmente, concorrono al trattamento in qualità di titolari;
- Banche dati gestite: elenca le banche dati coinvolte nel trattamento;

Per i trattamenti affidati all'esterno:

- Soggetto delegato: riporta tutte le indicazioni che riguardano il soggetto al quale sono state delegate le operazioni di trattamento (Denominazione della ditta, indirizzo completo, recapiti telefonici, ecc.) e il ruolo ricoperto agli effetti della disciplina sulla protezione dei dati personali;
- Rapporto contrattuale: riporta il quadro giuridico o contrattuale (nonché organizzativo e tecnico) in cui tale trasferimento si inserisce, in riferimento agli impegni assunti, anche all'esterno, per garantire la protezione dei dati stessi;
- Attività delegata: è indicata sinteticamente l'attività affidata all'esterno;
- Descrizione sintetica: descrizione sintetica dell'attività delegata;

L'Allegato DPS.01.1 elenca i Database (ovvero le banche dati o l'archivio informatico) in cui sono contenuti i dati. Uno stesso trattamento può richiedere l'utilizzo di dati che risiedono in più di una banca dati. Per ogni banca dati gestita dall'Azienda sono riportate le seguenti informazioni:

- Nome della Banca dati: è il nome assegnato alla Banca dati per una più immediata identificazione;
- Tipologia della banca dati: specifica se si tratta di un database informatico, cartaceo o entrambe la tipologie;
- Tipo di dati trattati: specifica se nella banca dati sono contenuti dati comuni ovvero se tra i dati archiviati sono presenti dati sensibili o giudiziari;
- Trattamenti gestiti: elenca i trattamenti gestiti dal database in oggetto;
- Accesso protetto con password: specifica se l'accesso alla banca dati è protetto da password;
- Frequenza aggiornamento password: specifica la frequenza di aggiornamento della password (giornaliera, settimanale, ecc..);
- Strumenti elettronici impiegati: elenca gli strumenti elettronici utilizzati;
- Strumenti non elettronici impiegati: specifica gli strumenti non elettronici utilizzati;

L'allegato DPS.01.2 elenca gli strumenti elettronici che sono utilizzati per le operazioni di trattamento svolte in modalità informatizzata.

In tale allegato sono inclusi sia gli strumenti hardware di qualsiasi tipo essi siano (personal

computer, palmari, dispositivi di backup, firewall, ecc.), sia gli strumenti software (sistemi operativi, antivirus, programmi generici, ecc.).

Di ogni strumento presente nell'azienda sono indicate le seguenti caratteristiche:

- Nome dello Strumento elettronico: è il nome assegnato allo Strumento per una più immediata identificazione;
- Tipo strumento: designa il tipo di strumento elettronico (PC, palmare, ecc.) utilizzato per le operazioni di trattamento dei dati;
- Descrizione: riporta la descrizione sintetica dello strumento elettronico;
- Accesso protetto con password: specifica se l'accesso allo strumento elettronico è protetto da password;
- Possibilità modifica password: specifica se la password è modificablile;
- Frequenza aggiornamento password: specifica la frequenza di aggiornamento della password (giornaliera, settimanale, ecc..);
- Responsabile delle credenziali: riporta il nominativo della persona designata per la custodia delle credenziali di autenticazione;
- Responsabile della manutenzione: riporta il nominativo della persona o società preposta alla manutenzione dello strumento elettronico;
- Frequenza aggiornamento antivirus: specifica la frequenza di aggiornamento dell'eventuale software antivirus installato (giornaliera, settimanale, ecc..);
- Database gestiti: riporta l'elenco dei database gestiti dallo strumento elettronico;
- Ubicazione: indica la sede dell'azienda (indirizzo completo) e il locale all'interno della stessa sede dove è posto lo strumento in esame;
- Utilizzatore abituale: specifica la persona che abitualmente utilizza lo strumento elettronico;
- Dettaglio caratteristiche: specifica tutte le caratteristiche hardware, le tipologie di connessioni ed i software installati;

L'allegato DPS.01.3 elenca gli strumenti non elettronici che sono utilizzati per le operazioni di trattamento svolte in modalità non informatizzata.

