

# Manuale della Privacy

Redatto ai sensi del D.Lgs. 196/2003 e del relativo disciplinare tecnico

 <p><b>FONDAZIONE</b> CENTRI DI RIABILITAZIONE <b>PADRE PIO ONLUS</b> <small>DEI FRATI MINORI CAPPUCCINI FOGGIA PROVINCIA DI SANT'ANGELO E PADRE PIO</small></p>	
Fondazione Centri di Riabilitazione Padre Pio Onlus	
71013 San Giovanni Rotondo FG	
Viale dei Cappuccini, 77	<b>Versione 1.0 - Data: 19/12/2016</b>



## Manuale della Privacy

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



### Dati generali

---

**Progetto** CentriPadrePio

**Descrizione**

**Denominazione** Fondazione Centri di Riabilitazione Padre Pio Onlus

**Indirizzo sede** Viale dei Cappuccini, 77

**Località sede** 71013 San Giovanni Rotondo (FG) - Italy

**Titolare** Fondazione Centri di Riabilitazione Padre Pio Onlus

**Versione** Versione 1.0

**Data** 19/12/2016

## Capitolo 1. PRESENTAZIONE DEL MANUALE

### 1.1 Oggetto e finalità

Il Manuale, redatto sulla base di quanto previsto dal DLgs 196/2003, 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 dalla Fondazione Centri di Riabilitazione "Padre Pio Onlus" 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 della Fondazione 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
- ✓ **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.
- ✓ 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. Struttura e Revisione del Documento

Il presente Manuale è strutturato in sezioni numerate progressivamente. Ogni sezione presenta degli allegati individuati con un codice alfanumerico seguito da due numeri. Il primo

numero identifica la Sezione del Manuale e il secondo il numero progressivo del documento, qualora una sezione presenti più di un allegato.

Il Manuale deve essere tenuto ed aggiornato dal Titolare del Trattamento, deve essere soggetto a revisione periodica e 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.

Il Manuale deve essere sottoposto a revisione entro e non oltre ogni 31 marzo.

I responsabili del trattamento hanno il compito di formulare le proposte di modificazione e integrazione nonché di garantire la corretta applicazione e conservazione del manuale.

Lo stato di revisione del documento è riportato in alto a destra, nella griglia di intestazione, contraddistinto da un numero progressivo e dalla data di approvazione.

## **1.5. 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 (Modalità 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 Disciplina tecnica in materia di misure minime 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, previa 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 del trattamento interno dei dati**

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 del trattamento dei dati 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, nonché 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 accesso ai locali e le misure da adottare per la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- ✓ Qualora il trattamento dei dati sia stato affidato in tutto o in parte all'esterno della struttura del titolare, controllare e garantire che tutte le misure di sicurezza riguardanti i dati personali siano applicate;
- ✓ Se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più incaricati della gestione e della manutenzione degli strumenti elettronici, della custodia delle copie delle credenziali e delle copie di sicurezza delle banche dati;



- ✓ verificare la liceità e la correttezza dei trattamenti ai sensi dell'art.11 del D.Lgs. n.196/2003 mediante l'effettuazione di controlli periodici;
- ✓ adeguare la modulistica approvata dal Titolare del Trattamento, al fine di fornire l'informativa agli interessati e per raccogliere il consenso, nei casi in cui necessita, dell'interessato al trattamento dei dati di tipo sensibile;
- ✓ redigere una relazione periodica sullo stato del processo di trattamento;
- ✓ valutare e quindi segnalare al Titolare per i trattamenti di propria competenza, le misure di sicurezza idonee e preventive da adottare ai sensi degli articoli da 33 a 36 del D.Lgs. n.196/2003 e del disciplinare tecnico di cui all'allegato B del medesimo;
- ✓ adottare le misure di sicurezza minime ai sensi degli articoli da 33 a 36 del Testo Unico in materia: le misure di protezione sono attualmente individuate dal disciplinare tecnico allegato B del Testo Unico e differenziate a seconda degli strumenti utilizzati per il trattamento (automatizzati oppure no) e della natura dei dati trattati (sensibili, giudiziari, comuni);
- ✓ delineare i profili dei soggetti che svolgono le operazioni di trattamento, all'interno della struttura di propria competenza, e individuare gli stessi come incaricati, fornendo loro istruzioni scritte, ai sensi dell'articolo 30 del D.Lgs. n.196/2003: a tal proposito occorre utilizzare la modulistica predisposta (allegati A. Lettere di nomina);
- ✓ fornire le informative agli interessati, ai sensi dell'art. 13 del D.Lgs. n 196/2003, adeguando la modulistica generale predisposta alle proprie esigenze (allegato C.01);
- ✓ raccogliere e conservare i moduli con il consenso espresso dagli interessati (allegato C.02) relativamente al trattamento dei dati sensibili;
- ✓ informare prontamente il Titolare di tutte le questioni rilevanti ai fini di legge;
- ✓ procedere alle verifiche sulla qualità dei dati trattati, in particolare curando il controllo sull'esattezza dei dati al momento della raccolta e provvedendo all'aggiornamento dei dati stessi;
- ✓ verificare i procedimenti di rettifica dei dati; l'interessato al trattamento dei dati personali può esercitare il diritto di accesso alle sue informazioni (ai sensi dell'art. 7 e seguenti del Testo unico della Privacy) e può chiedere l'aggiornamento, la rettificazione e, qualora vi abbia interesse, l'integrazione dei dati;
- ✓ verificare la corrispondenza delle finalità del trattamento rispetto alle disposizioni di legge e soprattutto al consenso manifestato dall'interessato nel caso di trattamento di dati sensibili;
- ✓ controllare la pertinenza, non eccedenza e completezza dei dati rispetto alle finalità del trattamento di propria competenza;
- ✓ provvedere alla cancellazione o alla trasformazione dei dati in forma anonima quando vi sia una richiesta dell'interessato (allegato C.04), ai sensi dell'art. 7 citato oppure quando si riscontri che il trattamento sia svolto in violazione di legge; nel caso di richiesta di blocco del trattamento comunicare la circostanza al Titolare;
- ✓ dare risposte ad esigenze di tipo operativo e gestionale, relative al trattamento, chiedendo, se necessario, parere al Titolare;

