GIUNTA REGIONALE DEL LAZIO

ESTRATTO DAL PROCESSO VERBALE DELLA SEDUTA DEL 29 NOV. 2004

ADDI' 29 NOV. 2004 NELLA SEDE DELLA REGIONE LAZIO, IN VIA CRISTOFORO COLOMBO, 212 ROMA, SI E' RIUNITA LA GIUNTA REGIONALE COSI' COSTITUITA:

STORACE	Francesco	Presidente	IANNARILLI	Antonello	Assessore
SIMEONI	Giorgio	Vice Presidente	PRESTAGIOVANNI	Bruno	"
AUGELLO	Andrea	Assessore	ROBILOTTA	Donato	"
CIARAMELLETTI	Luigi	"	SAPONARO	Francesco	"
CIOCCHETTI	Luciano	"	SARACENI	Vincenzo Maria	"
FORMISANO	Anna Teresa	"	VERZASCHI	Marco	"
GARGANO	Giulio	"			

ASSISTE IL SEGRETARIO Tommaso NARDINI

.....OMISSIS

ASSENTI: CIARAMELLETTI FORMISANO IANNARILLI SARACENI

DELIBERAZIONE N. - 1142 -

OGGETTO:

Approvazione delle Misure di sicurezza per il trattamento dei dati personali di cui all'articolo 34 del decreto legislativo 30 giugno 2003, n. 196 e successive modificazioni

GIUNTA REGIONALE DEL LAZIO SEGRETERIA REGIONE LAZIO

1142 29 NOV. 2004

OGGETTO: Approvazione delle Misure di sicurezza per il trattamento dei dati personali di cui all'articolo 34 del decreto legislativo 30 giugno 2003, n. 196 e successive modificazioni.

LA GIUNTA REGIONALE

SU PROPOSTA dell'Assessore al Personale, demanio, patrimonio e informatica;

VISTO il decreto legislativo 30 giugno 2003, n. 196 concernente "Codice in materia di protezione dei dati personali" e, in particolare:

1) l'articolo 34, il quale stabilisce che:
   - Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:
     a) autenticazione informatica;
     b) adozione di procedure di gestione delle credenziali di autenticazione;
     c) utilizzazione di un sistema di autorizzazione;
     d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
     e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
     f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
     g) tenuta di un aggiornato documento programmatico sulla sicurezza;
     h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.
2) l'articolo 35, il quale stabilisce che:
   - Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:
     a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
     b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
     c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

VISTA la legge regionale 18.2.2002, n. 6, e successive modifiche e integrazioni, concernente "Disciplina del sistema organizzativo della Giunta e del Consiglio e disposizioni relative alla dirigenza e al personale regionale";

VISTO il Regolamento Regionale 6.9.2002, n. 1, e successive modifiche e integrazioni, concernente "Regolamento di organizzazione degli uffici e dei servizi della Giunta regionale" e, in particolare, l'articolo 497 che detta disposizioni sulle Misure di sicurezza da adottare per la protezione dei dati presso le strutture della Giunta regionale;

VISTO il documento allegato, che forma parte integrante del presente atto, concernente "Misure di sicurezza per il trattamento dei dati personali presso le strutture della Giunta regionale del Lazio", redatto d'intesa tra l'Area "Coordinamento delle attività in materia di trattamento dei dati personali e gestione della banca dati dei procedimenti" della Direzione regionale "Organizzazione e personale" e l'Area "Innovazione tecnologica ed e-Governement" della Direzione regionale

1142 29 NOV. 2004

"Sistemi informativi e statistici – Provveditorato e patrimonio", entrambe del Dipartimento Istituzionale;

CONSIDERATO che il presente provvedimento non è soggetto alla procedura di concertazione con le parti sociali;

all'unanimità

DELIBERA

Di approvare il documento allegato, che forma parte integrante del presente atto, concernente "Misure di sicurezza per il trattamento dei dati personali presso le strutture della Giunta regionale del Lazio".

"Misure di sicurezza.doc"

IL PRESIDENTE: F.to Francesco STORACE
IL SEGRETARIO: F.to Tommaso Nardini

30 NOV. 2004

GIUNTA REGIONE LAZIO SEGRETERIA DELLA

DIPARTIMENTO ISTITUZIONALE
IL DIRETTORE
Dr. Alessandro RIDOLFI

Il presente documento è composto da n. 48 pagine

ALLEG. alla DELIB. N. 1142
DEL 20 NOV. 2004

SEGRETERIA DELLA GIUNTA REGIONE LAZIO

REGIONE LAZIO

Dipartimento "Istituzionale"

Direzione regionale "Organizzazione e personale"
Area "Coordinamento delle attività in materia di trattamento dei dati personali e gestione della banca dati dei procedimenti amministrativi"

Direzione regionale Sistemi informativi e statistici – provveditorato e patrimonio
Area "Innovazione tecnologica ed e-Governement"

MISURE DI SICUREZZA PER IL TRATTAMENTO DEI DATI PERSONALI PRESSO LE STRUTTURE DELLA GIUNTA REGIONALE DEL LAZIO

SOMMARIO

Sezione IV
Analisi del rischio e misure di sicurezza relative alle postazioni di lavoro

Sezione V
Analisi del rischio e misure di sicurezza relative ai PC portatili

Sezione VI
Analisi del rischio e misure di sicurezza relative ai supporti di memorizzazione

INTRODUZIONE

Il decreto legislativo 30.6.2003, n. 196 ("Codice in materia di protezione dei dati personali"), entrato in vigore il 1/1/2004, è il punto di arrivo di un percorso normativo iniziato con la legge 31 dicembre 1996, n. 675, "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali". Quest'ultima è stata la prima legge italiana di carattere generale sul trattamento dei dati personali a garanzia che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Il predetto provvedimento, sulla base dell'esperienza maturata in questi anni, riunisce in unico contesto la legge 675/1996 e gli altri decreti legislativi, regolamenti e codici deontologici che si sono succeduti e contiene anche importanti innovazioni tenendo conto della "giurisprudenza" del Garante e della normativa europea sulla riservatezza nelle comunicazioni elettroniche.

La Regione Lazio aveva già recepito nell'ordinamento regionale con la L.R. n. 6/2002 e con il R.R. n. 1/2002 le disposizioni della legge 675/1996. Si tratterà ora di adeguare tale normativa a quella del nuovo codice.

Il complesso di accorgimenti e cautele di tipo organizzativo e tecnologico che la pubblica amministrazione, a partire dal 1° gennaio 2004, deve improrogabilmente adottare al fine di evitare la dispersione, la perdita o l'uso illecito dei dati contenuti nei data base, rappresenta uno degli adempimenti più importanti da attuare per poter trattare i dati. La loro necessità è sottolineata dalla previsione delle sanzioni penali che si applicano pure nei casi di colpa, qualora non siano rispettati, anche in parte, gli standard previsti.

La normativa obbliga il titolare del trattamento dei dati personali della Regione Lazio ad adottare misure idonee ad evitare il danno, che consiste sia nell'accesso da parte di persone non legittimate a trattare dati personali soggetti a tutela, sia nella perdita o nel danneggiamento dei dati stessi.

L'Amministrazione regionale già adotta nelle singole strutture misure appropriate a tutelare i dati in suo possesso. Tuttavia, con il presente documento, si definisce:

1) un corpo organico di disposizioni in materia di sicurezza e tutela dei dati personali;
2) indicazioni pratiche in ordine alle varie misure (organizzative, procedurali, tecniche e logistiche) necessarie a garantire un idoneo livello di sicurezza dei dati contenuti nelle diverse e differenti banche dati gestite dall'Amministrazione regionale.

In proposito, preme sottolineare che le misure per la sicurezza e la protezione dei dati individuate con il presente documento non devono essere viste solo come un vincolo dal quale possono derivare una serie di sanzioni ma come un'occasione di crescita che consenta una maggiore trasparenza dei flussi di informazioni, la revisione delle attività svolte e delle procedure di gestione e il riordino degli archivi, ecc..

L'elaborazione del presente documento ha comportato la verifica delle misure di sicurezza già esistenti attraverso il monitoraggio delle modalità organizzative e l'aggiornamento costante a livello tecnologico.

Il documento prevede, tra l'altro, per i trattamenti informatizzati, l'adozione di un sistema di autenticazione informatica e di un sistema di autorizzazione che consenta l'accesso ai dati contenuti negli elaboratori e l'effettuazione delle operazioni automatizzate di trattamento sui dati stessi, solo a

coloro che ne hanno necessità in relazione alla mansione e che abbiano ricevuto formale autorizzazione. Misure queste che in alcuni casi sono state già adottate in precedenza ma che trovano nel presente documento una complessiva e omogenea applicazione.

Nello sviluppo di una cultura della protezione dei dati un ruolo fondamentale avrà la formazione del personale.

Il presente documento costituisce, pertanto, l'emanazione di una serie di disposizioni alle quali dovranno specificatamente attenersi i diversi attori, ognuno per la parte di rispettiva competenza, nello svolgimento delle attività istituzionali delle strutture organizzative della Giunta regionale.

Il presente documento costituisce, infine, una prima regolamentazione della materia ed è suscettibile di modifiche ed integrazioni sulla base dell'evoluzione del processo di realizzazione del Sistema Informativo dell'Ente, dell'innovazione tecnologia e delle osservazioni ed esperienze dell'utenza, oltre che dell'introduzione di nuove norme.

Il documento si articola in due Parti:

a) la Parte I, è dedicata alle disposizioni generali in materia di misure di sicurezza e alle figure previste dalla normativa sulla protezione dei dati personali;
b) la Parte II, individua le misure di sicurezza per il trattamento dei dati personali.

PARTE I

DISPOSIZIONI GENERALI

1. Finalità

Il presente documento definisce, ai sensi del decreto legislativo 30 giugno 2003, n. 196, le misure di sicurezza per il trattamento dei dati personali presso le strutture organizzative della Giunta regionale e i criteri organizzativi per la loro attuazione.

Per queste, si fa riferimento anche ai contenuti già esposti nelle direttive emanate nel tempo da Titolare.

In particolare, nel documento vengono definiti i criteri tecnici e organizzativi per:

a) l'autenticazione informatica per l'identificazione dell'incaricato;
b) l'adozione di procedure di gestione delle credenziali di autenticazione;
c) l'utilizzazione di un sistema di autorizzazione;
d) l'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
e) la protezione delle aree e dei locali interessati dalle misure di sicurezza, nonché le misure per controllare l'accesso ai locali medesimi;
f) la protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
g) l'adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
h) i criteri e le procedure per la sicurezza della trasmissione dei dati, ivi compresi quelli per le redazioni di accesso per via telematica;
i) l'adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari;
j) l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni;
k) la redazione e l'aggiornamento del Documento Programmatico sulla Sicurezza.

Le misure di sicurezza previste nel presente documento riguardano tutti i trattamenti di dati personali e si applicano al trattamento effettuato con strumenti elettronici di elaborazione o altri strumenti (cartacei, audio, visivi e audiovisivi, ecc...).

Nel presente documento si intende per:

a) "legge", il decreto legislativo 30 giugno 2003, n. 196;
b) "documento", le misure di sicurezza relative al trattamento dei dati individuate con il presente atto.

2. Definizioni

Ai sensi dell'articolo 4, comma 3, della legge, si intende per:

a) "**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 di distruzione e di perdita, anche accidentale, dei dati, nonché di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta dei dati stessi;

b) "**strumenti elettronici**", gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

c) "**autenticazione informatica**", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

d) "**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;

e) "**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;

f) "**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;

g) "**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;

h) **"intranet"**, l'estensione, geograficamente localizzata, della rete della Regione Lazio che utilizza le stesse caratteristiche di internet, protetta mediante i sistemi definiti nel presente documento;

i) **"extranet"**, parte della intranet della Regione Lazio, geograficamente distante, estesa ad utenti, anche esterni, selezionati, in maniera protetta, mediante i sistemi d'interconnessione definiti nel presente documento.

3. Figure previste dalla normativa a protezione dei dati personali

Nell'ambito della Regione Lazio l'applicazione della legge comporta l'attribuzione, in capo ai soggetti contemplati dall'ordinamento della stessa, di compiti e responsabilità propri delle seguenti figure:

- titolare del trattamento;
- responsabile del trattamento;
- incaricato del trattamento;
- altri soggetti.

3.1. Titolare

Il Titolare del trattamento dei dati personali contenuti nelle banche dati automatizzate o cartacee è la Regione Lazio. I compiti previsti in capo al titolare dalla legge sono affidati, ai sensi dell'articolo 477 del Regolamento Regionale n. 1/2002, al Direttore del Dipartimento Istituzionale il quale si avvale di una specifica struttura della direzione regionale "Organizzazione e personale" per il coordinamento delle attività in materia di trattamento dei dati personali.

Al titolare compete, in particolare:

a) la definizione dell'impianto organizzativo in materia di protezione dei dati personali;

b) la nomina dei responsabili dei trattamenti dei dati personali, e delle relative banche dati che li contengono, e la formulazione delle relative istruzioni, di cui all'articolo 477, comma 3, del R.R. 1/2002;

c) l'emanazione di disposizioni di sicurezza e salvaguardia dell'integrità dei dati;

d) l'adozione delle decisioni in ordine alle finalità del trattamento;

e) la definizione di linee strategiche per il trattamento;

f) la determinazione di direttive relative alle modalità del trattamento, costituenti le istruzioni impartite dal titolare al responsabile del trattamento;
g) la determinazione delle misure generali di sicurezza per il trattamento dei dati personali, in conformità con quanto disposto dagli articolo da 31 a 36 e dall'allegato "B" alla legge;
h) la pianificazione degli interventi di adeguamento;
i) la notificazione al Garante ai sensi dell'articolo 37 della legge, e tutte le altre comunicazioni e notificazioni al Garante, ove previste;
j) la cessazione del trattamento dei dati;
k) la redazione e l'aggiornamento del Documento Programmatico sulla Sicurezza.

3.2. I responsabili interni

I responsabili dei trattamenti dei dati personali contenuti nelle banche dati gestite dall'Amministrazione sono stati individuati nei Direttori delle Direzioni regionali, per le strutture sott'ordinate, e nei Direttori di Dipartimento, per le strutture di staff. I responsabili sono stati nominati con provvedimento del Titolare.

Il responsabile è preposto alla gestione e tutela dei dati personali nonché alla salvaguardia della integrità e della sicurezza degli stessi.