Di ogni strumento non elettronico presente nell'azienda sono indicate le seguenti caratteristiche:

- Nome dello Strumento non elettronico: è il nome assegnato allo Strumento per una più immediata identificazione;
- Tipo strumento: designa il tipo di strumento non elettronico;
- Descrizione: riporta la descrizione estesa dello strumento non elettronico, elencandone le caratteristiche salienti;
- Database gestiti: riporta l'elenco dei database gestiti dallo strumento non elettronico;
- Ubicazione: indica la sede dell'azienda (indirizzo completo) e il locale all'interno della stessa sede dove è posto lo strumento in esame;

L'allegato DPS.01.4 elenca le sedi e gli uffici o locali che sono coinvolti per le operazioni di trattamento.

Di ogni sede sono indicate le seguenti caratteristiche:

- Nome della sede: è il nome assegnato alla sede per una più immediata identificazione;
- Ubicazione: indica la sede dell'azienda (indirizzo, numero civico, città, ecc.);
- Recapiti telefonici: specifica i numeri di telefono e di fax dell'azienda;
- Accesso: specifica il tipo di accesso alla sede;

Di ogni ufficio o locale facente parte della sede indicata sono elencate le seguenti caratteristiche:

- Nome dell'ufficio/locale: è il nome assegnato all'ufficio/locale per permetterne l'identificazione;
- Piano: indica il piano dove è ubicato l'ufficio/locale;
- Caratteristiche di accesso e protezione: vengono elencate le tipologie di accesso e di protezione dell'ufficio;
- Responsabili ufficio/locale: vengono elencati i resposabili dell'ufficio/locale;
- Soggetti autorizzati: vengono elencati i soggetti autorizzati all'accesso nell'ufficio/locale;

## 4.3. Distribuzione dei compiti e delle responsabilità (Regola 19.2)

In questa sezione è descritta l'organizzazione della strutture aziendali (intese come reparti, dipartimenti, uffici, ecc.), i compiti e le relative responsabilità, in relazione ai trattamenti effettuati.

L'Allegato DPS.02 riporta l'elenco delle strutture coinvolte nelle operazioni di trattamento. Per ciascuna struttura elencata sono dettagliati i seguenti aspetti:

- Nome della Struttura: è il nome assegnato alla struttura per consentirne l'identificazione;
- Uffici: elenca gli uffici/locali nei quali opera la struttura aziendale;
- Responsabile della struttura: specifica il soggetto dirigente o responsabile della struttura (da non confondere con la figura del responsabile del trattamento), indicandone il ruolo o la qualifica;
- Trattamenti: indica i trattamenti svolti nella struttura;
- Incaricati della struttura: indica i soggetti incaricati all'interno della struttura, elencando, per ciascuno di essi, i compiti e i permessi assegnati;

## 4.4. Analisi dei rischi che incombono sui dati (Regola 19.3)

In questa sezione sono descritti gli eventi potenzialmente dannosi per la sicurezza dei dati e sono valutate le possibili conseguenze e la gravità in relazione al contesto fisico-ambientale di riferimento e agli strumenti elettronici utilizzati. Infine gli eventi rilevati sono posti in correlazione con le misure previste.

### 4.4.1. Valutazione dei rischi

Le misure minime di sicurezza, cui fanno riferimento gli artt. da 33 a 36 del D.Lgs. n.196/2003, debbono essere adottate, con riferimento al Disciplinare tecnico (Allegato B del succitato D.Lgs), in base ai rischi che possono individuarsi. In concreto i possibili eventi che possono manifestarsi possono essere compresi in tre categorie:

- Comportamenti degli operatori: si tratta di rischi connessi al mancato rispetto degli adempimenti e delle prescrizioni stabilite del D.Lgs 196/2003 in materia di trattamento di dati personali;
- Eventi relativi agli strumenti: comprendono i rischi propri del sistema informatico utilizzato dall'Azienda;
- Eventi relativi al contesto fisico-ambientale: includono tutti quegli eventi (naturali o artificiali) connessi al contesto in cui opera l'Azienda (guasti, eventi distruttivi, ingressi non autorizzati, ecc.).

Alla fase di individuazione dei possibili eventi segue la fase valutativa dei rischi, al fine di verificare:

- l'efficacia degli strumenti impiegati, che permette di assegnare al rischio un indice di rilevanza e di probabilità con la finalità ultima di individuarne anche le consequenziali azioni correttive;
- le misure che sono risultate non adeguate.

In particolare si è tenuto conto di due indici:

probabilità (p) di accadimento, che riguarda la frequenza riscontrata o riscontrabile;
rilevanza (m) delle conseguenze, nel caso lo stesso evento si verifichi.