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

La nomina di ciascun Responsabile del trattamento 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. 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 del trattamento dei dati personali delle responsabilità che gli sono affidate in conformità a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal Codice in materia di protezione dei dati personali (Dlgs. n.196 del 30 giugno 2003) e 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 del trattamento dei dati personali una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

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

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

### **2.3. Responsabile del trattamento esterno dei dati**

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, 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 dalla Fondazione.

La nomina di un soggetto esterno come Responsabile del trattamento comporta che il trasferimento di dati personali dalla Fondazione 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 della Fondazione - 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.

### **2.4. Responsabile del trattamento esterno agente come titolare autonomo**

A differenza di quanto previsto per il soggetto inquadrato come Responsabile del trattamento esterno dei dati, il responsabile che agisce come titolare autonomo è un soggetto esterno con potere decisionale autonomo.

In questo caso il trasferimento di dati personali dalla Fondazione al soggetto esterno è qualificabile come una comunicazione di informazioni. Per rendere tale comunicazione lecita sarà sufficiente che il titolare che ha raccolto i dati specifici nell'informativa i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati.

Per la loro nomina può essere utilizzato l'apposito modulo predisposto, previa l'esibizione da parte di tali soggetti dell'intera documentazione comprovante l'osservanza dei precetti imposti dalla Legge sulla Privacy. La nomina deve essere espressamente accettata dal legale rappresentante pro-tempore del soggetto giuridico nominato o dal soggetto che assumerà tale qualifica, ma non contiene informazioni riguardo i compiti assegnati e le istruzioni relative.

### **2.5. Incaricato del trattamento dei dati**

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.

Gli Incaricati del trattamento sono i soggetti che quotidianamente sono chiamati a rendere effettive le prescrizioni del D.Lgs. 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.

## **2.6. 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. 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 della Fondazione 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.

## **2.7. Responsabile della gestione e manutenzione degli strumenti elettronici**

È onere del Titolare del trattamento dei dati personali individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più Responsabili della gestione e della manutenzione degli strumenti elettronici.

Il Responsabile 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 Titolare, opportunamente firmata per ricevuta e da conservarsi agli atti.

È compito del Responsabile 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 o dell'Amministratore di sistema o dell'Incaricato alla custodia credenziali;
- ✓ 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 del trattamento 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.

## **2.8. Responsabile della custodia delle copie delle credenziali**

È onere del Titolare del trattamento individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più Responsabili della custodia delle copie delle credenziali.