Il responsabile, conformemente alle istruzioni impartite dal titolare:
a) attua le misure di sicurezza indicate con il presente documento ed eventualmente con altri predisposti dall'Amministrazione;
b) assicura la funzionalità di tutte le operazioni di trattamento dei dati;
c) individua e nomina gli incaricati del trattamento dei dati, gli incaricati della custodia delle chiavi di accesso ai locali server, gli incaricati della custodia delle password, gli incaricati del backup, gli incaricati della verifica delle registrazioni degli accessi;
d) mantiene aggiornata una lista degli incaricati del trattamento
e) approva per ciascun incaricato il profilo iniziale di accesso assegnato e le variazioni necessarie per mantenerlo aggiornato alle esigenze della mansione
f) verifica con cadenza almeno annuale che i profili di accesso assegnati agli incaricati siano adeguati e non eccedenti le esigenze della mansione
g) impartisce agli incaricati le istruzioni per la corretta elaborazione dei dati personali;
h) procede alle verifiche sulla metodologia di introduzione e di gestione dei dati, applicata attraverso controlli a campione da eseguirsi periodicamente;
i) provvede alla rettifica dei dati e sulle richieste di cui all'articolo 497 del R.R. 1/2002;
j) impartisce disposizioni operative per la sicurezza delle banche dati e dei procedimenti di gestione e/o trattamento degli stessi;
k) cura la relazione delle singole banche dati, cui sovrintende, con la struttura competente in materia di informatica;
l) cura l'informazione agli interessati relativa al trattamento dei dati e alla loro comunicazione e diffusione;
m) dispone motivatamente il blocco dei dati, qualora sia necessaria una sospensione temporanea delle operazioni del trattamento, dandone tempestiva comunicazione al titolare;
n) informa il titolare di ogni questione rilevante ai fini della legge;
o) aggiorna la struttura di coordinamento in relazione ad eventuali nuovi trattamenti di dati personali intrapresi;
p) distrugge i dati personali alla cessazione del trattamento degli stessi, provvedendo alle formalità di legge e dandone comunicazione alla struttura di coordinamento;

q) predispone, entro il 31 dicembre di ciascun anno, un rapporto scritto in merito agli adempimenti eseguiti ai fini della legge ed alle conseguenti risultanze, da trasmettere al titolare;
r) gestisce tempestivamente e, comunque, non oltre tre giorni successivi al loro ricevimento, i reclami degli interessati e le eventuali istanze del Garante;
s) collabora con il Titolare alla redazione del Documento Programmatico sulla Sicurezza.

3.3. I responsabili esterni

Le disposizioni previste nel presente documento si applicano anche alle società ed ai collaboratori esterni dell'Amministrazione regionale che, nell'ambito dei compiti loro affidati dalla Regione, devono procedere al trattamento di dati personali in qualità di responsabili o incaricati del trattamento, come formalmente designati dall'Amministrazione regionale e che utilizzino, per lo svolgimento dei propri compiti, dotazioni informatiche e non informatiche regionali.

3.4. Gli incaricati del trattamento dei dati

Gli incaricati del trattamento dei dati personali, designati per iscritto dal responsabile, sono i soggetti che effettuano materialmente le operazioni di trattamento.

Gli incaricati, in particolare, dovranno:
a) procedere alla raccolta di dati personali, anche mediante appositi moduli di raccolta;
b) consegnare agli interessati, al momento della raccolta dei dati, il modulo contenente l'informativa di cui all'articolo 13 della legge, salvo che l'informativa medesima sia stata fornita direttamente dal titolare o dal responsabile;
c) raccogliere, se previsto, al momento della raccolta dei dati, il consenso espresso, documentato per iscritto, degli interessati ai trattamenti previsti, salvo che a ciò abbiano provveduto direttamente il titolare o il responsabile, e salvo i casi di esonero previsti dalla stessa legge;
d) trattare i dati personali nella misura necessaria e sufficiente alle finalità proprie della banca dati nella quale vengono inseriti;
e) adottare, nel trattamento dei dati, tutte le misure di sicurezza che siano indicate, oggi o in futuro, dal titolare o dal responsabile. In particolare dovrà, come di seguito precisato,:
- per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su terminali altrui e/o di lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
- trattare i soli dati la cui conoscenza sia necessaria per lo svolgimento delle operazioni da effettuare;
- conservare i supporti informatici e/o cartacei contenenti i dati personali in modo da evitare che detti documenti siano accessibili a persone non autorizzate al trattamento dei dati medesimi;
- con specifico riferimento agli atti e documenti cartacei contenenti dati personali ed alle loro copie, restituire gli stessi al termine delle operazioni affidate;
- riporre e conservare gli atti e i documenti cartacei contenenti dati personali e loro copie sotto chiave in caso di allontanamento anche temporaneo dal posto di lavoro;
- utilizzare i supporti di memorizzazione usati solamente qualora i dati in essi precedentemente contenuti non siano in alcun modo recuperabili, altrimenti etichettarli e riporli negli appositi contenitori;
- copie di dati personali su supporti amovibili sono permesse solo se parte del trattamento; copie di dati sensibili devono essere espressamente autorizzate dal responsabile del trattamento. In

ogni caso tali supporti devono avere un'etichetta che li identifichi e non devono mai essere lasciati incustoditi;
- in ogni caso si constati o si sospetti un incidente di sicurezza deve essere data immediata comunicazione al responsabile del trattamento;
- qualora l'incaricato decida di proteggere il personal computer a lui affidato mediante l'attivazione della password di accensione, dovrà curarne la conservazione in luogo sicuro e protetto affinché la stessa non sia accessibile a terzi non autorizzati, pur restando nella disponibilità della propria linea manageriale;

f) segnalare al titolare o al responsabile eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle predette misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita , anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;

g) effettuare la comunicazione e la diffusione dei dati esclusivamente ai soggetti indicati dal titolare o dal responsabile e secondo le modalità stabilite dai medesimi;

h) mantenere, salvo quanto precisato al punto precedente, la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento dell'attività, per tutta la durata della medesima ed anche successivamente al termine di essa;

i) svolgere, in ogni caso, il trattamento dei dati personali per le finalità e secondo le modalità stabilite dal titolare e dal responsabile e, comunque, in modo lecito e secondo correttezza;

l) fornire al titolare o al responsabile, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire loro di svolgere efficacemente la propria attività di controllo;

m) in generale, prestare la più ampia e completa collaborazione al titolare ed al responsabile al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'attività nel rispetto della normativa vigente.

3.5. Altri soggetti

Per l'attuazione delle misure minime di sicurezza definite dalla legge sono individuati, inoltre, i seguenti soggetti:
- incaricati della custodia delle chiavi;
- incaricati del backup;
- incaricati della verifica degli accessi.

3.5.1. Gli incaricati della custodia delle chiavi

Gli incaricati della custodia delle chiavi sono i soggetti che custodiscono le chiavi c/o i dispositivi di accesso ai locali dove sono collocati i server od altre attrezzature contenenti dati.

Gli incaricati della custodia delle chiavi sono individuati dal/i responsabile/i del/i trattamento/i dei dati, previa verifica della dislocazione delle apparecchiature e dei servizi informatici utilizzati.

Gli incaricati della custodia delle chiavi, designati per iscritto dal/i responsabile/i del/i trattamento/i dei dati, devono adempiere ai loro compiti attenendosi alle istruzioni ricevute dal responsabile/i e nel rispetto delle indicazioni relative alle norme di sicurezza definite nel presente documento.

Gli incaricati della custodia delle chiavi, in particolare, dovranno:

a) custodire le chiavi di accesso e/o i dispositivi di accesso ai locali server in un luogo non accessibile da altri;
b) aprire i locali per necessità di gestione e manutenzione dei sistemi, dei locali e degli impianti, nonché per attività di pulizia ed affini ed altre attività comunque indispensabili;
c) annotare, su apposito registro, anche informatico, conservato nei locali server, ogni intervento indicando data e orario dell'intervento (inizio-fine), tipo di intervento, nome e cognome del tecnico intervenuto, Ditta o struttura, firma;
d) provvedere alla chiusura dei locali al termine degli interventi di cui alla lettera b).

3.5.2. Gli incaricati del backup

Gli incaricati del backup sono i soggetti che sovrintendono alle operazioni di salvataggio, anche automatico, dei dati contro il rischio di perdita dei dati stessi custoditi sui server e su altre attrezzature.

Gli incaricati del backup sono individuati dal/i responsabile/i del/i trattamento/i dei dati previa verifica della dislocazione delle apparecchiature e dei servizi informatici utilizzati.

Gli incaricati del backup, designati per iscritto dal/i responsabile/i del/i trattamento/i dei dati, devono adempiere ai loro compiti attenendosi alle istruzioni ricevute dal/i responsabile/i e dal Direttore della Direzione regionale competente in materia di informatica nel rispetto delle indicazioni relative alle norme di sicurezza definite nel presente documento.

Gli incaricati del backup, in particolare, dovranno:
a) controllare, giornalmente tramite apposita procedura predefinita l'esito del backup giornaliero;
b) riferire, in caso di esito negativo del backup, al responsabile del trattamento;
c) sostituire ogni mattina, sul sistema server, il supporto magnetico contenente i dati di backup del giorno precedente con quello etichettato con il nome del giorno in corso;
d) collocare il supporto magnetico contenente i dati di backup del giorno precedente in un luogo diverso da quello in cui sono posti i server in armadi ignifughi chiusi a chiave o in altro sito protetto; l'accesso a tali luoghi deve essere registrato ed è consentito al solo personale autorizzato e deve essere protetto con misure di sicurezza fisiche e/o logiche non minori di quelle adottate per il server;
e) ripristinare i dati in caso di necessità secondo le modalità predisposte dal responsabile del trattamento.

3.5.3. Gli incaricati della verifica degli accessi

Gli incaricati della verifica degli accessi sono i soggetti che controllano costantemente, o con cadenza programmata, la conformità degli accessi ai sistemi , alle attrezzature informatiche ed alle banche dati con i profili, le autenticazioni e le autorizzazioni assegnate.

Gli incaricati della verifica degli accessi sono individuati dal/i responsabile/i del/i trattamento/i dei dati previa verifica della dislocazione delle apparecchiature e dei servizi informatici utilizzati.

Gli incaricati della verifica degli accessi, designati per iscritto dal/i responsabile/i del/i trattamento/i dei dati, devono adempiere ai loro compiti attenendosi alle istruzioni ricevute dal responsabile/i nel rispetto delle indicazioni relative alle norme di sicurezza definite nel presente documento.

Gli incaricati della verifica degli accessi, in particolare, dovranno:

a) controllare la compatibilità delle autenticazioni effettuate con le disposizioni impartite;
b) verificare l'aggiornamento dei profili e delle autorizzazioni
c) segnalare i tentativi di autenticazione falliti, a medio e lungo termine
d) monitorare gli accessi alla rete mediante appositi strumenti
e) controllare i livelli di traffico sulla rete identificandone e segnalandone le provenienze

3.6. Direttore della Direzione regionale competente in materia di informatica

Il Direttore della Direzione regionale competente in materia di informatica è il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione.

Spetta al Direttore della Direzione regionale competente in materia di informatica:

- individuare specifiche istruzioni tecniche a garanzia della sicurezza, ad integrazione e chiarimento di quelle stabilite nel presente documento, nonché la verifica delle stesse nel corso della gestione (art. 484 del R.R. 1/2002);
- assistere tecnicamente le strutture in ordine all'applicazione delle misure di sicurezza per il trattamento dei dati personali (art. 484 del R.R. 1/2002);
- coordinare i rapporti con il concessionario del sistema informatico (art. 484 del R.R. 1/2002);

3.7. Concessionario della gestione del sistema informativo

La gestione del sistema informatico regionale è stata affidata dalla Giunta regionale alla Laziomatica S.p.a.

La predetta società è autorizzata a trattare i dati personali detenuti dall'amministrazione regionale in qualità di responsabile esterno.

4. Identificazione dei beni da proteggere

Il Titolare del trattamento dei dati - d'intesa con i Responsabili del trattamento dei dati e con il Direttore della Direzione regionale competente in materia di informatica – elabora ed aggiorna costantemente un elenco di tutte le risorse hardware, delle relative risorse software e delle banche dati, nonché della loro locazione fisica e dei relativi assegnatari.

Di tale elenco è conservata copia presso il Titolare e copia presso la Direzione regionale competente in materia di informatica.

4.1. Risorse hardware

Rientrano in questa categoria tutte le attrezzature informatiche hardware singole o composite quali personal computer, terminali, server, stampanti, disk drive, linee di comunicazione dati, rete interna, dispositivi di backup dei dati.

4.2. Risorse software

Rientrano in questa categoria: Sistemi operativi e software di base, software applicativi, gestori di base di dati, software di rete, programmi in formato sorgente e oggetto.

4.3. Banche dati

Si intende ogni informazione o singolo dato contenuto negli archivi informatizzati e non informatizzati comunque organizzato, suddiviso o contenuto in basi di dati, dati di transito, copie storiche, file di log.

4.4. Supporti di memorizzazione

Si intendono per supporti di memorizzazione i dischi, nastri e altri a lettura ottica, magnetica magneto-ottica, elettronica e altri su cui vengono tenute le copie permanenti dei software installati, le copie dei file di log e i backup.

4.5. Documentazione cartacea

Si intende appartenente a questa categoria ogni rappresentazione, formata su carta, del contenuto di atti, anche interni delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività amministrativa.

PARTE II

MISURE DI SICUREZZA

Capo I

Sicurezza dei dati e dei sistemi

5. Disposizioni generali

La sicurezza deve essere considerata da tutti gli utenti una componente integrante dell'attività quotidiana finalizzata alla protezione delle informazioni e delle apparecchiature da manomissioni, uso improprio o distruzione.

La normativa obbliga il titolare del trattamento ad adottare misure idonee ad evitare il danno, che può consistere sia nell'accesso da parte di persone non legittimate a trattare dati personali, sia nella perdita o nel danneggiamento dei dati stessi.

Le misure di sicurezza, pertanto, sono costituite dal complesso delle misure organizzative, tecniche, informatiche, logistiche e procedurali volte a ridurre al minimo i rischi di:

- distruzione o perdita, anche accidentale, dei dati;
- accesso non autorizzato;
- trattamento non consentito o non conforme alle finalità della raccolta;
- modifica dei dati in conseguenza di interventi non autorizzati o non conformi alla regole.