Il Rischio è che la risultante della probabilità e della rilevanza di un evento: l'indice R è quindi dato dal prodotto p x m. Secondo i criteri adottati dando a p e a m un valore fra 1 e 4, si ottiene il valore R compreso fra 1 e 16.

Probabilità (p)

Bassa (p=1):Non sono noti episodi
Media (p=2):Sono noti rari episodi
Alta (p=3): Noto qualche episodio
Altissima (p=4):Noti molti episodi

Rilevanza (m)

Bassa (p=1): Furto o distruzione dei dati

Media (p=2): Utilizzo illegale o alterazione dei dati

Alta (p=3): Perdita di dati causata da un uso non autorizzato
Altissima (p=4):Perdita dei dati a seguito di diffusione illegale

Il processo di individuazione degli eventi e la successiva valutazione dei rischi eventualmente manifestatisi deve essere ripetuto con cadenza almeno annuale e, comunque, ogni qualvolta si verifichi un evento grave connesso al trattamento o segnalato dall'installatore esterno delle misure minime di sicurezza.

Le misure minime di sicurezza devono tendere a 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. L'adeguatezza delle misure deve essere valutata, secondo le linee guida indicate in questo documento, tenendo conto delle conoscenze acquisite in base al progresso tecnico, alla natura dei dati trattati e alle specifiche caratteristiche del trattamento.

### 4.4.2. Rischi riguardanti il comportamento degli operatori

Sono stati individuati e valutati tutti i rischi previsti dalla legge, quali, ad es. il rischio di uso non autorizzato dei dati, il rischio di mancata conservazione o restituzione di documenti, il rischio di presa visione abusiva, il rischio di furto di credenziali di autenticazione, ecc. .

Un efficace contenimento al verificarsi di eventi inclusi in tale categoria si ottiene con un adeguato ed efficiente piano di formazione degli incaricati del trattamento che sono i soggetti potenzialmente esposti a compiere le più comuni violazioni della privacy quali, per esempio, comunicazioni o diffusioni illegittime di dati personali o utilizzo di tali dati per fini non conformi alle finalità del trattamento.

La formazione per rivelarsi pienamente efficace non può non comprendere una adeguata conoscenza del disposto normativo che possa realmente e proficuamente garantirne l'osservanza ed in definitiva possa abbattere significativamente i rischi connessi a tale primo settore, che è concordemente ritenuto il più rilevante ed in definitiva quello verso il quale dedicare gli sforzi più intensi.

### 4.4.3. Rischi riguardanti gli eventi relativi agli strumenti

Sono stati identificati e valutati gli eventi del sistema informatico installato nell'Azienda e tutti quelli che sono propri della sua normale attività quali, ad esempio, malfunzionamenti, azione di virus informatici, spamming o tecniche di sabotaggio, intercettazione di informazioni in rete, ecc. .

### 4.4.4. Rischi riguardanti gli eventi riguardanti il contesto

Sono stati identificati e valutati gli eventi propri del contesto in cui opera l'Azienda quali, ad esempio, eventi distruttivi naturali, artificiali, dolosi o accidentali, guasti a sistemi complementari, ingressi non autorizzati, ecc. .

L'allegato DPS.03 riporta l'elenco dei rischi individuati. Per ciascun rischio sono indicati:

- Evento rilevato: è l'evento che corrisponde ad una delle tre categorie descritte in precedenza identificato grazie alla categoria di appartenenza, alla descrizione e ad un codice identificativo univoco;
- Contromisure adottabili: elenca le contromisure adottabili per il rischio in oggetto;
- Impatto sulla sicurezza dei dati: descrive le principali conseguenze individuate per la sicurezza dei dati e ne valuta la loro gravità in base alla rilevanza e alla probabilità

stimata dell'evento espresse in termini sintetici (alta, media, bassa);

- Misure di sicurezza collegate: elenca le misure di sicurezza collegate al rischio in oggetto;

## 4.5. Misure in essere e da adottare (regola 19.4)

Questa sezione del DPS elenca dettagliatamente le misure in essere e da adottare per contrastare i rischi individuati. Per misura si intende lo specifico intervento tecnico od organizzativo posto in essere (per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia), come pure quelle attività di verifica e controllo nel tempo, essenziali per assicurarne l'efficacia. Le azioni necessarie per l'adozione di idonee misure di sicurezza riguardano:

- prevenzione: attività che permette di impedire gli accadimenti negativi, agendo direttamente sulla diminuzione delle probabilità di manifestazione dei pericoli;
- contrasto: attività che permette di impedire il verificarsi di effetti negativi in concomitanza del verificarsi di un evento;
- riduzione: attività che permette di diminuire la gravità degli effetti causati eventualmente dall'accadimento dell'evento di pericolo.