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

È compito del Responsabile 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 Titolare (o qualora nominato del Responsabile) del trattamento dei dati personali, avvalendosi del supporto tecnico del responsabile della manutenzione degli strumenti elettronici;
- ✓ gestire e custodire, in luogo sicuro, le credenziali di ogni incaricato del trattamento necessarie per accedere ai dati, in busta chiusa con indicato il nome dell'incaricato datata e sigillata mediante firma dell'incaricato su tutti i lembi che dovrà essere conservata dal custode in luogo sicuro e non accessibile agli altri incaricati e ai terzi e sostituita con la prevista periodicità;
- ✓ assicurare che il Codice per l'identificazione, laddove sia stato già utilizzato, non sia assegnato ad altri Incaricati del trattamento, neppure in tempi diversi;
- ✓ dare agli incaricati del trattamento le istruzioni relative all'utilizzo delle password, alle caratteristiche che le stesse devono avere, nonché alle modalità da seguire per la loro modifica in autonomia;
- ✓ revocare tutte le credenziali che non vengano utilizzate nel caso in cui l'incaricato perda i diritti che gli consentivano di accedere ai dati personali;
- ✓ se le credenziali non vengano utilizzate per più di sei mesi, revocare, ai soggetti incaricati del trattamento, le credenziali necessarie per l'accesso ai dati;
- ✓ nel caso in cui il Titolare del trattamento abbia la necessità indifferibile di accedere ad un elaboratore in caso di prolungata assenza o impedimento dell'incaricato che lo utilizza abitualmente, consegnare al titolare stesso la busta contenente la parola chiave dell'elaboratore sul quale egli può intervenire unicamente per necessità di operatività e sicurezza del sistema informativo;
- ✓ informare tempestivamente l'incaricato del quale, in sua assenza, è stata consegnata la parola chiave al titolare del trattamento, affinché questi provveda immediatamente alla sostituzione della parola chiave, e farsela consegnare in una nuova busta chiusa.

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

## **2.9. Responsabile 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 Titolare del trattamento dei dati personali, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più Responsabili delle copie di sicurezza delle banche dati.

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

Il Responsabile 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 del trattamento dei dati personali stabilisce, con il supporto tecnico del Responsabile 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 il Responsabile 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 o il Responsabile 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.

È compito dei Responsabili 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 del trattamento 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 al Responsabile della gestione e della manutenzione degli strumenti elettronici o, qualora questa figura non fosse presente, al Titolare, ogni eventuale problema che dovesse verificarsi nella normale attività di copia delle banche dati.

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

## **2.10. Responsabile della custodia delle aree e dei locali**

In conformità a quanto disposto dal punto 19.4 del Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Dlgs. n.196 del 30 giugno 2003), il Titolare del trattamento dei dati personali, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più Responsabili 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 Responsabile deve essere consegnata la lettera di incarico redatta in duplice copia di cui una deve essere restituita al Titolare, opportunamente firmata per ricevuta e da conservarsi agli atti.

I Responsabili 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. Allo scopo sono da considerare autorizzati tutti i soggetti identificati nel Documento Programmatico sulla Sicurezza;
- ✓ Identificare e registrare le persone ammesse, a qualunque titolo, dopo l'orario di lavoro;
- ✓ 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 Titolare del trattamento dei dati personali ritenga di non nominare alcun Responsabile 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 del trattamento 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 del trattamento dei dati personali, avvalendosi della collaborazione del Responsabile della custodia delle copie delle credenziali e del Responsabile 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 della Fondazione o società non devono essere usati per scopi diversi da quelli della Fondazione. 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 effettuata 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 elaboratori 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 della Fondazione.

### **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 del trattamento 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 del trattamento dei dati personali, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento;
- ✓ Consegnare a persone non autorizzate dal Responsabile del trattamento 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.

### 3.4. Videosorveglianza

Il trattamento dei dati personali effettuato mediante l'uso di sistemi di videosorveglianza non forma oggetto di legislazione specifica; al riguardo si applicano, pertanto, le disposizioni generali in tema di protezione dei dati personali.

#### 3.4.1. Principi generali

La raccolta, la registrazione, la conservazione e, in generale, l'utilizzo di immagini configura un trattamento di dati personali (*art. 4, comma 1, lett. b), del Codice*). È considerato dato personale, infatti, qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione.

Le norme sulla privacy non vietano l'installazione di sistemi di videosorveglianza e di registrazioni di immagini ma richiedono che tali sistemi siano conformi al "Codice in materia di protezione dei dati personali" e rispettino, in generale, la privacy dei cittadini. Ciò significa che occorre sempre rispettare questi tre principi:

1. L'installazione di telecamere è lecita solo quando altre misure di sicurezza siano ritenute insufficienti o inattuabili.
2. L'eventuale registrazione e conservazione delle immagini deve essere limitata nel tempo.
3. I cittadini devono sapere sempre e comunque se un'area è sottoposta a videosorveglianza.

La videosorveglianza è utilizzata per molteplici scopi, alcuni dei quali possono essere raggruppati nei seguenti ambiti generali:

- ✓ protezione e incolumità degli individui, ivi ricompresi i profili attinenti alla sicurezza urbana, all'ordine e sicurezza pubblica, alla prevenzione, accertamento o repressione dei reati svolti dai soggetti pubblici, alla razionalizzazione e miglioramento dei servizi al pubblico volti anche ad accrescere la sicurezza degli utenti, nel quadro delle competenze ad essi attribuite dalla legge;
- ✓ protezione della proprietà;
- ✓ rilevazione, prevenzione e controllo delle infrazioni svolti dai soggetti pubblici, nel quadro delle competenze ad essi attribuite dalla legge;
- ✓ acquisizione di prove.