Ai sensi dell'art. 31 della legge, le misure di sicurezza adottate per il trattamento dei dati personali devono essere:

- adeguate in relazione alle conoscenze acquisite in base al progresso tecnico e tali da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati o di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- adottate in via preventiva e differenziate in base alla natura dei dati e alle specifiche caratteristiche del trattamento.

Il Titolare del trattamento, pertanto, deve individuare preventive e idonee misure di sicurezza che devono almeno rispettare i parametri di sicurezza minimi dettati dalla legge (allegato "B" della legge).

Poiché il parametro previsto dalla legge è quello dell'idoneità delle misure minime necessarie ad evitare il danno, le misure di sicurezza elencate nel presente documento non rappresentano una limitazione all'adozione da parte dei responsabili di ulteriori misure idonee a garantire livelli di protezione maggiori e più adeguati alle singole situazioni.

Infine, va ricordato che le regole concernenti le misure di sicurezza individuate nel presente documento servono anche ad indirizzare il personale ad un utilizzo corretto delle dotazioni informatiche dell'amministrazione, anche ai fini della salvaguardia del patrimonio tecnologico ed informativo della stessa. Infatti tra le finalità implicite della legge sulla tutela dei dati personali vi è anche il perseguimento di un processo di crescita culturale del personale.

La legge distingue tra:

- trattamenti effettuati con strumenti elettronici;
- trattamenti effettuati con strumenti diversi da quelli elettronici

Capo II

Trattamenti effettuati con strumenti elettronici

Sezione I

Analisi del rischio e misure di sicurezza relative ai server

6. Misure di sicurezza organizzative

I dati personali per cui la legge richiede la tutela con misure idonee vengono memorizzati, nella maggior parte dei casi, sui server di rete. Per questo motivo va riservata una particolare attenzione alle misure di sicurezza e di protezione relative ai server.

Il responsabile del trattamento dei dati - d'intesa con il Direttore della Direzione regionale competente in materia di informatica – verifica anteriormente all'inizio del trattamento:

- che la configurazione e l'utilizzo delle risorse presenti sul server di rete della propria struttura sia funzionale alle esigenze di riservatezza delle banche dati contenenti dati personali;
- che la configurazione e l'utilizzo delle risorse di rete sia conforme all'impostazione di cui alla successiva *Sezione II "Analisi del rischio e misure di sicurezza relative alle risorse di rete e ai*

PC" del presente *Capo*, disponendo l'accesso differenziato attraverso il sistema di autenticazione informatica e il sistema di autorizzazione (vedasi paragrafo 15.2*)*.

7. Misure di sicurezza logistiche

Per un'adeguata collocazione dei server, devono essere adottate le misure logistiche illustrate nei paragrafi seguenti, idonee a garantire la protezione delle apparecchiature rispetto ai seguenti rischi:

- accesso fisico o logico non autorizzato;
- distruzione o perdita dei dati dovuta ad eventi fisici.

Il Direttore della Direzione regionale competente in materia di informatica e i tecnici che hanno accesso ai locali server devono informare il/i responsabile/i del/i trattamento/i nel caso in cui riscontrino il mancato rispetto delle misure di sicurezza logistiche qui elencate (ad esempio locali server lasciati aperti o mancata custodia delle chiavi degli stessi).

7.1. Protezione del server da accesso fisico non autorizzato

Per tutelare la riservatezza dei dati personali accessibili sul server e per proteggere l'efficienza delle apparecchiature, l'accesso ai locali in cui vi siano uno o più sistemi server è limitato nel seguente modo:

- le apparecchiature server devono essere poste in apposite stanze, destinate a contenere soltanto il server stesso ed eventualmente le apparecchiature di rete;
- ove sia logisticamente difficoltosa l'ubicazione del server in un apposito locale e per le strutture esistenti che non rispondono ai requisiti di cui al punto precedente, il responsabile del trattamento concorda con il Direttore della Direzione regionale competente in materia di informatica soluzioni organizzative alternative (es. armadi chiusi e appositamente allestiti) che offrano le medesime garanzie di sicurezza;
- se il locale è situato in una posizione tale da rendere agevole un'intrusione dall'esterno è necessario munirlo della protezione adeguata quale ad esempio l'apposizione di barre anti intrusione alle finestre;
- l'accesso ai locali server deve essere protetto tramite la chiusura a chiave del locale;
- la chiave va custodita da personale incaricato della custodia dal responsabile del trattamento;
- il personale incaricato della custodia delle chiavi è tenuto a riporle in un luogo non accessibile da altri.

7.1.1. Accesso di personale interno della struttura

Possono accedere ai locali in cui sono presenti uno o più server, secondo le modalità previste nel presente documento e per i fini previsti dalla legge :

- il Direttore della Direzione regionale competente in materia di informatica o il Dirigente della struttura interna da questi incaricato;
- il responsabile del trattamento;
- il custode delle chiavi;
- il personale della struttura che deve accedervi per l'espletamento dei compiti propri, per le necessità di gestione e manutenzione dei sistemi, dei locali e degli impianti nonché per attività di pulizia ed affini ed altre attività comunque indispensabili.
- gli incaricati della registrazione degli accessi

7.1.2. Accesso di personale esterno alla struttura

Gli interventi di manutenzione o adeguamento sui server, sui locali che li contengono e sui relativi impianti, sono richiesti o comunque autorizzati dal Direttore della Direzione regionale competente in materia di informatica o dal responsabile del trattamento dei dati. Quando, per l'espletamento di compiti di servizio e per altre attività, è necessario consentire l'accesso a personale esterno o a personale dipendente della Regione non appartenente alla struttura, vanno osservate le seguenti misure:

- il locale viene aperto dal personale custode delle chiavi;
- ciascun intervento è annotato su un apposito registro conservato nella stanza del server recante data e orario dell'intervento (inizio-fine), descrizione dell'intervento con attestazione di conformità in caso di interventi di sicurezza, nome e cognome del tecnico intervenuto, Ditta o Struttura, firma;
- al termine dell'intervento, l'incaricato della custodia della chiave provvede alla chiusura dei locali;
- nessun soggetto estraneo può accedere ai sistemi server se non accompagnato dal personale indicato nel precedente punto 7.1.1 "Accesso del personale interno della struttura".

7.1.3. Accesso di personale esterno alla struttura per servizi di pulizie o simili

Poiché non sussiste la necessità di effettuare quotidianamente le operazioni di pulizia nella stanza contenente il server; le giornate in cui il personale addetto alle pulizie accede alla medesima vanno programmate, anche al fine dell'apertura del locale.

Le operazioni di pulizia devono svolgersi quando è presente il personale addetto alla custodia della chiave, che provvede personalmente all'apertura;
Infine, gli accessi sono registrati nell'apposito registro di cui sopra.

7.2. Protezione dei dati dal rischio di perdita dovuta ad eventi fisici

Tra gli eventi fisici che possono portare alla perdita dei dati per distruzione delle apparecchiature vengono considerati:

a) incendio;
b) surriscaldamento delle apparecchiature;
c) anomalie di alimentazione elettrica;
d) altri eventi (allagamenti, crolli ecc.).

7.2.1. Misure per il rischio di incendio

Contro l'eventualità che un incendio nei locali in cui sono custoditi i sistemi server possa causare danni irreversibili ai dati sono necessarie le seguenti misure di sicurezza:

- in prossimità del server deve essere installato un dispositivo antincendio con rilevatore fumi e allarme acustico;
- le cassette di backup devono essere conservate in un armadio ignifugo, chiuso a chiave, dislocato in un locale diverso da quello che ospita il server.

7.2.2. Misure per il rischio di surriscaldamento delle apparecchiature

Contro l'eventualità del surriscaldamento delle apparecchiature, con il conseguente rischio di incendio e di danneggiamento dei dati è necessario:

- installare le apparecchiature in locali dotati di un idoneo impianto di condizionamento.

7.2.3. Misure per il rischio di anomalie nell'alimentazione elettrica

Contro l'eventualità che anomalie dell'alimentazione elettrica dei sistemi server possano danneggiare i dati memorizzati è necessario predisporre un collegamento ad un gruppo statico di continuità.

7.2.4. Misure per il rischio di altri eventi (allagamenti)

Occorre evitare la collocazione dei server in locali scantinati o seminterrati (a rischio allagamenti). Qualora indispensabile, i locali devono essere dotati di un sistema di rilevamento di allagamento connesso a un sistema di allarme.

8. Misure di sicurezza tecniche, informatiche e procedurali

La sicurezza dei server deve essere tutelata con le misure tecniche, informatiche e procedurali idonee a garantire la protezione delle apparecchiature rispetto ai seguenti rischi:

- accesso logico non autorizzato o non conforme alle regole;
- distruzione o perdita dei dati dovuta ad attacchi esterni (es.: virus);
- distruzione o perdita dei dati dovuta ad attacchi di malintenzionati;
- perdita dei dati.

8.1. Protezione da accessi logici non autorizzati

Per accesso logico, nel contesto di questo documento, si intende l'accesso ai dati contenuti sul server attraverso la rete telematica nella quale il server è inserito. La protezione è attuata mediante l'utilizzo di credenziali di autenticazione con le modalità previste nel successivo paragrafo 15.2.

8.2. Protezione dai virus

I virus sono particolari programmi predisposti per essere eseguiti all'insaputa dell'utente che possono causare danni ai dati memorizzati sul computer o al sistema operativo del computer stesso.

Sui sistemi utilizzati presso l'amministrazione regionale il Direttore della Direzione regionale competente in materia di informatica provvede ad installare e a mantenere un software antivirus costantemente aggiornato via intranet che garantisca una protezione idonea ad evitare il verificarsi di danni ai dati causati dai virus informatici.

8.3. Protezione da malintenzionati

Ogni computer collegato in rete può essere soggetto a tentativi di connessione effettuati da utenti che utilizzano altri computer collegati alla rete Internet. Per fare fronte a questo rischio i server sono collegati alla rete Internet attraverso la rete telematica locale che è protetta mediante firewall dalla distruzione o perdita dei dati dovuta ad attacchi di malintenzionati che agiscono collegandosi dall'esterno.

8.4. Protezione dal rischio di perdita dei dati

Per ovviare al rischio di perdita dei dati sui server dovrà essere presente un sistema di salvataggio automatico degli stessi.

Il salvataggio automatico:

- garantisce il recupero dei dati a fronte di guasti hardware o software, limitando i disagi connessi con la discontinuità del servizio;
- consente di recuperare dati o file accidentalmente eliminati o erroneamente modificati.

8.4.1. Il salvataggio dei dati (backup)

La Direzione regionale, competente in materia di informatica, dovrà individuare le banche dati e gli archivi da sottoporre alle politiche di salvataggio.

La migliore efficacia delle misure di salvataggio è garantita se sono mantenute:

- l'indipendenza dei dati dall'hardware, dai sistemi operativi, dalle applicazioni e dall'ambiente software;
- le logiche d'aggregazione degli archivi, le relazioni esistenti tra gli stessi e tra i singoli dati, gli indici, nonché le decodifiche dei dati non espliciti.
- le documentazioni tecniche necessarie per l'utilizzo dei dati e delle procedure di ricostruzione degli archivi.

E', quindi, necessario che, contestualmente ai dati, vengano salvate le documentazioni e le procedure di ricostruzione degli archivi, le procedure di ricostruzione delle relazioni e delle aggregazioni, nonché le codifiche.

Inoltre, la validità delle archiviazioni contenenti oggetti che includono dati o dati legati ad oggetti è garantita dal rigoroso mantenimento di tutte componenti software. Pertanto, alle procedure di salvataggio dei dati dovranno seguire le procedure di salvataggio degli oggetti, delle applicazioni o programmi e sistemi sovrastanti, con le stesse precauzioni e frequenze.

Un significativo incremento dell'efficacia delle misure di salvataggio può essere raggiunto:

a) corredando gli archivi con documenti, prodotti mediante strumenti, linguaggi e/o sistemi di tipo cross system/platform, universalmente riconosciuti da organismi di standardizzazione, che ne modellizzino e rappresentino la struttura, le componenti e le relazioni (analisi funzionale, ecc...);
b) allegando agli archivi o inglobandoli all'interno di programmi "auto esplodenti" i cui linguaggi siano indipendenti dalla piattaforma hardware e dal sistema operativo ospite o che risultino eseguibili sui sistemi operativi e sulle piattaforme maggiormente diffusi.

Il salvataggio di tutti gli archivi dovrà essere effettuato mediante codifica ASCII (8 bit) code page (secondo necessità). Qualora i sistemi non adottassero tale codifica (es: EBCDIC) , una delle due copie, previste nei punti successivi, dovrà essere tradotta. I responsabili del trattamento, per il tramite degli incaricati del backup, provvederanno a pianificare le conversioni necessarie, con particolare riferimento alla conversione dei formati di tipo numerico, data ed in genere dei caratteri speciali. Per quanto riguarda immagini, filmati, disegni , testi formattati (es: pdf) ecc. la scelta del formato, ovvero dello standard, è di competenza del Titolare che la determinerà sulla base del criterio d'indipendenza, d'intesa con i Responsabili del trattamento ed il Direttore della Direzione Regionale competente in materia di informatica.

8.4.2. La logica di backup

La logica di backup dei dati personali dovrà diversificarsi:

1) sulla base della tipologia dei dati distinguendo quelli "comuni" da quelli sensibili e giudiziari e applicando, a quest'ultimi, le stesse misure di sicurezza che dovranno essere adottate ai dati

relativi allo stato di salute, alla vita sessuale ed alle informazioni genetiche. Gli archivi contenenti la posta elettronica sono assimilati a quest'ultimi;

2) sulla base delle finalità che si intendono perseguire, distinguendo i salvataggi destinati a:
   - mantenimento del servizio "on line" (a "caldo", ad orario o ad evento) con frequenza minima giornaliera;
   - ad estrazioni e/o elaborazioni periodiche con frequenza mensile;
   - a fini storici (con frequenza annuale e pluriennale);
   - a fini statistici (con frequenza da determinare).

3) sulla base del metodo, ovvero in funzione dell'ordine dei volumi (quantità) da salvare:
   - salvataggio giornaliero completo degli archivi e dei dati connessi;
   - salvataggio per differenze (mensile o bisettimanale completo, più le differenze giornaliere).