Dopo aver analizzato e valutato i fattori di rischio, relativi ai comportamenti degli operatori, agli strumenti e al contesto fisico-ambientale, sono state individuate le misure di prevenzione, contrasto o riduzione più idonee per il rischio che si intende fronteggiare.

L'allegato DPS.04 riporta l'elenco delle misure di sicurezza.

Per ogni insieme di misure corrispondenti ad un dato rischio, sono elencati i trattamenti interessati, le misure in essere e da adottare e le schede analitiche corrispondenti alle misure già in essere nell'Azienda. In dettaglio sono riportati i seguenti campi:

- Nome dell'insieme di misure: è il nome assegnato all'insieme di misure per consentirne l'identificazione;
- Descrizione: riporta una descrizione sommaria dell'insieme di misure indicando tutti gli elementi ritenuti utili per una completa applicazione delle regole esposte;
- Rischio contrastato: contiene gli elementi informativi relativi al rischio contrastato, così come definito nei precedenti paragrafi, per il quale si prendono in considerazione le misure elencate di seguito;
- Misure in essere: sono elencate le misure già adottate dall'Azienda per fronteggiare un dato rischio. Per ciascuna misura è fornita la descrizione. Completa il quadro una eventuale scheda tecnica analitica di dettaglio che riguarda la misura. Per ogni scheda sono riportate le seguenti informazioni: data di compilazione, descrizione sintetica, tipologia (preventiva, contrasto, contenimento effetti), data di successiva revisione ed elenco degli autori della scheda;
- Misure da adottare: sono elencate le misure da adottare per fronteggiare un dato rischio. Per ciascuna misura è fornita la descrizione. Completa il quadro una eventuale scheda tecnica analitica di dettaglio che riguarda la misura. Per ogni scheda sono riportate le seguenti informazioni: data di compilazione, descrizione sintetica, tipologia (preventiva, contrasto, contenimento effetti), data di successiva revisione ed elenco degli autori della

scheda;

- Trattamenti interessati: elenca i trattamenti di dati personali che sono interessati dall'insieme di misure prese in considerazione.

L'insieme delle misure di sicurezza in essere o da adottare, per ogni categoria di rischi individuati, è dinamicamente aggiornato con l'obiettivo di un miglioramento continuo del Sistema Sicurezza dell'Azienda.

Le misure sono sottoposte a riesame con cadenza almeno annuale e comunque ogni qualvolta si riscontri una non conformità (sia tecnica che normativa) o una generica necessità di intervento.

## 4.6. Criteri e modalità di ripristino della disponibilità dei dati (regola 19.5)

In questa sezione sono descritti i criteri e le procedure adottate per il ripristino dei dati in caso di loro danneggiamento o di inaffidabilità della base dati.

L'importanza di queste attività deriva dall'eccezionalità delle situazioni in cui il ripristino ha luogo: è essenziale che, quando sono necessarie, le copie dei dati siano disponibili e che le procedure di reinstallazione siano efficaci.

Il Disciplinare tecnico (Allegato B al D.Lgs. 196/2003) al punto 19.5 impone '...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...'. Il punto 23 stabilisce che '...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.'

Considerato che ogni sistema informatico deve prevedere un piano di emergenza per soddisfare le specifiche del disciplinare tecnico è necessario riferirsi alle procedure già applicate ed in particolare alla dichiarazione di responsabilità dell'installatore esterno all'Azienda, per quel che riguarda le misure minime di sicurezza del trattamento dei dati personali e tra queste quelle previste per le copie di backup.

Il Titolare ed il Responsabile del trattamento dei dati personali hanno previsto una serie di procedure di recupero immediato dei dati in caso di attacchi e, comunque, delle copie di salvataggio periodiche dei dati personali trattati.

Per il raggiungimento di tale obiettivo sono state analizzati e testati tutti gli strumenti informatici hardware e software dell'intero sistema informatico aziendale.

L'allegato DPS.05 riporta in dettaglio, per tutte le banche dati gestite in maniera informatica, le procedure di salvataggio e ripristino adottate nell'Azienda.