#### 3.4.2. Informativa

Gli interessati devono essere sempre informati che stanno per accedere in una zona videosorvegliata; ciò anche nei casi di eventi e in occasione di spettacoli pubblici (es. concerti, manifestazioni sportive).

A tal fine, il Garante ritiene che si possa utilizzare lo stesso modello semplificato di informativa "minima", indicante il titolare del trattamento e la finalità perseguita, già individuato ai sensi dell'art. 13, comma 3, del Codice nel provvedimento del 2004 e riportato in *fac-simile* nell'allegato n. 1 al provvedimento del Garante.

Il Garante, al fine di rafforzare la tutela dei diritti e delle libertà fondamentali degli interessati, ritiene fortemente auspicabile che l'informativa, benché non obbligatoria, laddove l'attività di videosorveglianza sia espletata ai sensi dell'art. 53 del Codice, sia comunque resa in tutti i casi nei

quali non ostante in concreto specifiche ragioni di tutela e sicurezza pubblica o di prevenzione, accertamento o repressione dei reati.

### **3.4.3. Misure di sicurezza**

I dati raccolti mediante sistemi di videosorveglianza devono essere protetti con idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini (artt. 31 e ss. del Codice).

Devono quindi essere adottate specifiche misure tecniche ed organizzative che consentano al titolare di verificare l'attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa (se soggetto distinto dal titolare medesimo, nel caso in cui questo sia persona fisica).

È inevitabile che, in considerazione dell'ampio spettro di utilizzazione di sistemi di videosorveglianza, anche in relazione ai soggetti e alle finalità perseguite nonché della varietà dei sistemi tecnologici utilizzati, le misure minime di sicurezza possano variare anche significativamente. È tuttavia necessario che le stesse siano quanto meno rispettose dei principi che seguono:

- ✓ in presenza di differenti competenze specificatamente attribuite ai singoli operatori devono essere configurati diversi livelli di visibilità e trattamento delle immagini. Laddove tecnicamente possibile, in base alle caratteristiche dei sistemi utilizzati, i predetti soggetti, designati incaricati o, eventualmente, responsabili del trattamento, devono essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza;
- ✓ laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, deve essere altresì attentamente limitata la possibilità, per i soggetti abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o duplicazione;
- ✓ per quanto riguarda il periodo di conservazione delle immagini devono essere predisposte misure tecniche od organizzative per la cancellazione, anche in forma automatica, delle registrazioni, allo scadere del termine previsto;
- ✓ nel caso di interventi derivanti da esigenze di manutenzione, occorre adottare specifiche cautele; in particolare, i soggetti preposti alle predette operazioni possono accedere alle immagini solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche ed in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini;
- ✓ qualora si utilizzino apparati di ripresa digitali connessi a reti informatiche, gli apparati medesimi devono essere protetti contro i rischi di accesso abusivo di cui all'art. 615-ter del codice penale;
- ✓ la trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza deve essere effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless (tecnologie *wi-fi*, *wi-max*, *Gprs*).

### **3.4.4. Responsabili e Incaricati**

Il titolare o il responsabile devono designare per iscritto tutte le persone fisiche, incaricate del trattamento, autorizzate sia ad accedere ai locali dove sono situate le postazioni di controllo, sia ad utilizzare gli impianti e, nei casi in cui sia indispensabile per gli scopi perseguiti, a visionare le immagini (*art. 30 del Codice*). Deve trattarsi di un numero delimitato di soggetti, specie quando il titolare si avvale di collaboratori esterni. Occorre altresì individuare diversi livelli di accesso in corrispondenza delle specifiche mansioni attribuite ad ogni singolo operatore, distinguendo coloro che sono unicamente abilitati a visionare le immagini dai soggetti che possono effettuare, a determinate condizioni, ulteriori operazioni (es. registrare, copiare, cancellare, spostare l'angolo visuale, modificare lo zoom, ecc.).

### **3.4.5. Durata della conservazione**

Nei casi in cui sia stato scelto un sistema che preveda la conservazione delle immagini, in applicazione del principio di proporzionalità (v. *art. 11, comma 1, lett. e), del Codice*), anche l'eventuale conservazione temporanea dei dati deve essere commisurata al tempo necessario, e predeterminato, a raggiungere la finalità perseguita.