8.4.3. La variazione di frequenza

Oltre a quanto indicato nel precedente paragrafo B), la frequenza dei salvataggi è determinata:

- da ogni importante cambiamento del software d'ambiente e/o di sistema;
- da ogni significativa evoluzione tecnologica;
- dalla modifica dei diritti sugli strumenti software e hardware di gestione dei dati;
- dalle informazioni circa presumibili condizioni di pericolo, dovute ad attacchi di qualsiasi tipo;
- dal significativo cambiamento del software applicativo.

8.4.4. La completezza, le procedure, le verifiche ed i supporti.

La completezza, l'efficacia e l'affidabilità delle procedure e degli strumenti di salvataggio, essendo indirizzata al "disaster tolerant ", deve comprendere:

a) la completezza dei dati.
   aa) i dati, più o meno statici, inglobati in programmi, classi, ovvero oggetti di qualsiasi genere, sono considerati parte integrante dei dati di riferimento. Pertanto, devono essere salvati e documentati in appositi archivi al primo utilizzo o modifica. Successivamente seguono le medesime procedure previste per i dati ai quali si riferiscono (vedasi precedenti paragrafi 8.4.2 e 8.4.3*);*
   ab) la creazione di una nuova relazione tra gli archivi, o la modifica di una esistente comporta il previo salvataggio degli archivi;
   ac) i dati personali non "comuni", resi temporaneamente non intelligibili ai sensi del comma 6 dell'articolo 22 della legge, vengono archiviati contemporaneamente ai dati ai quali si riferiscono nel luogo separato prestabilito.
   ad) i procedimenti, le informazioni, i dati, le chiavi, i programmi, gli algoritmi, gli schemi e le documentazioni necessari per attuare il punto precedente vengono salvati, nel luogo separato prestabilito, contemporaneamente ai dati od oggetti ai quali si riferiscono;
   ae) sulla base di quanto previsto nel precedente paragrafo 8.4.3, la scelta della tecnica di separazione, di cui all'art. 22, punti 6 e 7, della legge è determinata dal responsabile del trattamento, mentre il luogo e le modalità sono determinate dal Titolare.
   af) alla completezza dei dati si applicano sempre le disposizioni di cui al precedente paragrafo 8.4.1.

b) i dati strutturati e non strutturati seguono le medesime regole di sicurezza di cui al precedente paragrafo 8.4.1.

c) il completamento delle procedure e dei procedimenti.
   ca) le copie dei salvataggi giornalieri dovranno essere conservate per un mese (durata procedimento). Decorso tale termine, i supporti magnetici potranno essere riutilizzati. La procedura dovrà garantire:

- il salvataggio di due copie giornaliere degli archivi di cui almeno una verificata mediante il ripristino della stessa. Tale copia dovrà essere conservata in luogo prestabilito diverso da quello in cui è ubicato il server (disaster recovery);
- il salvataggio di due copie delle variazioni (nell'ipotesi di salvataggio per differenze), con le modalità di cui al punto precedente;

cb) le copie dei salvataggi mensili dovranno essere conservate almeno per un anno (durata procedimento) e, nei casi di sostanziali modifiche (batch ed on line) agli archivi (dovute a modifiche della logica del trattamento) per 10 anni, assicurando la copia antecedente e susseguente il trattamento (intero procedimento) onde, ove necessario, verificare e/o ricostruirne la logica (indipendentemente dalla documentazione) di cui all'articolo 7, lettera c) della legge.

cc) per i salvataggi annuali (al fine di garantire l'osservanza di quanto disposto dall'articolo 16, lettera d) della legge, per ogni archivio) dovranno essere effettuate due copie, una a dicembre ed una a giugno, sottoposte a doppia cifratura simmetrica o asimmetrica, seguite dalla distruzione dei dati originali. Le due chiavi, entrambe indispensabili per la ricostruzione dei dati, saranno in possesso del titolare, per le attività e nei limiti di cui agli articoli 101, punto 1, e 11, lettera d), della legge.

cd) per quanto riguarda i dati statistici, verranno forniti ogni anno all'ufficio preposto gli schemi degli archivi e dei dati. L'ufficio determinerà le regole per le estrapolazioni, sulla base delle quali verranno prodotti i nuovi archivi da mantenere a tempo indeterminato.

d) Verifiche.

Il responsabile del trattamento:

- ogni giorno, in presenza o in previsione di pericoli di cui al precedente paragrafo 8.4.3, dovrà, se necessario: procedere al blocco temporaneo dei dati e/o dei servizi avvisando sempre il titolare; produrre una ulteriore copia dei dati; avvisare, se opportuno, l'utenza;
- ogni fine mese, per ogni attrezzatura, dovrà verificare i contratti in essere adeguandoli eventualmente alle variate condizioni di diritto oppure, in alternativa, disporre la necessaria conversione;
- ogni sei mesi, oppure ad ogni significativa evoluzione tecnologica, dovrà valutare i costi ed i benefici di un eventuale piano di conversione da attuare nei sei mesi successivi;
- una volta ogni anno, oppure al variare significativo del cambiamento del software d'ambiente e/o di sistema", adeguare le attrezzature (software e/o hardware) alla nuova realtà, previa eventuale conversione della codifica dei dati;
- una volta ogni 2 anni, oppure al variare delle condizioni previste nelle tre alinee precedenti (variazioni contrattuali, evoluzione tecnologica, cambiamento del software), procedere alla copia "refreshing" degli archivi e, quando necessario, alla sostituzione dei supporti di memorizzazione.

Al fine di garantire il ripristino dei dati (articolo 34, lettera f) della legge) ed assicurarne quindi l'indipendenza di cui al precedente paragrafo 8.4.1, dovranno essere prodotte e verificate periodicamente idonee procedure di migrazione degli archivi.

e) Supporti

Il salvataggio su supporti informatici di memorizzazione di massa si basa sui principi di affidabilità ed economicità dei mezzi; pertanto, la scelta dovrà orientarsi essenzialmente verso supporti rimovibili di tipo:

- ottico, a seconda del volumi (di cui al precedente paragrafo 8.4.2 punto 3) usando, a seconda dello scopo finale, il salvataggio transitorio (giornaliero per i servizi "on line") o permanente (mensile, storico o statistico), rispettivamente su supporti riscrivibili e non riscrivibili. La scelta dei supporti ottici è (salvo ulteriori determinazioni) limitata ai formati standard CD-R/RW , DVD-R/RW;

- magnetico, a seconda del volumi (nei casi di cui al precedente paragrafo 8.4.2, punto 3) e in quelli giornalieri e mensili). La scelta dei supporti magnetici , con particolare riferimento ai nastri, è condizionata alle verifiche mensili circa i cambiamenti dell'hardware e del software di base. Per quanto riguarda in particolare l'uso dei nastri magnetici, per i salvataggi mensili, annuali e pluriennali è richiesto che la rilettura dei dati sia possibile da almeno un produttore diverso da quello che ha prodotto l'archivio.
- magneto-ottico, nell'ambito delle stesse considerazioni formulate nell'alinea precedente, il responsabile del trattamento dovrà valutare gli effetti dell'evoluzione tecnologica;

Quando possibile, gli archivi dovranno essere suddivisi in singoli sotto files, inferiori ad un Giga Byte, rispettando possibilmente la suddivisione logica pre - organizzata degli stessi.

In tutti i casi la percentuale d'uso dei supporti riscrivibili non dovrà superare il 60 % circa delle possibilità garantite dal produttore.

I supporti removibili di memorizzazione che contengono dati devono essere sempre custoditi e conservati in luoghi diversi da quelli ove vengono originariamente trattati.

I dati "non comuni" contenuti nei supporti removibili, utilizzati all'interno dei locali ove viene effettuato il trattamento, esaurito l'intero "procedimento" vengono resi inutilizzabili ai sensi del punto 22 , dell'allegato "B" della legge.

8.4.5. Tecnologie e prodotti

I prodotti dedicati esclusivamente all'archiviazione dei dati o i programmi inclusi nei gestori dei database (es: backup, export) possono essere usati:
- per produrre la prima copia giornaliera, verificata mediante il ripristino della stessa;
- per produrre la prima copia mensile, a discrezione del responsabile;
- per produrre la prima copia definitiva, se in grado di produrre l'indipendenza dai sistemi operativi, dalle applicazioni e dall'ambiente software (come strumento di passaggio, esportazione o migrazione);
- in tutti i casi, se in grado di raggiungere tutti gli obiettivi sin qui elencati.

I server che per l'archiviazione dei dati adottano sistemi di storage "raid" e "fault tolerant", considerata la ridondanza, possono produrre una sola copia dei dati a condizione che:
- venga effettuata e verificata su di un'attrezzatura diversa dalla precedente e su di un altro sistema, secondo quanto previsto al precedente paragrafo 8.4.4., lettera d), ultimo periodo;
- venga effettuata la separazione dei dati di cui al precedente paragrafo 8.4.2 punto 1);
- venga rispettato quanto indicato nel paragrafo 8.4.1, ultimo periodo.

8.4.6. Controlli e prevenzioni

Il responsabile del trattamento:

a) nei casi di significativo cambiamento del software applicativo, prima di riattivare la banca dati e/o il servizio effettua un controllo sui movimenti (variazioni) dell'archivio (fase di test) al fine di verificare il buon funzionamento dei programmi. In base al numero dei movimenti ed alla tipologia degli stessi, per espletare tale controllo dovrà essere selezionato un campione significativo. Nel caso in cui l'incaricato accerti errori o importanti differenze avviserà il responsabile o il titolare e, quando possibile, l'utenza;

b) nei casi in cui il ripristino della seconda copia dell'archivio non andasse a buon fine e/o non avesse ancora verificato la prima, mediante il ripristino, informerà il titolare, assumendo ogni responsabilità relativa alla riattivazione del servizio e dei dati;
c) nel caso in cui adottasse automatismi di logging o journaling di sistema o d'ambiente (proprietario) verificherà quotidianamente l'integrità referenziale dei dati e del sistema o del sottosistema e, in caso di disallineamento, dopo aver bloccato il servizio, avviserà il titolare ed eventualmente l'utenza. Quando i sistemi automatici indicati prevedono la possibilità di gestire più di una copia dei "movimenti", questa possibilità dovrà essere attivata; in tal modo la procedura rientra nei casi di cui alla lettera ca) del paragrafo 8.4.4, seconda alinea;
d) nel caso in cui adottasse logging o journaling applicativi verranno assunti i comportamenti di cui al precedente lettera a).

Per quanto riguarda le registrazioni (logs) di accesso ai servizi e di autenticazioni, ogni attivazione o disattivazione ed ogni inserimento, cancellazione o modifica dei dati nelle medesime contenuti, dovrà essere preventivamente autorizzato dal titolare.

8.4.7. I luoghi di conservazione

Per "luogo" di conservazione prescelto s'intende ogni locale, computer, attrezzatura hardware e/o software, sito, cassaforte, cassetta postale (e–mail), ufficio postale (e-post office) idoneo a contenere e garantire la conservazione d'informazioni, archivi, documentazioni, programmi , formule e "chiavi".

Per "chiavi" si intendono: parole, frasi, file, oggetti, procedure, programmi, regole, formule, sequenze e protocolli informatici finalizzati al mascheramento dei dati e delle trasmissioni.

La scelta del luogo di conservazione è effettuata in funzione del tipo di risorsa (oggetto) da conservare nel rispetto della legge e delle istruzioni contenute nel presente documento .

Il Titolare, d'intesa con i Responsabili del trattamento e il Direttore della Direzione Regionale competente in materia di informatica, individuerà per il salvataggio dei dati i luoghi diversi da quelli in cui originariamente e stabilmente risiedono.

8.4.8. Il ripristino dei dati

Immediatamente al termine del backup, dovrà esserne effettuata la verifica tramite la procedura di ripristino, che dovrà essere eseguita giornalmente su una macchina differente.

Tale procedura genererà dei log, che potranno essere inviati agli incaricati del trattamento al fine di valutarne immediatamente l'esito. Il responsabile del trattamento sarà quindi in grado di prendere gli adeguati provvedimenti.

Nel caso di danneggiamento o perdita dei dati, la procedura provvederà al ripristino degli stessi in un tempo che, nel caso di trattamento di dati sensibili o giudiziari, non sarà superiore ai 7 giorni.

Sezione II

Analisi del rischio e misure di sicurezza relative alla rete e alle interconnessioni, sia per le trasmissioni dati che per le comunicazioni vocali digitali (voice over IP)

9. Misure di sicurezza organizzative

L'incaricato può accedere ad una apparecchiatura di rete previa autorizzazione da parte Direttore della Direzione regionale competente in materia di informatica.

In questo modo l'incaricato può, sulla base della specifica richiesta o programmazione di intervento:

- accedere fisicamente alla specifica apparecchiatura di rete;
- accedere logicamente alla specifica apparecchiatura di rete, con le procedure di autenticazione descritte al successivo paragrafo 15.2.

10. Misure logistiche

Per un'adeguata collocazione delle apparecchiature di rete, devono essere adottate misure idonee a garantire la protezione delle apparecchiature rispetto ai seguenti rischi:

- accesso fisico non autorizzato;
- distruzione o perdita dei dati dovuta ad eventi fisici e/o logici (salvataggio delle configurazioni).

Il Direttore della Direzione regionale competente in materia di informatica e i tecnici che hanno accesso alle apparecchiature di rete devono informare il/i responsabile/i del/i trattamento/i nel caso in cui riscontrino il mancato rispetto delle misure di sicurezza.

11. Misure tecniche

11.1. Sicurezza reti locali (perimetro interno)

La sicurezza della rete interna è basata su una suddivisione della struttura in VLAN. Gli apparati attivi sono predisposti per l'autenticazione dei singoli utenti tramite UserID e password.

Tutti i collegamenti interni sono sezionati su diverse LAN collegate:

- WAN-MAN regionale, WAN-MAN Sanità, Internet Fibra;
- per le connessioni individuali gli accessi sono autenticati tramite il Kerberos

11.2. Sicurezza interconnessioni

La Regione Lazio adotta due sistemi di interconnessione: uno, basato sui servizi RUPAR (Rete Unitaria della Pubblica Amministrazione Regionale), e uno basato su collegamenti commutati.