In dettaglio per il salvataggio dei dati sono previste le voci specificate nel seguente elenco:

- Nome della Banca dati: è il nome assegnato alla Banca dati per una più immediata identificazione;
- Tipologia della banca dati: specifica se si tratta di una banca dati informatica, cartacea o

entrambe;

- Tipologia dei dati: specifica se nella banca dati sono contenuti dati comuni ovvero se tra i dati archiviati sono presenti dati sensibili o giudiziari;
- Procedura salvataggio: contiene una approfondita descrizione di natura tecnica con le istruzioni operative delle procedure da seguire per il salvataggio periodico dei dati;
- Frequenza salvataggio: indica la frequenza (giornaliera, settimanale, ecc.) con la quale procedere all'esecuzione delle copie di backup dei dati;
- Numero di copie: specifica il numero di copie di backup previste;
- Incaricato del salvataggio: indica la persona che, all'interno dell'Azienda, ha il compito di eseguire il salvataggio e/o di controllarne l'esito;
- Supporti salvataggio: specifica il tipo dei supporti di memorizzazione, cioè dei supporti magnetici o ottici utilizzati per le copie di sicurezza dei dati (nastri, CD, DVD, ecc.) ed ogni altro supporto rimovibile;
- Ufficio conservazione copie: specifica l'ufficio/locale nel quale sono conservati i supporti di memorizzazione;
- Tipo conservazione delle copie: specifica la natura dello strumento utilizzato per la conservazione (armadio con serratura, ecc..);
- Dettaglio conservazione delle copie: eventuale descrizione dettagliata riguardante l'ubicazione delle copie;

Per la sezione dedicata al ripristino sono riportate le seguenti informazioni:

- Procedure operative di ripristino: contiene la descrizione di natura tecnica con le istruzioni operative delle procedure da seguire per l'esecuzione dei test di efficacia delle procedure di ripristino;
- Frequenza prove di ripristino: indica la frequenza prevista (settimanale, mensile, ecc.) con la quale effettuare i test di efficacia delle procedure di ripristino dei dati adottate.
- Incaricato: indica la persona che, all'interno dell'Azienda, ha il compito di eseguire le prove di ripristino dei dati;

## 4.7. Pianificazione degli interventi formativi previsti (regola 19.6)

In questa sezione sono riportate le informazioni necessarie per disporre di un quadro sintetico dell'impegno formativo che si prevede di sostenere in attuazione della normativa.

### 4.7.1 Scopo della formazione

La previsione degli interventi formativi degli incaricati del trattamento rientra tra gli aspetti più importanti del presente documento programmatico sulla sicurezza e ciò in quanto ha senso parlare di effettiva sicurezza del trattamento solo in costanza di un dettagliato piano di formazione degli incaricati.

Da quanto evidenziato consegue che la sola predisposizione e applicazione di sofisticati strumenti di sicurezza non siano sufficienti a garantire la sicurezza se non affiancati da capacità e/o adeguate conoscenze del personale chiamato alla loro gestione.

Una gestione non improntata a principi di correttezza da parte degli operatori, la mancanza di

chiare direttive esplicative e l'assenza di strumenti di controllo di facile e rapida applicazione, costituiscono le cause principali perché si causino, anche in maniera inconsapevole, danni agli interessati ed in definitiva rappresentano la causa prima di trattamenti illegittimi.

Quanto premesso trova effettivo riscontro nel Disciplinare tecnico (Allegato B al D.Lgs. 196/2003) che al punto 19.6 impone '...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'.

### 4.7.2 Aggiornamento e programmi individuali di formazione

Dopo avere affrontato nel dettaglio l'importanza di tale adempimento deve, comunque, ricordarsi che la formazione deve essere sempre aggiornata in base al disposto del D.Lgs n. 196/2003 in coincidenza con l'obbligo di aggiornamento del Documento Programmatico sulla Sicurezza. Deve tenersi ben presente la distinzione tra:

- Aggiornamento periodico
- Aggiornamento specifico

L'aggiornamento periodico deve essere realizzato sotto la diretta vigilanza del Responsabile del Trattamento o del diverso soggetto identificato dal Titolare del trattamento, con cadenza almeno annuale.

L'aggiornamento specifico deve essere tempestivamente effettuato ogni qualvolta l'incaricato sia deputato a trattare nuove banche dati oppure utilizzi nuovi strumenti informatici e/o nuove e diverse procedure.

Muovendo da questa considerazione ne discende che se l'incaricato viene assegnato a nuove mansioni o se viene trasferito da un settore ad un altro deve essere effettuato un nuovo e specifico aggiornamento mediante un programma individuale che deve essere impartito dal Responsabile in relazione alla nuova e specifica attività di trattamento svolta.