La conservazione deve essere limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria. Solo in alcuni casi, per peculiari esigenze tecniche (mezzi di trasporto) o per la particolare rischiosità dell'attività svolta dal titolare del trattamento (ad esempio, per alcuni luoghi come le banche può risultare giustificata l'esigenza di identificare gli autori di un sopralluogo nei giorni precedenti una rapina), può ritenersi ammesso un tempo più ampio di conservazione dei dati che, sulla scorta anche del tempo massimo legislativamente posto per altri trattamenti, si ritiene non debba comunque superare la settimana.

Per i comuni e nelle sole ipotesi in cui l'attività di videosorveglianza sia finalizzata alla tutela della sicurezza urbana, il termine massimo di durata della conservazione dei dati è limitato "ai sette giorni successivi alla rilevazione delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza, fatte salve speciali esigenze di ulteriore conservazione".

### **3.4.6. Diritti degli interessati**

Deve essere assicurato agli interessati identificabili l'effettivo esercizio dei propri diritti in conformità al Codice, in particolare quello di accedere ai dati che li riguardano, di verificare le finalità, le modalità e la logica del trattamento (*art. 7 del Codice*).

In riferimento alle immagini registrate non è in concreto esercitabile il diritto di aggiornamento, rettificazione o integrazione in considerazione della natura intrinseca dei dati raccolti, in quanto si tratta di immagini raccolte in tempo reale riguardanti un fatto obiettivo (*art. 7, comma 3, lett. a), del Codice*). Viceversa, l'interessato ha diritto di ottenere il blocco dei dati qualora essi siano trattati in violazione di legge (*art. 7, comma 3, lett. b), del Codice*).

### **3.4.7. Prescrizioni e sanzioni**

Il Garante invita tutti i titolari dei trattamenti di dati personali effettuati tramite sistemi di videosorveglianza ad attenersi alle prescrizioni indicate nel presente provvedimento.

Le misure necessarie prescritte con il presente provvedimento devono essere osservate da tutti i titolari di trattamento. In caso contrario il trattamento dei dati è, a seconda dei casi, illecito oppure non corretto, ed espone:

- ✓ all'inutilizzabilità dei dati personali trattati in violazione della relativa disciplina (*art. 11, comma 2, del Codice*);
- ✓ all'adozione di provvedimenti di blocco o di divieto del trattamento disposti dal Garante (*art. 143, comma 1, lett. c), del Codice*), e di analoghe decisioni adottate dall'autorità giudiziaria civile e penale;
- ✓ all'applicazione delle pertinenti sanzioni amministrative o penali (*artt. 161 e ss. del Codice*)

## Capitolo 4. DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

### 4.1. Premessa

Obiettivo principale del Documento Programmatico sulla Sicurezza (DPS) è di fornire un resoconto dettagliato delle misure di sicurezza adottate dalla Fondazione 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 dalla Fondazione 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.

Nella tabella 19.1.a. è riportato l'elenco dei trattamenti svolti dalla Fondazione 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;
- ✓ Consenso obbligatorio: specifica se è necessario, per il trattamento in oggetto, fornire il consenso;
- ✓ 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 macrostruttura (direzione del personale) oppure uffici specifici (ufficio paghe, ufficio sviluppo risorse, ufficio controversie sindacali, ecc.);
- ✓ Altre strutture coinvolte nel trattamento: sono elencate le altre strutture della Fondazione che eventualmente concorrono allo svolgimento delle operazioni di trattamento dei dati personali;
- ✓ Fonte normativa: eventuali riferimenti a norme e leggi che autorizzano al trattamento dei dati;
- ✓ Rilevanti finalità di interesse pubblico:
- ✓ Descrizione: fornisce la descrizione estesa del trattamento;
- ✓ Contitolari del trattamento: elenca i soggetti esterni che, eventualmente, concorrono al trattamento in qualità di titolari;
- ✓ Finalità del trattamento: elenco delle eventuali finalità di interesse pubblico, se presenti;
- ✓ Natura dei dati: sono elencate dettagliatamente le caratteristiche del trattamento con riferimento alla natura dei dati trattati;
- ✓ Categorie interessate: sono elencate dettagliatamente le categorie degli interessati;
- ✓ Modalità di trattamento: sono elencate le modalità con le quali vengono esplicitati i trattamenti;
- ✓ Comunicazione e diffusione: sono elencate le categorie di soggetti o enti ai quali vengono comunicati i dati relativi ai trattamenti;
- ✓ Banche dati gestite: elenca le banche dati coinvolte nel trattamento.

Nella tabella 19.1.b. è riportato l'elenco dei trattamenti svolti all'esterno con altre informazioni aggiuntive rispetto al precedente allegato, tra le quali:

- ✓ Soggetto delegato: riporta tutte le indicazioni che riguardano il soggetto al quale sono state delegate le operazioni;
- ✓ 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.