La sicurezza perimetrale di rete è basata su due firewall in failover.
Tutti i collegamenti entranti/uscenti della RUPAR, oltre che da Internet e verso altre reti, sono filtrati sul firewall con una serie di politiche di sicurezza e filtering.

11.3. Cifratura/autenticazione delle connessioni e dei dati sulla rete

La Regione Lazio adotta:

- per l'interconnessione con gli enti pubblici territoriali regionali, autorizzati a collegarsi alla rete regionale, la RUPAR (la quale consente di connettersi attraverso ADSL via VPN per garantire la protezione dei dati nell'attraversamento dei mezzi trasmessivi);
- per l'interconnessione con le aziende sanitarie regionali, la RUPAR SANITA (attraverso ADSL via VPN IPSEC);
- per l'interconnessioni individuali, accessi su rete commutata PSTN o ISDN (attraverso autenticazioni realizzate tramite RADIUS amministrato da Laziomatica).
- il management delle interconnessioni e garantito da più modalità NAT su ip e MAC, SSL e/o HTTPS ed eventuale certificato.

Sezione III

Analisi del rischio e misure di sicurezza relative alle risorse di rete e ai PC

12. Misure di sicurezza organizzative

L'incaricato, tramite la procedura di accesso logico descritta nel successivo paragrafo 18.1. lettera "B", può accedere, sulla base delle specifiche autorizzazioni, ad una stazione di lavoro connessa o non connessa alla rete della struttura.

In questo modo l'incaricato può:

- accedere alle risorse presenti fisicamente sulla macchina stessa (dischi fissi);
- accedere alle risorse di rete (cartelle del disco fisso del server su cui l'incaricato ha diritto di accesso);
- condividere con altri utenti risorse quali file, cartelle e stampanti;
- condividere con altri utenti applicazioni (Protocollo, Pratiche, ecc.);
- usufruire della centralizzazione delle operazioni di backup (nel caso in cui i dati siano salvati sul server) e di aggiornamento software.

13. Descrizione della configurazione standard delle stazioni di lavoro

Le unità logiche disponibili, in base alle configurazioni standard, sono in sintesi le seguenti:

13.1. Unità hardware

Per unità locali del computer si intendono, nel presente documento, i seguenti componenti:

- box con:
  a) unità centrale di elaborazione (CPU);
  b) hard disk;
  c) memoria centrale;
  d) porte di comunicazione (seriali, USB, parallele, ethernet);
- video;
- tastiera;
- mouse;

- stampante;
- scanner

13.2. Unità software

- sistema operativo (Windows);
- strumenti di ufficio (Office);
- programmi antivirus

14. Misure di sicurezza informatiche

In base alla configurazione appena descritta vanno adottate le seguenti misure:
- va privilegiato per la memorizzazione dei dati l'utilizzo delle risorse di rete evitando l'uso delle unità presenti fisicamente sul PC (dischi fissi/locali C e D);
- in ogni caso le elaborazioni riguardanti dati personali vanno memorizzate sui dischi di rete;
- anche se alcuni programmi applicativi consentono la protezione dei singoli file mediante l'apposizione di specifiche password tale pratica va evitata.

Tuttavia, va rilevato che la password sul file come misura di sicurezza non è adeguata e può essere controproducente. Infatti tali password possono essere perse o dimenticate, rendendo molto difficile il recupero dei dati.

14.1. Uso dei dischi fissi/locali (C:\ e altri)

Poiché anche l'utilizzo dei dischi fissi/locali presenta inconvenienti sotto il profilo della sicurezza dei dati, nell'impossibilità di usare le unità di rete, si devono adottare le seguenti misure di sicurezza.
- i dischi fissi locali non vanno utilizzati come unico e predominante strumento di lavoro;
- vanno effettuati periodici backup dei dati su supporti magnetici, al fine di evitarne la perdita, con modalità analoghe a quelle descritte nella *Sezione VI del presente Capo*;
- tali supporti vanno conservati secondo le modalità individuate nella Sezione VI "Analisi del rischio e misure di sicurezza relative ai supporti di memorizzazione" del presente Capo.

Sezione IV

Analisi del rischio e misure di sicurezza relative alle postazioni di lavoro

15. Misure di sicurezza organizzative

A ciascun incaricato viene assegnata una directory, in un'area disco di un server che sia sottoposta a backup, dove allocare i dati che devono essere mantenuti in maniera sicura. L'accesso a queste directory è consentito esclusivamente all'incaricato del trattamento e all'incaricato del backup.

15.1. Il sistema operativo per le postazioni di lavoro

Presso ciascuna postazione di lavoro è consentita l'installazione delle seguenti due categorie di sistemi operativi:

- commerciale, dotato di licenza d'uso;
- commerciale, dotato di licenza G.L.P.;

L'installazione di sistemi diversi da quelli indicati va autorizzata dal responsabile del trattamento, d'intesa con il Direttore della Direzione regionale competente in materia di informatica.

La conformità dei sistemi viene di norma verificata dal Direttore della Direzione regionale competente in materia di informatica.

Il sistema deve essere installato solo da supporti fisici originali o istallazione da rete autorizzata.

Il sistema deve consentire di:

- regolare l'accesso contro il rischio di utilizzo dei dati da parte di persone non autorizzate, mediante il sistema di autenticazione informatica e l'individuazione dei profili di autorizzazione;
- registrare gli accessi, riusciti e falliti, a livello di sistema e di base dati;
- registrare gli accessi in lettura e scrittura effettuati attraverso il sistema di gestione delle basc dati; (sentire le società esterne)
- registrare tutti gli accessi in lettura e scrittura ai singoli archivi. (sentire le società esterne)

Il responsabile del trattamento individua uno o più incaricati della verifica delle predette registrazioni.

Le operazioni di verifica delle registrazioni debbono essere effettuate almeno settimanalmente. I problemi riscontrati vanno segnalati al responsabile del trattamento che individuerà le opportune contromisure.

Il Direttore della Direzione regionale competente in materia di informatica dispone l'aggiornamento dei sistemi in dotazione con cadenza almeno mensile al fine di prevenire la vulnerabilità degli strumenti elettronici, e in particolare contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, e a correggere eventuali difetti.

Per quanto riguarda le misure di sicurezza da adottare e i comportamenti che devono tenere gli incaricati si rinvia anche alle indicazioni riportate nella Sezione III "Analisi del rischio e misure di sicurezza relative alle risorse di rete e ai PC" del presente Capo.

15.2. Sistema di autenticazione informatica

Tutte le postazioni di lavoro devono essere protette da:

a) una credenziale di autenticazione di accesso alle risorse del PC, qualora attivata;
b) una credenziale di autenticazione di accesso alle risorse del dominio di appartenenza (trattasi della credenziale di autenticazione prevista dal Disciplinare Tecnico Allegato B della Legge);
c) una credenziale di autenticazione di accesso per le applicazioni che lo prevedono.

Per gli incaricati che accedono da postazioni fuori dal dominio, le credenziali di autenticazione richieste dal Disciplinare Tecnico sopra richiamato sono stabilite a livello delle singole applicazioni.

15.2.1. Accesso alle risorse del PC

Per quanto riguarda la credenziale di autenticazione di accesso alle risorse del PC, qualora attivata, l'inserimento della password di accensione fornita dal Sistema Informativo all'atto della assegnazione della postazione, deve essere immediatamente modificata a cura dell'incaricato, che ne avrà la responsabilità della conservazione. Tale password di accensione va modificata dall'incaricato con cadenza semestrale.

Ai fini dell'assistenza tecnica, la password di accensione può essere comunicata agli addetti e sostituita al termine dell'intervento.

15.2.2. Accesso alle risorse del dominio di appartenenza

L'accesso ad ogni trattamento o a un insieme di trattamenti con un computer collegato alla rete, è consentito agli incaricati dotati di credenziali di autenticazione, mediante il superamento di una procedura di autenticazione. Ogni accesso, o tentativo di accesso, a tali informazioni dovrà essere registrato con un sistema che garantisca l'inalterabilità delle registrazioni stesse.

Le credenziali di autenticazione sono formate da un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo.

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

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

Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

Qualora, in caso di prolungata assenza o impedimento dell'incaricato, si renda necessario per ragioni improrogabili l'utilizzo di dati o applicazioni accessibili in via esclusiva con i suoi codici di accesso è necessario rispettare le seguenti regole:

Il responsabile del trattamento

- verifica
  - che sussista un'improrogabile necessità di accedere ai dati per ragioni di servizio,
  - che sia stata accertata l'impossibilità o la notevole difficoltà di raggiungere l'incaricato
- individua un incaricato designato ad operare in vece dell'incaricato assente;
- richiede per iscritto alla Direzione Sistemi Informativi di disporre di "forzare" l'utenza impostando una nuova password che dovrà essere comunicata alla persona incaricata di effettuare

l'accesso, la quale potrà iniziare ad operare solo previa sostituzione della password con una diversa solo a lui nota

Al ritorno dell'assegnatario, la Direzione Sistemi Informativi provvede ad effettuare una nuova "forzatura" impostando una nuova password per l'assegnatario che riprenderà ad operare normalmente previa sostituzione della password con una diversa solo a lui nota.

15.3. Sistema di autorizzazione

La procedura di autenticazione consente di ottenere uno specifico insieme di privilegi di accesso ed utilizzo, denominato profilo, rispetto alle risorse del sistema informatico. A ciascun profilo può essere associato un gruppo di incaricati che condividono gli stessi privilegi di accesso e utilizzo.

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

Quando per gli incaricati sono individuati profili di autorizzazione (vedasi definizione riportata al paragrafo 2. lettera f) di ambito diverso é utilizzato un sistema di autorizzazione (vedasi definizione riportata al paragrafo 2. lettera g).

L'utilizzazione del sistema di autorizzazione richiede:

- un'analisi delle esigenze organizzative della struttura, per individuare la configurazione adatta;
- la creazione da parte del Direttore della Direzione regionale competente in materia di informatica di gruppi di abilitazione, nei quali gli incaricati saranno inseriti a seconda delle attività cui sono preposti.

Il responsabile del trattamento deve segnalare la variazione della composizione dei gruppi di incaricati al Direttore della Direzione regionale competente in materia di informatica per l'adeguamento delle abilitazioni; il predetto Direttore provvede a configurare i permessi sulle unità di rete e la composizione dei gruppi di incaricati.

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

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

16. Salvataggio dei dati di postazioni di lavoro

Il responsabile del trattamento può/deve avvalersi di spazi esterni messi a disposizione sul file server per effettuare copie dei dati.

I dati prima di essere salvati sul server devono essere verificati mediante ripristino degli stessi, inglobati in file crittografati con chiave simmetrica e poi copiati.

Nell'ipotesi in cui i dati contenuti nel PC non possono essere salvati sul server con le modalità sopra descritte, si dovrà effettuare ad ogni variazione/fine giornata il salvataggio di due copie degli archivi di cui almeno una verificata mediante il ripristino della stessa. Tale copia dovrà essere conservata in luogo prestabilito dal responsabile del trattamento comunque diverso da quello ove è ubicato il PC.

17. Misure di sicurezza logistiche

Una adeguata protezione dei luoghi di lavoro serve a garantire la sicurezza dei dati personali custoditi al loro interno. Per garantire questa sicurezza vanno adottate misure logistiche idonee a garantire la protezione di documenti, supporti informatici e apparecchiature rispetto al rischio di:

- accesso fisico non autorizzato;
- distruzione o perdita dei dati dovuta ad eventi fisici.

17.1. Protezione delle postazioni da accesso fisico non autorizzato

Per accesso fisico s'intende l'entrata ai locali in cui vi sono uno o più postazioni di lavoro dotate di PC. Le misure di sicurezza devono garantire contro il rischio di accesso fisico ai locali o intrusione da parte di persone non autorizzate. L'accesso fisico alla postazione di lavoro collegata in rete da parte di estranei non identificati rappresenta un potenziale rischio per la sicurezza dei dati custoditi sul server della rete, anche se la persona non può conoscere le password e le credenziali di autenticazione. Per evitare questo rischio si devono adottare le seguenti misure di sicurezza:

17.1.1. Personale interno alla struttura

Relativamente al personale interno alla struttura:

- le postazioni di lavoro sono accessibili solo da quanti ne hanno titolo, in qualità di responsabili o incaricati del trattamento, di tecnici autorizzati o altro, nei soli limiti in cui ciò sia funzionale allo svolgimento dei compiti della struttura o per lo svolgimento di attività di manutenzione, di pulizia e affini, nonché per altre attività comunque indispensabili;
- l'accesso fisico ai luoghi di lavoro è protetto tramite la presenza di personale addetto ovvero tramite la chiusura delle vie di accesso;
- in ogni caso gli uffici aperti al pubblico devono essere presidiati da personale addetto; negli orari diversi da quelle di servizio, ove non vi sia comunque un presidio, la porta di accesso all'ufficio deve rimanere chiusa.

17.1.2. Personale esterno alla struttura

Relativamente al personale esterno alla struttura:

- la persona esterna può accedere ai locali solo quando è presente un addetto;
- la persona esterna deve farsi riconoscere al personale di portineria e seguire le regole stabilite dal responsabile per l'accesso del pubblico alla struttura;

17.1.3. Interventi di assistenza e manutenzione

A. Assistenza in remoto

Gli interventi di assistenza, installazione e aggiornamento dei software e, in generale, quelli volti a fronteggiare guasti o temporanei black-out nel funzionamento delle postazioni di lavoro,

sono di norma effettuati dalla società Laziomatica Spa senza la necessità dell'intervento di un tecnico informatico presso la postazione di lavoro.

Il sistema di assistenza in remoto consente, previa autorizzazione del dipendente/utente, di condividere a distanza con l'operatore del supporto tecnico l'utilizzo di tastiera, mouse e schermo, senza che l'utente stesso perda il controllo di quanto avviene al proprio PC e ai dati eventualmente accedibili attraverso lo stesso.

B. Assistenza con intervento locale del tecnico

Se invece sono necessari interventi di manutenzione sulla macchina o di assistenza, adeguamento, ecc. presso la postazione di lavoro, è necessario che l'utente o il referente informatico o, in loro assenza altro dipendente della struttura, assista alle operazioni di manutenzione.

L'ufficio deve trattenere e conservare copia del rapporto di intervento rilasciato dalla ditta intervenuta. Tale rapporto deve contenere:

- data e orario dell'intervento (inizio e fine);
- descrizione sintetica del tipo di intervento;
- attestazione di conformità dell'intervento alle disposizioni relative di cui al Disciplinare Tecnico sulle misure minime di sicurezza (All. B alla legge)
- nome e cognome del tecnico intervenuto;
- denominazione della ditta;
- firma del tecnico e dell'utente che assiste all'intervento.