Nell'allegato DPS.06 sono riportate le voci specificate nel seguente elenco:

- Intervento formatico: è il nome assegnato al corso per permetterne l'identificazione;
- Argomento: è elencato l'argomento trattato nel corso;
- Classi di incarico interessate: individua le classi omogenee di incarico a cui l'intervento è destinato e/o le tipologie di incaricati interessati;
- Dati del corso: tempo previsto, numero di interessati, numero di interessati formati negli anni precedenti e da formare nell'anno in corso;
- Partecipanti previsti: elenco dei partecipanti previsti per l'intervento formativo.

## 4.8. Trattamenti affidati all'esterno (Regola 19.7)

Questa sezione riporta un quadro sintetico delle attività affidate a terzi che comportano il

trattamento di dati, con l'indicazione sintetica del quadro giuridico o contrattuale (nonché organizzativo e tecnico) in cui tale trasferimento si inserisce, in riferimento agli impegni assunti, anche all'esterno, per garantire la protezione dei dati stessi. L'allegato DPS.07 riporta le informazioni essenziali:

- Nome del trattamento: nome assegnato al trattamento;
- Descrizione sintetica: descrizione sintetica del trattamento;
- Tipologia dei dati trattati: specifica se nel trattamento sono coinvolti dati comuni o sensibili o giudiziari;
- Soggetto delegato: riporta tutte le indicazioni che riguardano il soggetto al quale sono state delegate le operazioni di trattamento (Denominazione della ditta, indirizzo completo, recapiti telefonici, ecc.) e il ruolo ricoperto agli effetti della disciplina sulla protezione dei dati personali;
- Rapporto contrattuale: riporta gli estermi contrattuali del rapporto in essere con l'azienda;
- Sede: riporta l'indirizzo completo;
- Attività delegata: è indicata sinteticamente l'attività affidata all'esterno;
- Descrizione sintetica: è una descrizione sintetica dell'attività delegata;

## 4.9. Cifratura dei dati o separazione dei dati identificativi (regola 19.8)

In questa sezione sono rappresentate le modalità di protezione adottate in relazione ai dati per cui è richiesta la cifratura o la separazione fra dati identificativi e dati sensibili, nonché i criteri e le modalità con cui viene assicurata la sicurezza di tali trattamenti.

Il presente paragrafo evidenzia le ulteriori misure in caso di trattamento di dati sensibili o giudiziari richieste dal disciplinare tecnico del D.Lgs. n. 196/2003 ed in particolare dal punto 19.8. per i dati personali idonei a rivelare lo stato di salute. Vengono, pertanto, individuati dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Per comprendere nel dettaglio gli adempimenti da effettuarsi occorre richiamare il punto 20 del disciplinare tecnico secondo quale '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'ed il successivo punto 21 che stabilisce, inoltre, che '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', oltre ancora il punto 22 secondo il quale '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'.

Per quanto riportato nel detto disciplinare, il punto 23 prescrive che '...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'.

Per quanto sopra riportato non v'è dubbio che la protezione crittografica dei dati, cui si riferisce lo stesso Testo Unico in materia di trattamento di dati personali, rappresenti un prezioso strumento di

tutela e di sicurezza contro i rischi di accesso ai dati personali.

Deve porsi particolare attenzione al trattamento dei dati sensibili poiché debbono essere archiviati nel sistema informatico centrale con estrema sicurezza, perché l'accesso alla consultazione e/o alla modificazione dei dati sensibili sarà sempre condizionato dal rispetto della procedura di identificazione degli incaricati ed in definitiva dei seguenti criteri, in base ai quali:

- L'incaricato deve essere precisamente individuato ed autenticato;
- L'incaricato può trattare i dati sensibili solo con un appropriato profilo di autorizzazione;
- L'incaricato deve essere in possesso della chiave di lettura o cifratura.

Per quanto detto, e per le menzionate procedure gestionali dei dati sensibili, deve evidenziarsi in definitiva che i dati sensibili debbono essere nettamente separati e gestiti autonomamente ed indipendentemente da ogni incaricato, unicamente in base al proprio profilo di autorizzazione.