La tabella 19.1.c. elenca le Banche dati 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 dalla Fondazione 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 le 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.

La tabella 19.1.d. 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 elettronico presente nella Fondazione 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;
- ✓ Sede ubicazione: riporta il nome della sede in cui è ubicato lo strumento elettronico;
- ✓ Indirizzo: riporta l'indirizzo della sede in cui è ubicato lo strumento elettronico;
- ✓ Ufficio: riporta il nome dell'ufficio in cui è ubicato lo strumento elettronico;
- ✓ Dettaglio ubicazione: riporta una descrizione dettagliata del luogo in cui è ubicato lo strumento elettronico;
- ✓ Banche dati gestite: riporta l'elenco delle banche dati gestite dallo strumento elettronico;
- ✓ Gestione dati sensibili: riporta la presenza o meno di dati sensibili gestiti dallo 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 modificabile;



- ✓ Connessioni presenti: indica la presenza ed il tipo di connessioni presenti nello strumento elettronico;
- ✓ Frequenza aggiornamento password: specifica la frequenza di aggiornamento della password (giornaliera, settimanale, ecc.);
- ✓ Frequenza aggiornamento antivirus: specifica la frequenza di aggiornamento dell'eventuale software antivirus installato (giornaliera, settimanale, ecc.);
- ✓ Utilizzatori abituali: specifica le persone che abitualmente utilizzano lo strumento elettronico;
- ✓ Software installati: specifica tutte le caratteristiche hardware ed i software installati.

La tabella 19.1.e. elenca gli strumenti non elettronici che sono utilizzati per le operazioni di trattamento svolte in modalità non informatizzata. Di ogni strumento non elettronico presente nella Fondazione sono indicate le seguenti caratteristiche:

- ✓ 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;
- ✓ Sede ubicazione: riporta il nome della sede in cui è ubicato lo strumento non elettronico;
- ✓ Indirizzo: riporta l'indirizzo della sede in cui è ubicato lo strumento non elettronico;
- ✓ Ufficio: riporta il nome dell'ufficio in cui è ubicato lo strumento non elettronico;
- ✓ Dettaglio ubicazione: riporta una descrizione dettagliata del luogo in cui è ubicato lo strumento non elettronico;
- ✓ Banche dati gestite: riporta l'elenco delle banche dati gestiti dallo strumento non elettronico.

La tabella 19.1.f. elenca le sedi che sono coinvolte 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;
- ✓ Descrizione: riporta una descrizione della sede;
- ✓ Sede principale: designa la funzione di sede principale oppure no;
- ✓ Indirizzo: riporta l'indirizzo della sede;
- ✓ Località: indica la località in cui è ubicata la sede;
- ✓ Recapiti: specifica i numeri di telefono e di fax della Fondazione;
- ✓ Modalità di accesso: specifica il tipo di accesso alla sede;
- ✓ Uffici: elenca gli uffici presenti nella sede.

La tabella 19.1.g. elenca gli uffici che sono coinvolti per le operazioni di trattamento. Di ogni ufficio sono indicate le seguenti caratteristiche:

- ✓ Ufficio: è il nome assegnato all'ufficio per permetterne l'identificazione;
- ✓ Sede appartenenza: riporta il nome della sede a cui l'ufficio appartiene;
- ✓ Descrizione: riporta una descrizione dell'ufficio;
- ✓ Piano: indica il piano dove è ubicato l'ufficio;
- ✓ Accesso: indica la possibilità di accesso o meno all'ufficio;
- ✓ Tipo chiusura: riporta il tipo di chiusura presente;
- ✓ Impianto antincendio: riporta la presenza o meno di un impianto antincendio;
- ✓ Sistema di allarme: riporta la presenza o meno di un sistema di allarme ed il tipo di sistema;



- ✓ Sistemi di protezione: riporta il tipo di protezione;
- ✓ Responsabili: vengono elencati i responsabili dell'ufficio;
- ✓ Soggetti autorizzati: vengono elencati i soggetti autorizzati all'accesso nell'ufficio.

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

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

La tabella 19.2.a. riporta l'elenco delle strutture coinvolte nelle operazioni di trattamento. Per ciascuna struttura elencata sono dettagliati i seguenti aspetti:

- ✓ Struttura della Fondazione: è il nome assegnato alla struttura per consentirne l'identificazione;
- ✓ Descrizione: riporta una descrizione della struttura;
- ✓ Uffici nei quali opera la struttura: elenca gli uffici nei quali opera la struttura della Fondazione;
- ✓ Trattamenti svolti: indica i trattamenti svolti nella struttura;
- ✓ Responsabili dei trattamenti: specifica i soggetti responsabili dei trattamenti svolti dalla struttura;
- ✓ Incaricati dei trattamenti: indica i soggetti incaricati dei trattamenti svolti dalla struttura;