Ove non già presenti nello schema, tali dati devono essere apposti dal personale dell'ufficio in presenza del tecnico intervenuto. La descrizione dell'intervento non può contenere codifiche dal significato non immediatamente comprensibile per l'utente che sottoscrive il rapporto.

17.2. Protezione dei dati dal rischio di distruzione o perdita dovuta ad eventi fisici

Gli eventi fisici che possono costituire fonte di rischio per le postazioni di lavoro sono quelli indicati nella Parte II – Capo II – Sezione I "Analisi del rischio e misure di sicurezza relative ai server".

Al fine di ridurre al minimo i rischi di distruzione o perdita di dati, è consigliabile prediligere il lavoro sui dischi di rete, la cui protezione è assicurata dalle misure di sicurezza e di salvataggio automatico adottate per i server.

In caso di utilizzo dei dischi installati fisicamente sul PC (C e D), vanno effettuati periodici backup dei dati su supporti magnetici, da conservare secondo quanto disposto nel precedente paragrafo 8.4..

18. Misure di sicurezza tecniche, informatiche e procedurali

La sicurezza delle postazioni di lavoro deve essere tutelata con le misure tecniche, informatiche e procedurali idonee a garantire la protezione delle apparecchiature rispetto ai seguenti rischi:

- accesso logico non autorizzato o non conforme alle regole;
- distruzione o perdita dei dati dovuta ad attacchi esterni (es.: virus);

- distruzione o perdita dovuta ad attacchi di malintenzionati;
- perdita accidentale dei dati.

18.1. Protezione da accessi logici non autorizzati

Ferme restando le misure indicate nel paragrafo precedente, per la protezione da accesso logico non autorizzato l'incaricato deve osservate le seguenti misure di sicurezza:

- le password e le credenziali di autenticazione non vanno comunicate o condivise con altre persone; è interesse dell'incaricato evitare che altri utilizzino la sua password d'accesso in quanto dalla registrazione dell'attività effettuata dal sistema risulterebbe a lui attribuito il trattamento effettuato da altri, con connessa responsabilità in caso di trattamenti scorretti o non autorizzati o illeciti;
- le password e le credenziali di autenticazione non vanno trascritte su supporti agevolmente accessibili da parte di terzi;
- le password e le credenziali di autenticazione del personale nel frattempo cessato, assente per lungo periodo o che è stato assegnato ad altra struttura o attività non vanno utilizzati.

Il dirigente è tenuto, in caso di entrata in servizio, cessazione, mobilità o cambio di mansioni del personale assegnatario di dotazioni informatiche, a provvedere alla richiesta dei relativi nuovi inserimenti, delle cancellazioni o delle modifiche alle abilitazioni che si rendano necessarie.

L'incaricato è tenuto, inoltre, a:

- sostituire la password ad intervalli regolari; il sistema consente la sostituzione della password da parte dell'incaricato; il sistema consente anche di impostare per tutta la rete un vincolo che impone a tutti gli incaricati di cambiare le password entro periodi prestabiliti;
- rendere inaccessibile il sistema dalla propria postazione di lavoro ogni volta che si assenta;
- impostare uno screen saver automatico protetto da password con tempo di attivazione inferiore ai 5 minuti di inattività della macchina;
- usare, se accede alla rete da una postazione di lavoro non assegnatagli, il proprio identificativo utente e la propria password e non chiedere di utilizzare la password del collega.

18.1.1. Ripristino della password

Nel caso di perdita e/o dimenticanza della password o delle credenziali di autenticazione, il Direttore della Direzione regionale competente in materia di informatica deve impostare nuove credenziali di autenticazione e comunicarle all'incaricato. L'incaricato potrà poi provvedere alle ulteriori sostituzioni.

Per il ripristino della parola chiave si segue la seguente procedura:

- richiesta scritta di ripristino firmata dall'incaricato;
- sottoscrizione della richiesta, per autorizzazione, del responsabile del trattamento dei dati;
- la richiesta può essere fatta dal solo responsabile nel caso in cui sussistano le necessità di accesso ai dati in assenza dell'incaricato;
- inoltro della richiesta al Direttore della Direzione regionale competente in materia di informatica, anche via fax.

Questa procedura va seguita anche qualora, a seguito del blocco dell'accesso per mancato utilizzo per più di 6 mesi, sia necessario richiederne lo sblocco.

Le prescrizioni descritte non rappresentano un mero formalismo, ma sono funzionali a garantire la sicurezza, in quanto predisposte per dare la certezza al Direttore della Direzione regionale competente in materia di informatica che la richiesta di ripristino password proviene da chi è effettivamente legittimato al trattamento dei dati.

18.1.2. Protezione da accessi logici non autorizzati a PC non connessi alla rete

Per l'accesso logico ai PC non connessi al server di rete della struttura, bisogna adottare, prima dell'inizio del trattamento dei dati personali, le seguenti misure:

- se il sistema operativo lo consente, impostare la password e le credenziali di autenticazione per l'accesso logico al PC, che vanno fornite a ciascun incaricato del trattamento di dati personali;
- se invece sul PC è installato un sistema operativo privo di servizi di multiutenza va attivata una password e credenziali di autenticazione a seconda della marca, modello e data di fabbricazione del computer eseguita da un tecnico esperto;
- sostituzione della password e delle credenziali di autenticazione ad intervalli regolari e deposito presso il custode.

18.1.3. Protezione da accessi logici non autorizzati agli applicativi

L'accesso logico alla posta elettronica e ad altri programmi applicativi può essere protetto da parola chiave, associata o meno ad un user-id. Per quanto riguarda gli applicativi vanno osservate le seguenti disposizioni:

- le applicazioni che trattano dati personali, devono essere protette con un sistema di autenticazione;
- la password e l'eventuale codice identificativo sono personali; pertanto devono essere adottate le cautele previste nel precedente paragrafo 18.1.;
- se necessario, la creazione, la modificazione e la cancellazione delle abilitazioni vengono richieste dal responsabile del trattamento dei dati.

18.2. Protezione dai virus

I PC connessi in rete sono protetti da un prodotto antivirus installato e connesso ai sistemi server con aggiornamento periodico automatico via Internet/Intranet a carico dell'amministrazione. Sui PC non connessi al server di rete della struttura è invece necessario installare un prodotto antivirus ad hoc che, per risultare efficace nel tempo, dovrà essere aggiornato periodicamente secondo le modalità richieste dal prodotto stesso. L'aggiornamento è a carico dell'amministrazione.

18.3. Protezione dai malintenzionati

I posti di lavoro ed i server della struttura sono collegati alla rete interna regionale; la protezione, relativamente alla distruzione o perdita di dati dovuta ad attacchi esterni da parte di malintenzionati, via Internet, è effettuata da 2 Firewall Netscreen 500 gestiti da Laziomatica Spa.

Si ricorda comunque che la difesa dagli attacchi di questo tipo è comunque assicurata solo se viene data puntuale applicazione a tutto il complesso delle regole di sicurezza comprese nel presente documento.

18.4. Protezione dal rischio di perdita accidentale dei dati

Per i dati contenuti nei dischi di rete, viene effettuato il backup definito al precedente paragrafo 8.4.

Invece per i dati contenuti nei dischi installati fisicamente sul PC (C:\ e D:\) è necessario che ciascun operatore provveda a periodici backup dei dati su supporti magnetici e alla conservazione dei supporti stessi nel rispetto delle disposizioni individuate al precedente paragrafo 8.4..

Sezione V

Analisi del rischio e misure di sicurezza relative ai pc portatili

19. Misure di sicurezza organizzative

Per l'adozione delle misure di sicurezza organizzative sui PC portatili:

- il responsabile del trattamento deve specificare per iscritto agli assegnatari gli utilizzi consentiti;
- i PC portatili devono essere usati solo dai soggetti autorizzati dal responsabile ed unicamente per gli utilizzi a cui sono destinati.

20. Misure di sicurezza logistiche

Una adeguata protezione dei PC portatili serve a garantire la sicurezza dei dati personali custoditi al loro interno.

Per garantire questa sicurezza vanno adottate misure logistiche idonee ad assicurare la protezione di documenti, supporti informatici e apparecchiature rispetto al rischio di:

- accesso fisico non autorizzato o furto;
- distruzione o perdita dei dati dovuta ad eventi fisici.

20.1. Protezione da accesso fisico non autorizzato e dal furto

Il personale che ha in consegna un PC portatile è tenuto a:

- evitare l'abbandono del portatile che potrebbe esporlo al rischio di furto;
- custodire i portatili non collegati negli elementi di arredo muniti di serratura (armadi, cassettiere...);
- escludere l'accesso ai dati da parte di soggetti non autorizzati al trattamento, evitando, così, che tali dati giungano a conoscenza di terzi;
- evitare, ove non strettamente necessario per lo svolgimento dei compiti affidati, la connessione del portatile a reti che non siano quelle regionali;
- in caso di utilizzo condiviso del portatile, registrare tutti gli assegnatari e, ove possibile, i rispettivi periodi di utilizzo.

21. Misure di sicurezza tecniche, informatiche e procedurali

La sicurezza dei PC portatili deve essere tutelata con le misure tecniche, informatiche e procedurali idonee a garantire la protezione delle apparecchiature rispetto ai seguenti rischi:

- accesso logico non autorizzato o non conforme alle regole;
- distruzione o perdita dei dati dovuta ad attacchi esterni (es.: virus);
- distruzione o perdita dovuta ad attacchi di malintenzionati;
- perdita accidentale dei dati.

21.1. Protezione da accesso logico non autorizzato

Si richiamano, in quanto compatibili con le caratteristiche tecniche del PC portatile e con le esigenze organizzative, le misure previste per l'accesso logico alle postazioni di lavoro fisse descritte alla Sezione IV del presente Capo.

21.2. Protezione dai virus

Per ridurre al minimo il pericolo di perdite di dati a causa di virus informatici è necessario verificare che sia installato un prodotto antivirus ad hoc che, per risultare efficace nel tempo, deve essere aggiornato periodicamente secondo le modalità richieste dal prodotto stesso.

21.3. Applicazione degli aggiornamenti periodici di sicurezza.

Con frequenza almeno semestrale i software dei server, delle altre apparecchiature informatiche e dei personal computer individuali devono essere aggiornati applicando le "patch" rese disponibili dal produttore volte a prevenire le vulnerabilità e a correggerne i difetti.

21.4. Protezione dai malintenzionati

I PC portatili, quando collegati a rete diversa da quella interna regionale o connessi a Internet via modem ad un provider diverso da Laziomatica SpA, non usufruiscono della protezione effettuata tramite 2 Firewall Netscreen 500 gestiti da Laziomatica Spa . Pertanto, a fronte del pericolo di attacchi esterni dei malintenzionati, vanno adottate le seguenti cautele:

- evitare, ove non strettamente necessario per lo svolgimento dei compiti affidati, la connessione del portatile a reti che non siano quella regionale;
- ove non si possa garantire un utilizzo disconnesso da reti, concordare idonee misure di protezione con la struttura competente in materia di informatica.

21.5. Protezione dal rischio di perdita accidentale dei dati

Anche il PC portatile può essere dotato di scheda di rete e, quindi, può essere connesso alla rete dell'ufficio. In questo caso se il PC è correttamente configurato è possibile connettersi al server con la stessa credenziale di autenticazione che si usa per le stazioni di lavoro fisse e accedere alle risorse di rete. Sarà così possibile salvare sul disco tutti i dati che sono stati elaborati con il portatile e memorizzati sul suo disco fisso. In seguito per garantire una migliore tutela della sicurezza dei dati stessi, sarà possibile cancellarli dal disco fisso del portatile. I dati salvati sul server usufruiranno del salvataggio automatico di backup.

Nel caso non sia possibile connettere il portatile alla rete dell'ufficio, il personale che lo ha in uso è tenuto a:

- provvedere a periodici (almeno una volta alla settimana) backup dei dati contenuti nel disco fisso del portatile su supporti magnetici;
- custodire i predetti supporti con le precauzioni individuate nel precedente paragrafo 8.4.

Sezione VI

Analisi del rischio e misure di sicurezza relative ai supporti di memorizzazione

22. Misure di sicurezza logistiche

Nell'uso e nella conservazione dei supporti di memorizzazione si devono porre in essere le misure necessarie a ridurre al minimo i rischi di:

- accesso fisico non autorizzato;
- furto e manomissione dei dati da parte di malintenzionati;
- distruzione o perdita dei dati dovuta ad eventi fisici;
- perdita accidentale dei dati.

22.1. Reimpiego

Ai sensi dell'articolo 7 della legge:
"i supporti già utilizzati per il trattamento, ove contenenti dati sensibili o giudiziari, possono essere riutilizzati qualora le informazioni precedentemente contenute non siano tecnicamente in alcun modo recuperabili; altrimenti devono essere distrutti."

Per il reimpiego dei supporti di memorizzazione, qualora gli stessi debbano essere consegnati a terzi, devono essere adottate le seguenti indicazioni operative:

- **floppy disk e cd-rom riscrivibili**: prima di essere consegnati a terzi, debbono essere sottoposti ad una specifica operazione che garantisca la cancellazione delle informazioni precedentemente contenute;
- **hard disk**: prima di essere consegnato a terzi, deve essere sottoposto ad una specifica operazione che garantisca la cancellazione delle informazioni precedentemente contenute;nel caso in cui, a seguito di intervento tecnico, si presenti la necessità di sostituire l'hard disk, è necessario procedere al recupero dei dati contenuti nello stesso, ove possibile e opportuno; dopo aver effettuato tale verifica si dovrà rendere fisicamente inutilizzabile l'hard disk sostituito (distrutti mediante rottura); si ricorda che l'hard disk potrebbe costituire un mezzo di esportazione illegittima di dati personali qualora gli stessi fossero recuperati da personale non autorizzato.