L'allegato DPS.08 riporta le informazioni essenziali:

- Nome della banca dati: è il nome assegnato alla banca dati interessata per una più immediata identificazione;
- Tipologia della banca dati: specifica se si tratta di una banca dati informatica, cartacea o entrambe;
- Tipologia dei dati trattati: specifica se nel trattamento sono coinvolti dati comuni o sensibili o giudiziari;
- Protezione scelta: elenca la tipologia di protezione scelta;
- Descrizione tecnica: riporta una descrizione della tecnica utilizzata per la cifratura o separazione dei dati;
- Data di effettività: riporta la data di attuazione delle procedure descritte;

# Capitolo 5. DIRITTI DELL'INTERESSATO

## 5.1. Premessa

Questa sezione del Manuale si occupa di formalizzare tutti gli adempimenti che l'azienda deve obbligatoriamente seguire nei riguardi del soggetto interessato al trattamento di dati personali e, più in generale, della gestione di tutte le richieste che giungono dall'esterno.

Nel titolo II, il Codice individua i diritti dell'interessato, che possono distinguersi in diritti di conoscenza, diritti di accesso, diritti di intervento e diritti di opposizione. Per interessato, è bene ricordarlo, si intende la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

In dettaglio, ai sensi dell'art. 7 del DLgs 196/2003, l'interessato ha diritto d'accesso ai propri dati personali che siano detenuti dal Titolare. Inoltre ai sensi dello stesso articolo, sono formalizzate le procedure da adottare per il rispetto delle richieste dell'interessato e per la gestione operativa delle stesse.

Sono altresì descritte le procedure di cui all'art. 13 del DLgs 196/2003, in tema di informativa da fornire agli interessati e di raccolta del consenso al trattamento di dati personali (C.01 - C.02 - C.03).

## 5.2. Riferimenti normativi

D.Lgs. n.196/2003

Parte I Disposizioni generali – Titolo II Diritti dell'interessato

- Art. 7 (Diritto di accesso ai dati personali ed altri diritti)
- Art. 8 (Esercizio dei diritti)
- Art. 9 (Modalita di esercizio)
- Art. 10 (Riscontro all'interessato)

Parte I Disposizioni generali – Titolo III Regole generali per il trattamento dei dati

- Capo I Regole per tutti i trattamenti - Artt. 11-17
- Capo III Regole ulteriori per privati ed enti pubblici economici - Artt. 23-27

## 5.3. Il diritto di conoscere

L'interessato ha diritto di ottenere conferma della presenza di dati personali che lo riguardano. Egli non solo ha diritto di rivolgersi al Titolare o al Responsabile per chiedere dell'esistenza di suoi dati personali, quanto ha diritto ad ottenere indicazioni circa l'esistenza di dati che lo riguardano,

l'origine, le finalità e le modalità di trattamento, la logica applicata in caso di trattamento dei suoi dati con strumenti elettronici e gli estremi identificativi del Titolare e dei Responsabili che trattano i suoi dati.

La richiesta di accesso dell'interessato può essere rinnovata, anche senza motivazione.

Al soggetto interessato devono essere date tutte le informazioni e le indicazioni circa i suoi dati trattati, non limitandosi a rispondere in termini generici, ma fornendo dettagliatamente tutte le informazioni che lo riguardano e che sono oggetto di trattamento (es. nome, cognome, indirizzo, telefono, e-mail, ecc.).

L'art. 13 del Testo Unico in materia di trattamento dei dati personali indica una serie di elementi che devono essere necessariamente presenti nell'informativa che il Titolare del Trattamento dei dati personali deve obbligatoriamente rendere all'interessato o alla persona presso la quale sono raccolti i dati.

Le informazioni da fornire riguardano:

- il nome, la denominazione o la ragione sociale e il domicilio, la residenza o la sede del Titolare e, se designato, del Responsabile;
- le finalità e le modalità del Trattamento;
- la natura obbligatoria o facoltativa del conferimento dei dati;
- le conseguenze di un eventuale rifiuto;
- i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati e l'ambito di diffusione dei dati medesimi;
- i diritti di cui all'articolo 7 del DLgs 196/2003.

Al fine di permettere il più agevole raggiungimento ed il maggiore soddisfacimento degli scopi previsti nell'art. 13 del DLgs 196/2003 e garantire agli interessati un reale, efficace e trasparente controllo del Trattamento dei dati personali che li riguardano, si è ritenuto di fornire opzionalmente un'informativa scritta, anche nei casi in cui la normativa consente la possibilità di fornire una informativa solo orale o per i casi di trattamento non condizionato dal previo consenso dell'interessato in quanto rientrante integralmente nella previsione dei casi di esclusione del consenso previsti dalla normativa.