La tabella 19.2.b. riporta per ogni soggetto l'elenco dei ruoli svolti. I ruoli elencati in questa tabella sono Responsabile trattamento, Incaricato del trattamento, Responsabile trattamento esterno, Responsabile trattamento esterno autonomo. Per ogni soggetto sono riportate le seguenti informazioni:

- ✓ Soggetto: riporta il nome del soggetto ed il ruolo svolto;
- ✓ Categoria (interno/esterno): indica se il soggetto è appartenente o meno all'organico interno della Fondazione;
- ✓ Strutture di appartenenza: riporta l'elenco delle strutture in cui il soggetto svolge un ruolo;
- ✓ Responsabile trattamento: riporta l'elenco dei trattamenti di cui il soggetto svolge mansioni di responsabile;
- ✓ Incaricato trattamento: riporta l'elenco dei trattamenti di cui il soggetto svolge mansioni di incaricato;
- ✓ Responsabile trattamento esterno: riporta l'elenco dei trattamenti esterni di cui il soggetto svolge mansioni di responsabile;
- ✓ Responsabile trattamento esterno autonomo: riporta l'elenco dei trattamenti di cui il soggetto svolge mansioni di responsabile esterno autonomo.

La tabella 19.2.c. riporta per ogni soggetto l'elenco di eventuali altri ruoli svolti. I ruoli elencati in questa tabella sono Amministratore di sistema, Responsabile manutenzione strumenti elettronici, Responsabile integrità dei dati, Responsabile custodia credenziali, Responsabile custodia locali, Responsabile pulizia locali.

#### **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.

Per ogni rischio presente sono elencate le seguenti informazioni:

- ✓ Evento rilevato: riporta il tipo di evento;
- ✓ Nome assegnato: riporta il nome assegnato al rischio;



- ✓ Descrizione: riporta una descrizione del rischio;
- ✓ Categoria dell'evento: indica la categoria di appartenenza del rischio;
- ✓ Contromisure adottabili: riporta l'elenco delle contromisure adottate per contrastare il rischio;
- ✓ Impatto sulla sicurezza dei dati: riporta i livelli di rilevanza e probabilità;

#### **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 dalla Fondazione;
- ✓ Eventi relativi al contesto fisico-ambientale: includono tutti quegli eventi (naturali o artificiali) connessi al contesto in cui opera la Fondazione (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  $p \times m$ . 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 nella Fondazione 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 la Fondazione quali, ad esempio, eventi distruttivi naturali, artificiali, dolosi o accidentali, guasti a sistemi complementari, ingressi non autorizzati, ecc.

### **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.

La tabella 19.4.a. riporta l'elenco delle misure di sicurezza. Per ogni misura corrispondente ad un dato rischio sono riportati i seguenti campi:

- ✓ Misura di sicurezza: è il nome assegnato alla misura di sicurezza per consentirne l'identificazione;
- ✓ 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 di sicurezza;



- ✓ Descrizione: riporta una descrizione sommaria dell'insieme di misure indicando tutti gli elementi ritenuti utili per una completa applicazione delle regole esposte;
- ✓ Elementi interessati: sono elencati tutti gli elementi interessati dalla misura di sicurezza (sedi, uffici, strumenti elettronici e non elettronici, banche dati e trattamenti);
- ✓ Contromisure in essere: sono elencate le misure già adottate dalla Fondazione 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 (tabella successiva 19.4.b.);
- ✓ Contromisure da adottare: sono elencate le misure da adottare per fronteggiare un dato rischio;

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 della Fondazione.

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.

La tabella 19.4.b. riporta l'elenco delle schede analitiche legate alle contromisure di sicurezza. Per ogni contromisura corrispondente ad un dato rischio sono riportati i seguenti campi:

- ✓ Contromisura: nome della contromisura;
- ✓ Appartenente a: nome della misura;
- ✓ Tipo (da adottare/in essere): specifica se la contromisura è stata adottata oppure no;
- ✓ Descrizione breve: breve descrizione;
- ✓ Descrizione: descrizione più dettagliata;
- ✓ Tipologia: indica la tipologia;
- ✓ Data compilazione: data di compilazione della scheda analitica;
- ✓ Data successiva revisione: data della revisione della scheda analitica;
- ✓ Autori: Riporta l'elenco dei soggetti autori della scheda analitica.

#### **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 alla Fondazione, per quel che riguarda le misure minime di sicurezza del trattamento dei dati personali e tra queste quelle previste per le copie di backup.

È necessario che il Titolare ed il Responsabile del trattamento dei dati personali prevedano 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 analizzate e consigliabile testare tutti gli strumenti informatici hardware e software dell'intero sistema informatico della Fondazione.