Sezione VII

Analisi del rischio e misure di sicurezza relative a Internet

23. Misure di sicurezza organizzative

- L'utilizzo di una connessione ad Internet (ad esempio via modem) attraverso un provider diverso da Laziomatica SpA espone il PC utilizzato ai rischi normalmente presenti nel corso di una connessione ad Internet in assenza della protezione garantita dai firewall presenti nella rete interna regionale. L'eventuale attacco alla macchina nel corso della navigazione non protetta diventa un fattore di rischio per l'intera rete regionale;
- l'accesso a siti "impropri" e lo scaricamento di file non autorizzati, oltre ad essere in contrasto con il codice di disciplina del dipendente regionale, in alcuni casi possono essere illegali e puniti dalla legge penale;
- l'utilizzo della connessione Internet della Regione per finalità non riconducibili all'attività di lavoro, anche se non produce un costo diretto, può diventare causa di sovraccarico della linea e può portare a un deterioramento della velocità della connessione per tutti gli utenti;
- le informazioni presenti su siti Internet non connessi a istituzioni conosciute possono essere non accurate, non valide o deliberatamente false: ogni decisione basata su di esse deve essere valutata adeguatamente;
- qualora il collegamento alla rete Internet avviene al di fuori della rete interna regionale (ad es. tramite PC portatile), ogni macchina che può accedere a Internet (o il server se gli elaboratori sono in rete) va protetta da un antivirus aggiornato;
- i messaggi di posta elettronica di cui non si conosce il mittente vanno trattati con la massima circospezione; non bisogna cliccare sugli eventuali allegati senza pensarci; si tenga presente che i danni per virus ricevuti attraverso la posta elettronica rappresentano da soli la grande maggioranza delle cause di eventi dannosi per virus informatico all'interno delle reti aziendali.

CAPO III

Trattamenti effettuati con strumenti diversi da quelli elettronici

24. Misure di sicurezza organizzative

Nel caso di trattamento dei dati effettuato con strumenti diversi da quelli elettronici o comunque automatizzati (supporto cartaceo o altri supporti quali fotografie, fiche, slides, diapositive, ecc.) sono previsti due diversi standard di sicurezza:

- per il trattamento di dati comuni;
- per il trattamento di dati sensibili o giudiziari (art. 22, 23 e 24 della legge).

25. Misure logistiche

Il personale addetto al trattamento di dati personali deve porre in essere le misure necessarie a ridurre al minimo i rischi di:

- accesso fisico non autorizzato;
- furto o manomissione dei dati da parte di malintenzionati;

- distruzione o perdita dei dati dovuta ad eventi fisici;
- perdita accidentale dei dati.

25.1. Protezione dall'accesso fisico non autorizzato o dalla manomissione dei dati

Le misure idonee ad evitare l'accesso fisico non autorizzato o la manomissione dei dati da parte di malintenzionati sono le seguenti:

25.1.1. Dati personali comuni

I documenti contenenti dati personali comuni sono conservati in archivi ad accesso selezionato: pertanto l'accesso ai dati è consentito ai soli incaricati del trattamento, al responsabile del trattamento nonché al personale che deve accedervi per l'espletamento di compiti comunque connessi con il trattamento;

Questi documenti possono essere estratti dall'archivio e affidati alla custodia dell'incaricato del trattamento per il tempo strettamente necessario al trattamento medesimo: egli ha cura di garantirne la riservatezza e provvede al deposito in archivio al termine delle operazioni; tale disposizione va precisata nelle istruzioni formalmente fornite all'incaricato stesso nell'atto di nomina;

La struttura che custodisce dati personali su supporto fisico deve dotarsi di arredi (cassettiere, armadi ecc.) muniti di meccanismi di serratura adatta a garantire la sicurezza, da destinare ad archivio di documenti contenenti dati personali.

25.1.2. Dati sensibili e giudiziari

- L'accesso ai dati sensibili e giudiziari è limitato agli incaricati del trattamento, al responsabile del trattamento nonché al personale che deve accedervi per l'espletamento di compiti comunque connessi con il trattamento;
- Gli archivi devono essere ad accesso selezionato e controllato: i documenti contenenti dati personali sensibili e giudiziari devono essere conservati in elementi di arredo (armadi o cassettiere) muniti di serratura a chiave (o altro sistema che offra pari garanzie di sicurezza); la chiusura a chiave garantisce tanto la selezione del personale autorizzato ad accedere, quanto il controllo sugli accessi medesimi;
- La chiave deve essere custodita da personale incaricato della custodia dal responsabile;
- Il personale incaricato della custodia delle chiavi è tenuto a riporle in un luogo non agevolmente accessibile da altri;
- L'archivio viene aperto e chiuso dal personale custode delle chiavi;
- I soggetti ammessi all'archivio dopo l'orario di servizio devono essere identificati e registrati;
- I documenti, anche quando estratti dall'archivio per essere affidati agli incaricati per uno specifico trattamento, devono essere comunque custoditi in arredi muniti di serratura e depositati in archivio al termine del trattamento; pertanto, quando l'incaricato abbandona la propria postazione di lavoro, i documenti devono essere riposti e conservati sotto chiave; questa disposizione va precisata nelle istruzioni formalmente fornite all'incaricato stesso nell'atto di nomina.

25.1.3. Protezione dei locali archivio contenenti dati personali sensibili e giudiziari

Poiché è obbligatorio archiviare i documenti contenenti dati personali sensibili e giudiziari in arredi (armadi o cassettiere) chiusi a chiave, l'accesso ai locali che contengono i documenti può non essere soggetto a particolari restrizioni. Resta fermo l'obbligo per l'incaricato e il responsabile

di verificare che gli elementi di arredo siano sempre chiusi e che vengano rispettate le misure sopra riportate relative alla custodia delle chiavi e all'apertura degli archivi.

Se non c'è immediata disponibilità di arredi muniti di serratura per l'archiviazione dei documenti contenenti dati personali sensibili e giudiziari, gli archivi devono in ogni caso essere ubicati in appositi locali chiusi a chiave e, se appare agevole l'intrusione dall'esterno, muniti di sbarre.

Una apposita stanza-archivio chiusa a chiave può essere una soluzione adatta anche nel caso di armadi con serratura, in quanto aumenta il livello di protezione dei dati stessi.

Il personale diverso dagli incaricati del trattamento che accede a questi locali deve essere accompagnato da uno dei soggetti incaricati del trattamento o dal custode delle chiavi che deve verificare che non vi sia un accesso ai dati sensibili e giudiziari contenuti nei documenti (es: apertura e consultazione dei fascicoli).

25.2. Protezione dal rischio di perdita dei dati dovuta ad eventi fisici

Un archivio è sottoposto al rischio di svariati tipi di eventi che possono provocare la distruzione o il danneggiamento dei documenti. Per ridurre al minimo questo rischio le principali misure da prendere sono le seguenti:
- i locali adibiti ad archivio devono essere collocati in luoghi sicuri, evitando ad esempio scantinati e piani seminterrati che sono a rischio di allagamenti;
- nelle strutture devono essere presenti idonei dispositivi antincendio.

25.3. Misure per prevenire lo smarrimento accidentale dei documenti

Al fine di evitare lo smarrimento accidentale dei documenti l'incaricato del trattamento deve aver cura di depositare i documenti negli appositi archivi non appena cessate le operazioni di trattamento.

CAPO IV

Videosorveglianza

26. Principi generali

Il sistema di videosorveglianza è costituito da un insieme di apparecchiature di registrazione automatica mediante video operanti da postazioni fisse che registrano su apposite cassette quanto appare nel campo visivo dell'apparecchiatura.

Il Garante per la protezione dei dati personali ha già emesso una serie di prescrizioni (*"decalogo" pubblicato sul Bollettino del Garante n. 14/15, p. 28*, aggiornato e integrato con provvedimento del 29.4.2004) per la gestione dei sistemi di videosorveglianza, che si richiamano in sintesi nel presente atto.

La Regione Lazio, nello svolgimento dell'attività di videosorveglianza, osserva le seguenti cautele nel rispetto del principio di proporzionalità tra mezzi impiegati e fini perseguiti:

PRESCRIZIONI DEL GARANTE (=DECALOGO)	APPLICAZIONI NELLA REALTA' REGIONALE
	Principio di liceità
1. **Tutti gli interessati devono determinare esattamente le finalità perseguite attraverso la videosorveglianza e verificarne la liceità in base alle norme vigenti. Se l'attività è svolta in presenza di un pericolo concreto o per la prevenzione di specifici reati, occorre rispettare le competenze che le leggi assegnano per tali fini solo a determinate amministrazioni pubbliche, prevedendo che alle informazioni raccolte possano accedere solo queste amministrazioni.**	Il trattamento dei dati attraverso sistemi di videosorveglianza è possibile solo se è fondato su uno dei presupposti di liceità previsti per gli organi pubblici. La videosorveglianza deve avvenire nel rispetto, oltre che della disciplina in materia di protezione dei dati, di quanto prescritto da altre disposizioni di legge da osservare in caso di installazione di apparecchi audiovisivi. Si richiamano, al riguardo, le vigenti norme dell'ordinamento civile e penale in materia di interferenze illecite nella vita privata, di tutela della dignità, dell'immagine, del domicilio e degli altri luoghi cui è riconosciuta analoga tutela (toilette, cabine, spogliatoi, ecc.). Vanno tenute presenti, inoltre, le norme riguardanti la tutela dei lavoratori, con particolare riferimento alla legge 300/1970 (Statuto dei lavoratori).
2. **Il trattamento dei dati deve avvenire secondo correttezza e per scopi determinati, espliciti e legittimi.**	**Principio di necessità** Poiché l'installazione di un sistema di videosorveglianza comporta in sostanza l'introduzione di un vincolo per il cittadino, ovvero di una limitazione e comunque di un condizionamento, va applicato il principio di necessità e, quindi, va escluso ogni uso superfluo ed evitati eccessi e ridondanze. Ciascun sistema informativo e il relativo programma informatico vanno conformati già in origine in modo da non utilizzare dati relativi a persone identificabili quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi (es., programma configurato in modo da consentire, per monitorare il traffico, solo riprese generali che escludano la possibilità di ingrandire le immagini). Il *software* va configurato anche in modo da cancellare periodicamente e automaticamente i dati eventualmente registrati.
3. **Occorre rispettare i princìpi di pertinenza e di non eccedenza, raccogliendo solo i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese, evitando - quando non indispensabili - immagini dettagliate, ingrandite o dettagli non rilevanti, e stabilendo in modo conseguente la localizzazione delle telecamere e le modalità di ripresa.**	**Principio di proporzionalità** Nel commisurare la necessità di un sistema al grado di rischio presente in concreto, va evitata la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli, o per le quali non ricorre un'effettiva esigenza di deterrenza (come quando, ad esempio, le telecamere vengono installate solo per meri fini di apparenza o di "prestigio"). Gli impianti di videosorveglianza possono essere attivati solo quando altre misure siano ponderatamente valutate insufficienti o inattuabili (quali: controlli da parte di addetti, sistemi di allarme, misure di protezione degli ingressi, abilitazioni agli ingressi).

Prima di installare un impianto di videosorveglianza si deve valutare, obiettivamente e con un approccio selettivo, se l'utilizzazione ipotizzata sia in concreto realmente proporzionata agli scopi prefissi e legittimamente perseguibili.

La proporzionalità va valutata in ogni fase o modalità del trattamento. In particolare, quando si deve stabilire:

- se sia sufficiente, ai fini della sicurezza, rilevare immagini che non rendono identificabili i singoli cittadini, anche tramite ingrandimenti;
- se sia realmente essenziale ai fini prefissi raccogliere immagini dettagliate;
- la dislocazione, l'angolo visuale, l'uso di *zoom* automatici e le tipologie - fisse o mobili - delle apparecchiature;
- quali dati rilevare, se registrarli o meno, se avvalersi di una rete di comunicazione o creare una banca di dati, indicizzarla, utilizzare funzioni di fermo-immagine o tecnologie digitali, abbinare altre informazioni o interconnettere il sistema con altri gestiti dallo stesso titolare o da terzi;
- la durata dell'eventuale conservazione (che, comunque, deve essere sempre temporanea).

In applicazione del predetto principio va altresì delimitata rigorosamente:

- anche presso luoghi pubblici o aperti al pubblico, quando sia di legittimo ed effettivo interesse per particolari finalità, la ripresa di luoghi privati o di accessi a edifici;
- l'utilizzazione di specifiche soluzioni quali il collegamento ad appositi "centri" cui inviare segnali di allarme sonoro o visivo, oppure l'adozione di interventi automatici per effetto di meccanismi o sistemi automatizzati d'allarme (chiusura accessi, afflusso di personale di vigilanza, ecc.), tenendo anche conto che in caso di trattamenti volti a definire profili o personalità degli interessati il Codice prevede ulteriori garanzie;
- l'eventuale duplicazione delle immagini registrate;
- la creazione di una banca di dati quando, per le finalità perseguite, è sufficiente installare un sistema a circuito chiuso di sola visione delle immagini, senza registrazione (es. per il monitoraggio del traffico o per il controllo del flusso ad uno sportello pubblico).

Principio di finalità

Gli scopi perseguiti devono essere determinati, espliciti e legittimi. Ciò comporta che la Regione Lazio può effettuare il trattamento per motivi di sicurezza interna.