Il Titolare non può, in ogni caso, omettere o rifiutarsi di fornire le suddette informazioni su richiesta dell'interessato.

## 5.4. Il diritto di controllare

L'interessato, oltre ad avere il diritto di conoscere l'esistenza di dati personali che lo riguardano, ha anche il diritto ad ottenere una serie di adempimenti, da parte di chi tratta i dati, che pongano rimedio ad eventuali inesattezze dei dati stessi.

L'interessato ha diritto di chiedere ed ottenere l'aggiornamento e la rettificazione dei dati, qualora essi siano inesatti e la loro integrazione.

Il Codice prevede che il Titolare debba comunicare l'aggiornamento, la rettifica o l'integrazione ai soggetti ai quali i dati sono stati comunicati o diffusi. Tale operazione può essere evitata solo nel caso in cui per adempiere il diritto debbano essere impiegati mezzi evidentemente sproporzionati rispetto al diritto tutelato.

## 5.5. Il diritto di opposizione

L'interessato ha il diritto di opporsi, in tutto o in parte, per motivi legittimi, al trattamento e può richiedere la cancellazione, la trasformazione o il blocco dei dati.

Nel valutare la legittimità del motivo, ha valore il comportamento del soggetto interessato, nel senso che può essere giudicato motivo non legittimo quello di un soggetto che abbia fornito spontaneamente i suoi dati e poi, senza motivi oggettivamente validi, voglia che siano cancellati solo per creare ad esempio disagi nella organizzazione della banca dati. Altresì l'interessato ha in ogni caso il diritto di opporsi al trattamento dei suoi dati ai fini di invio di materiale pubblicitario o per indagini di mercato o comunicazioni commerciali.

## 5.6. Esercizio dei diritti

L'interessato può avanzare la richiesta di accesso ai suoi dati al Titolare o al Responsabile, anche senza particolari formalità (es. lettera raccomandata, e-mail), anche utilizzando l'apposito modello previsto (C.04). Anche durante una telefonata l'interessato può avanzare, all'impiegato con cui è in contatto in quel momento, la richiesta di accesso ai suoi dati. Sarà cura dell'impiegato avanzare la richiesta al Responsabile. La norma prevede che l'interessato debba dimostrare la sua identità esibendo un documento di riconoscimento ovvero allegando copia dello stesso se la richiesta viene effettuata via posta o mezzo analogo.

Il Titolare o il Responsabile devono fornire riscontro alla richiesta entro 15 giorni dal suo ricevimento oppure informare l'interessato di eventuali ritardi nella risposta per validi motivi inerenti la complessità nell'espletamento.

Le modalità di risposta ad una richiesta consistono nell'estrazione dei dati e nella trasmissione degli stessi mediante mezzi idonei, rendendo gli stessi dati comprensibili e, se l'interessato ne facesse richiesta, trasferendo gli stessi anche su supporti informatici oppure trasmettendoli per via telematica.

Di norma va precisato che vanno fornite solo le informazioni e non copie di documenti di cui queste fanno parte, ossia l'interessato non può pretendere di avere copia di tutti i documenti in cui siano presenti suoi dati.

## 5.7. Garanzie per i dati sensibili

Ai sensi dell'art. 26 del DLgs 196/2003 i soggetti privati possono effettuare trattamento di dati sensibili solo con il consenso scritto dell'interessato e previa autorizzazione del Garante. Tale principio non si applica ai dati relativi agli aderenti alle confessioni religiose o ad organizzazione di

carattere sindacale. Inoltre i dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante, quando il trattamento è effettuato da associazioni, enti od organismi senza scopo di lucro, a carattere politico, filosofico, religioso o sindacale.

Gli esercenti professioni sanitarie trattano i dati personali idonei a rivelare lo stato di salute con il consenso dell'interessato e anche senza autorizzazione del Garante se il trattamento riguarda dati e operazioni indispensabili per perseguire una finalità di tutela della salute o dell'incolumità dell'interessato. È possibile il trattamento anche senza il consenso dell'interessato, e previa autorizzazione del Garante, se le finalità di cui al precedente punto riguardano un terzo o la collettività. Per i casi citati il consenso è prestato con modalità semplificate disciplinate dagli artt. 78, 79 e 80 del DLgs 196/2003.

# Appendice. DISCIPLINARE TECNICO

## Allegato B. 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, nonchè 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, nonchè 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.