Per ogni banca dati sono riportate le seguenti informazioni:

- ✓ 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;
- ✓ Dati comuni: specifica se nella banca dati sono contenuti dati comuni;
- ✓ Dati sensibili o giudiziari: specifica se nella banca dati sono contenuti dati sensibili o giudiziari;
- ✓ Incaricato salvataggio: indica la persona che, all'interno della Fondazione, ha il compito di eseguire il salvataggio e/o di controllarne l'esito;
- ✓ Procedura salvataggio: contiene una approfondita descrizione di natura tecnica con le istruzioni operative delle procedure da seguire per il salvataggio periodico dei dati;
- ✓ Numero di copie: specifica il numero di copie di backup previste;
- ✓ Frequenza salvataggio: indica la frequenza (giornaliera, settimanale, ecc.) con la quale procedere all'esecuzione delle copie di backup dei dati;
- ✓ Ubicazione conservazione copie: specifica la sede e l'ufficio nel quale sono conservati i supporti di memorizzazione;
- ✓ 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;
- ✓ 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;
- ✓ Incaricati prove ripristino: indica i soggetti che, all'interno della Fondazione, hanno il compito di eseguire le prove di ripristino dei dati;
- ✓ Procedure 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 ripristino: indica la frequenza prevista (settimanale, mensile, ecc.) con la quale effettuare i test di efficacia delle procedure di ripristino dei dati adottate.

#### **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.

Per ogni intervento formativo sono riportate le voci specificate nel seguente elenco:

- ✓ Intervento formativo: è il nome assegnato al corso per permetterne l'identificazione;
- ✓ Classi di incarico: individua le classi omogenee di incarico a cui l'intervento è destinato e/o le tipologie di incaricati interessati;
- ✓ Ore previste: indica il numero di ore previste per il corso;
- ✓ Anno di svolgimento: indica l'anno di svolgimento del corso;
- ✓ Numero partecipanti: indica il numero di partecipanti;
- ✓ Partecipanti previsti: elenco dei partecipanti previsti per l'intervento formativo.
- ✓ Interessati da formare in interventi successivi: numero di interessati da formare nell'anno in corso;

#### **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. Per ogni trattamento affidato all'esterno vengono riportate le seguenti informazioni:

- ✓ Nome del trattamento: nome assegnato al trattamento;
- ✓ Descrizione sintetica: è una descrizione sintetica dell'attività delegata;
- ✓ 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 e il ruolo ricoperto agli effetti della disciplina sulla protezione dei dati personali;
- ✓ Rapporto contrattuale: riporta gli estremi contrattuali del rapporto in essere con la Fondazione;
- ✓ Attività delegata: è indicata la tipologia di attività affidata all'esterno;
- ✓ Descrizione attività delegata: è riportata una descrizione dell'attività affidata all'esterno;
- ✓ Indirizzo: riporta l'indirizzo completo;

- ✓ Località: riporta il nome della località;

#### **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.

Per ogni banca dati per i quali è prevista la cifratura dei dati, si riportano le informazioni essenziali:

- ✓ 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;
- ✓ Dati comuni: specifica se nel trattamento sono coinvolti dati comuni;
- ✓ Dati sensibili o giudiziari: specifica se nel trattamento sono coinvolti dati 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 la Fondazione 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.

Il Responsabile del trattamento ed i singoli incaricati sono tenuti a fornire le informative approvate dal Titolare del Trattamento.

Le informative possono essere fornite agli interessati anche dagli incaricati del Trattamento, con libertà di forme decise dai Responsabili. Particolare attenzione deve essere prestata ai moduli per ottenere il consenso degli interessati per il Trattamento dei dati sensibili. Tali moduli devono essere approvati dal Titolare del Trattamento.

Possono ricevere il consenso al Trattamento anche gli incaricati che provvedono alla elaborazione della documentazione ed alla conservazione della relativa modulistica secondo quanto previsto nelle istruzioni impartite loro.

### 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 (Modalità 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.

È da considerare che i soggetti pubblici, per poter trattare i dati personali, non necessitano di ottenere il previo consenso da parte degli interessati. La legge sulla privacy a tal proposito prevede due regimi di legittimazione diversi a seconda della natura dei soggetti titolari del Trattamento:

- a) **Soggetto privato:** se a procedere al Trattamento è un soggetto privato (cui sono equiparati gli enti pubblici economici), questo deve chiedere preliminarmente il consenso all'interessato, salvo i casi di esclusione espressamente previsti dal legislatore;
- b) **Soggetto pubblico:** per i soggetti pubblici, al contrario, vige il principio di finalità istituzionale (o secondo altri di competenza) ossia essi possono trattare solo i dati che sono necessari per lo svolgimento di funzioni istituzionali.

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.