	Tali sistemi, pertanto, possono essere introdotti come misura complementare volta a migliorare la sicurezza all'interno o all'esterno di edifici (o impianti ove si svolgono attività produttive, industriali, commerciali o di servizi), o allo scopo di agevolare l'eventuale esercizio, in sede di giudizio civile o penale, del diritto di difesa del titolare del trattamento o di terzi sulla base di immagini utili in caso di fatti illeciti. In ogni caso, possono essere perseguite solo finalità determinate e rese trasparenti, ossia direttamente conoscibili attraverso adeguate comunicazioni e/o cartelli di avvertimento al pubblico (fatta salva l'eventuale attività di acquisizione di dati disposta da organi giudiziari o di polizia giudiziaria), e non finalità generiche o indeterminate, tanto più quando esse siano incompatibili con gli scopi che vanno esplicitamente dichiarati e legittimamente perseguiti. Le finalità così individuate devono essere correttamente riportate nell'informativa.
4. **Nei casi in cui la legge impone la notificazione al Garante dei trattamenti di dati personali effettuati da determinati soggetti, questi devono indicare fra le modalità di trattamento anche la raccolta di informazioni mediante apparecchiature di videosorveglianza. Non è prevista alcuna altra forma di specifica comunicazione o richiesta di autorizzazione al Garante.**	**Verifica preliminare** I trattamenti di dati personali nell'ambito di una attività di videosorveglianza devono essere effettuati rispettando le misure e gli accorgimenti prescritti dal Garante, anche con un provvedimento generale, come esito di una verifica preliminare attivata d'ufficio o a seguito di un interpello del titolare, quando vi sono rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità degli interessati. A questo fine, il Garante ha prescritto, quale misura opportuna per favorire il rispetto delle previsioni di legge, di sottoporre alla verifica preliminare dell'Autorità (anche in tal caso, con eventuali provvedimenti di carattere generale) i sistemi di videosorveglianza che prevedono una raccolta delle immagini collegata e/o incrociata e/o confrontata con altri particolari dati personali (ad es. biometrici), oppure con codici identificativi di carte elettroniche o con dispositivi che rendono identificabile la voce. La verifica preliminare del Garante occorre anche in caso di digitalizzazione o indicizzazione delle immagini (che rendono possibile una ricerca automatizzata o nominativa) e in caso di videosorveglianza c.d. dinamico-preventiva che non si limiti a riprendere staticamente un luogo, ma rilevi percorsi o caratteristiche fisionomiche (es. riconoscimento facciale) o eventi improvvisi, oppure comportamenti anche non previamente classificati. **Notificazione** Gli stessi trattamenti devono essere notificati al Garante solo se rientrano in casi specificatamente previsti (art. 37 del Codice). A tale riguardo l'Autorità ha disposto che non vanno comunque notificati i trattamenti relativi a comportamenti illeciti o fraudolenti, quando riguardano immagini o suoni conservati temporaneamente per esclusive finalità di sicurezza o tutela delle persone o del patrimonio.

	Autorizzazioni I trattamenti soggetti a verifica preliminare devono essere autorizzati preventivamente dal Garante, anche attraverso autorizzazioni generali, quando riguardano dati sensibili o giudiziari (ad esempio in caso di riprese di persone malate o di detenuti). Non devono essere sottoposti all'esame preventivo del Garante, a meno che l'Autorità lo abbia disposto, i trattamenti di dati a mezzo videosorveglianza, fuori dei casi indicati nel precedente punto "verifica preliminare".
5. Si devono fornire alle persone che possono essere riprese indicazioni chiare, anche se sintetiche, che avvertano della presenza di impianti di videosorveglianza, fornendo anche le informazioni necessarie ai sensi dell'art. 10 della legge n. 675/1996. Ciò è tanto più necessario quando le apparecchiature non siano immediatamente visibili.	**Informativa** Gli interessati devono essere informati che stanno per accedere o che si trovano in una zona videosorvegliata e dell'eventuale registrazione; ciò anche nei casi di eventi e in occasione di spettacoli pubblici (concerti, manifestazioni sportive) o di attività pubblicitarie (attraverso *web cam*). L'informativa agli interessati deve essere fornita con gli elementi previsti dal Codice, anche con formule sintetiche, ma chiare e senza ambiguità, e non solo mediante pubblicazione, oppure attraverso una temporanea affissione di manifesti. Tali soluzioni possono concorrere ad assicurare trasparenza in materia, ma non sono di per sé sufficienti per l'informativa che deve aver luogo nei punti e nelle aree in cui si svolge la videosorveglianza. Tuttavia il Garante ha individuato ai sensi dell'art. 13, comma 3, della legge un modello semplificato di informativa "minima", riportato alla fine del presente Capo, che può essere utilizzato, in particolare, in aree esterne, fuori dei casi di verifica preliminare indicati nel punto successivo. Il modello è ovviamente adattabile a varie circostanze. In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, vanno installati più cartelli. In luoghi diversi dalle aree esterne il modello va integrato con almeno un avviso circostanziato che riporti gli elementi indicati dal predetto art. 13, con particolare riguardo alle finalità e all'eventuale conservazione. Il supporto con l'informativa: • deve essere collocato nei luoghi ripresi o nelle immediate vicinanze, non necessariamente a contatto con la telecamera; • deve avere un formato ed un posizionamento tale da essere chiaramente visibile; • può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati se le immagini sono solo visionate o anche registrate.

6. **Occorre rispettare scrupolosamente il divieto di controllo a distanza dei lavoratori e le precise garanzie previste al riguardo (art. 4 legge 300/1970).**	Nelle attività di sorveglianza occorre rispettare il divieto di controllo a distanza dell'attività lavorativa e ciò anche in caso di erogazione di servizi per via telematica mediante c.d. "*web contact center*". Vanno poi osservate le garanzie previste in materia di lavoro quando la videosorveglianza è impiegata per esigenze organizzative e dei processi produttivi, ovvero è richiesta per la sicurezza del lavoro. Queste garanzie vanno osservate sia all'interno degli edifici, sia in altri luoghi di prestazione di lavoro (é illegittima l'installazione di sistemi di videosorveglianza in luoghi riservati esclusivamente ai lavoratori o non destinati all'attività lavorativa (ad es. bagni, spogliatoi, docce, armadietti e luoghi ricreativi).
7. **Occorre determinare con precisione il periodo di eventuale conservazione delle immagini, prima della loro cancellazione, e prevedere la loro conservazione solo in relazione a illeciti che si siano verificati o a indagini delle autorità giudiziarie o di polizia.**	In applicazione del principio di proporzionalità, anche l'eventuale conservazione temporanea dei dati deve essere commisurata al grado di indispensabilità e per il solo 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 degli uffici, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria. Un eventuale allungamento dei tempi di conservazione deve essere valutato come eccezionale e comunque in relazione alla necessità derivante da un evento già accaduto o realmente incombente, oppure alla necessità di custodire o consegnare una copia specificamente richiesta dall'autorità giudiziaria o di polizia giudiziaria in relazione ad un'attività investigativa in corso. Il sistema impiegato deve essere programmato in modo da operare al momento prefissato - ove tecnicamente possibile - la cancellazione automatica da ogni supporto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.

8. **Occorre designare per iscritto i soggetti - responsabili e incaricati del trattamento dei dati (artt. 8 e 19 della legge 675/1996) - che possono utilizzare gli impianti e prendere visione delle registrazioni, avendo cura che essi accedano ai soli dati personali strettamente necessari e vietando rigorosamente l'accesso di altri soggetti, salvo che si tratti di indagini giudiziarie o di polizia.**	Si devono designare per iscritto tutte le persone fisiche, incaricate del trattamento, autorizzate ad utilizzare gli impianti e, nei casi in cui è indispensabile per gli scopi perseguiti, a visionare le registrazioni. Deve trattarsi di un numero molto ristretto di soggetti, in particolare quando ci si avvale di una collaborazione esterna. Vanno osservate le regole ordinarie anche per ciò che attiene all'eventuale designazione di responsabili del trattamento, avendo particolare cura al caso in cui la Regione Lazio si avvalga di un organismo esterno anche di vigilanza privata. La designazione dei responsabili ed incaricati "esterni" è effettuata solo se l'organismo esterno svolge prestazioni strumentali e subordinate alle scelte del titolare del trattamento.

	Quando i dati vengono conservati - naturalmente per un tempo limitato in applicazione del principio di proporzionalità - devono essere previsti diversi livelli di accesso al sistema e di utilizzo delle informazioni, avendo riguardo anche ad eventuali interventi per esigenze di manutenzione. Occorre prevenire possibili abusi attraverso opportune misure basate in particolare su una "doppia chiave" fisica o logica che consentano una immediata ed integrale visione delle immagini solo in caso di necessità (da parte di addetti alla manutenzione o per l'estrazione dei dati ai fini della difesa di un diritto o del riscontro ad una istanza di accesso, oppure per assistere la competente autorità giudiziaria o di polizia giudiziaria). Va infatti tenuto conto che l'accessibilità regolamentata alle immagini registrate da parte degli addetti è fattore di sicurezza. Sono, infine, opportune iniziative periodiche di formazione degli incaricati sui doveri, sulle garanzie e sulle responsabilità, sia all'atto dell'introduzione del sistema di videosorveglianza, sia in sede di modifiche delle modalità di utilizzo.
9. **I dati raccolti per determinati fini (ad esempio, ragioni di sicurezza, tutela del patrimonio) non possono essere utilizzati per finalità diverse o ulteriori (ad esempio, pubblicità, analisi dei comportamenti di consumo), salvo le esigenze di polizia o di giustizia, e non possono essere diffusi o comunicati a terzi.**	La Regione Lazio può effettuare attività di videosorveglianza solo ed esclusivamente per svolgere funzioni istituzionali che deve individuare ed esplicitare con esattezza e di cui sia realmente titolare in base all'ordinamento di riferimento. Diversamente, il trattamento dei dati non è lecito. Le specifiche norme di legge o di regolamento e le funzioni legittimamente individuate dalla Regione Lazio costituiscono l'ambito operativo entro il quale il trattamento dei dati si intende consentito. La comunicazione a terzi è lecita solo se espressamente prevista da una norma di legge o di regolamento. Il Codice individua poi specifiche regole volte invece a consentire, in un quadro di garanzie, riprese audio-video a fini di documentazione dell'attività istituzionale di organi pubblici. In tale fattispecie, la Regione Lazio non deve richiedere la manifestazione del consenso degli interessati.

27. Misure di sicurezza

I dati devono essere protetti da idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, perdita, anche accidentale, di accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta. Si applicano, nella fattispecie, le misure di sicurezza previste nel presente atto.

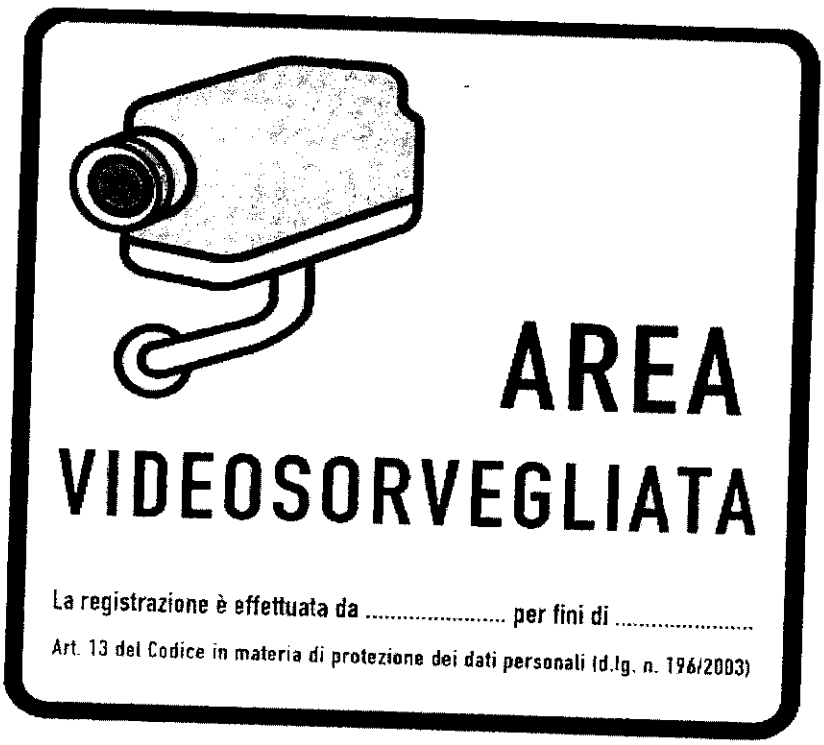
Qualora la Regione Lazio si avvalga di un soggetto esterno deve ricevere dall'installatore una descrizione scritta dell'intervento effettuato che ne attesti la conformità alle regole in materia.

28. Documentazione delle scelte

Le ragioni delle scelte, cui si è fatto richiamo, devono essere adeguatamente documentate in un atto autonomo conservato presso il titolare e il responsabile del trattamento e ciò anche ai fini dell'eventuale esibizione in occasione di visite ispettive, oppure dell'esercizio dei diritti dell'interessato o di contenzioso.

29. 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 e di ottenere l'interruzione di un trattamento illecito, in specie quando non sono adottate idonee misure di sicurezza o il sistema è utilizzato da persone non debitamente autorizzate.



- Se le immagini non sono registrate, sostituire il termine "registrazione" con quello di "rilevazione".

CAPO V

Informazione e formazione

30. L'informazione e la formazione degli incaricati al trattamento dei dati

Il Direttore del Dipartimento "Istituzionale", d'intesa con il Direttore della direzione regionale competente in materia di informatica, con il Direttore della direzione regionale competente in materia di formazione, con il dirigente della struttura competente in materia di trattamento dei dati personali e con i responsabili del trattamento, elabora sia il "manuale per la sicurezza" da aggiornarsi almeno ogni due anni e, comunque, ogni qualvolta si renda necessario, sia il piano annuale di formazione e/o di aggiornamento degli stessi incaricati, come iscritti nell'apposito elenco.

Il responsabile del trattamento può provvedere ad elaborare un'apposita appendice con la quale personalizza il manuale per la sicurezza sulla base di particolari esigenze organizzative della struttura.

Il manuale per la sicurezza viene consegnato agli incaricati contestualmente alle credenziali di autenticazione.

Il Direttore della Direzione regionale competente in materia di informatica provvede ad informare tempestivamente i responsabili del trattamento di ogni eventuale problema di sicurezza di cui dovesse venire a conoscenza.

Il responsabile del trattamento provvede, anche per il tramite del Dirigente della struttura di coordinamento delle attività per il trattamento dei dati personali e/o del Direttore della Direzione regionale competente in materia di informatica, ad informare tempestivamente gli incaricati:

- della presenza di virus negli elaboratori dell'ufficio;
- di comportamenti da parte del personale non conformi alle disposizioni di sicurezza;
- della periodica necessità di variazione delle credenziali di autenticazione da parte degli incaricati;
- della disponibilità di programmi di aggiornamento relativi all'antivirus.

Il Direttore del Dipartimento "Istituzionale", d'intesa con il Dirigente della struttura di coordinamento delle attività per il trattamento dei dati personali, il Direttore della Direzione regionale competente in materia di informatica e i responsabili dei trattamenti dei dati, verifica ogni anno, entro il 31 dicembre, le necessità di formazione del personale incaricato del trattamento dei dati con lo scopo di fornire ogni informazione necessaria a migliorare la sicurezza del trattamento nonché per rendere edotti gli incaricati stessi dei rischi individuati e dei modi per prevenirne i danni.

31. Revisioni

Il presente documento verrà revisionato annualmente ed, eventualmente, sottoposto a modifiche.