LINEE GUIDA PER I RESPONSABILI

Azienda USL 1 di Sassari

Le misure di sicurezza per la tutela della privacy dei dati personali e sensibili

Documento	DPS-LGR01/1
Edizione	21/11/2005

Introduzione

L'**autorità Garante della Privacy**, istituita nel 1996, si propone di tutelare il diritto alla privacy di tutti, sia che si tratti di persone fisiche ovvero di persone giuridiche, enti o associazioni. Vengono quindi focalizzati tutti i processi aziendali che interessano dati personali, entrando nel merito delle finalità e della liceità dei "trattamenti" che vengono effettuati.
In questo contesto l'Azienda USL 1 di Sassari, in qualità di titolare dei trattamenti dei dati necessari per l'espletamento della propria missione, dopo aver provveduto agli adempimenti previsti dalla Legge, intende sensibilizzare tutto il personale alle misure di sicurezza per la tutela dei dati e della Privacy.
Queste "linee guida" sono in particolare destinate ai Responsabili di strutture semplici o complesse, per ricordare la Responsabilità di ciascuno nell'osservare le direttive aziendali in materia di Responsabilità e misure di sicurezza in azienda.
Le "linee guida" sono state strutturate nei seguenti capitoli:

- Il Decreto Legislativo 196/03 in sintesi – per illustrare gli aspetti fondamentali del testo unico e fornire utili riferimenti per eventuali approfondimenti sulla materia
- L'organizzazione per la sicurezza – per illustrare la ripartizione delle Responsabilità e dei compiti per la tutela dei dati personali nel contesto operativo dell'Azienda USL 1 di Sassari.
- Le misure di sicurezza – per fornire indicazioni sulle misure di sicurezza adottate in azienda, alle quali tutti devono attenersi
- L'affidamento di dati personali all'esterno – per illustrare i criteri applicati per garantire l'adozione delle misure minime di sicurezza, in caso di trattamenti di dati personali affidati all'esterno
- Il controllo generale sullo stato della sicurezza -- le procedure previste per il controllo sullo stato della sicurezza

Indice del Contenuto

1 Il Decreto Legislativo 196/03 in sintesi

Il "Testo Unico sulla Privacy" (Dlgs.196/03) entrato in vigore il primo gennaio 2004, riprende ed integra la normativa introdotta dalla Legge 675/96 e dal DPR.318/99, prevedendo l'obbligo di garantire la sicurezza, l'integrità e la disponibilità dei dati personali.
Citiamo per chiarezza alcuni passaggi significativi del codice:

Diritto alla protezione dei dati personali: art. 1 del TU

"Chiunque ha diritto alla protezione dei dati personali che lo riguardano."

Come si nota, l'art.1 introduce nell'ordinamento il "diritto alla protezione dei dati personali", diritto fondamentale della persona, autonomo rispetto al più generale diritto alla riservatezza: un diritto che tiene conto delle molteplici prerogative legate al trattamento dei dati personali, anche oltre quelle attinenti al riserbo e alla tutela della vita privata.
In tal modo il legislatore italiano si adegua al quadro normativo comunitario che, nella Carta dei diritti del cittadino europeo, garantisce già tale diritto fondamentale (art. 8) che si accinge ad assumere una connotazione ancora più solenne nel quadro dei lavori della Convenzione europea.

Principio di necessità nel trattamento dei dati: art. 3 del TU

"I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità."

L'art. 3 introduce il "principio di necessità" nel trattamento dei dati personali, in base al quale, sin dalla loro configurazione, i sistemi informativi ed i software devono essere predisposti in modo da assicurare che i dati personali o identificativi siano utilizzati solo se indispensabili per il raggiungimento delle finalità consentite, e non anche quando i medesimi obiettivi possano essere raggiunti mediante l'uso di dati anonimi o che comunque consentano una più circoscritta identificazione degli interessati.
Il principio introdotto integra e completa, con riferimento alla configurazione stessa dell'ambiente in cui i dati sono trattati, il principio di pertinenza e non eccedenza dei dati trattati già operante in relazione al trattamento dei medesimi dati (art. 11, già art. 9, l. n. 675/1996).
Si tratta di una regola di ordine generale in specie per i sistemi e i programmi che verranno d'ora in poi predisposti.

Con il testo unico, che assume le caratteristiche di un vero e proprio "codice privacy e sicurezza", il legislatore ha provveduto a coordinare le norme sinora vigenti in materia, apportando inoltre numerose integrazioni e modificazioni, anche per assicurare una migliore e più chiara attuazione della normativa.

1.1 La struttura del TU

Il nuovo **codice** si compone di tre parti, che contengono, rispettivamente:

1. le **disposizioni generali** (articoli da 1 a 45), riguardanti le regole *sostanziali* della disciplina del trattamento dei dati personali, applicabili a tutti i trattamenti, nonché le regole specifiche che si devono osservare per i trattamenti effettuati da soggetti *pubblici* e quelle che trovano applicazione per i trattamenti effettuati da soggetti *privati* e da *enti pubblici economici;*
2. le **disposizioni particolari**, che si applicano per specifici trattamenti (articoli da 46 a 140), ad integrazione o eccezione alle disposizioni generali, contenute nella Prima parte;
3. le disposizioni relative alle **azioni di tutela** dell'interessato e al **sistema sanzionatorio** (articoli da 141 a 172), cui si aggiungono le norme di modifica, finali e di carattere transitorio (articoli da 173 a 186).

Il codice è completato da **tre allegati**, le cui disposizioni si devono quindi intendere come parte integrante dello stesso, contenenti quanto segue:

- i **codici di deontologia** (*allegato A*), a partire dai tre che risultano ad oggi approvati (riguardanti rispettivamente l'attività giornalistica, gli scopi storici e gli scopi statistici nell'ambito del SISTAN - Sistema statistico nazionale), ai quali andranno ad aggiungersi quelli di futura approvazione;
- il **disciplinare tecnico in materia di misure minime di sicurezza** (*allegato B*), il quale potrà essere adeguato all'evoluzione del settore, in modo flessibile, con decreti ministeriali non regolamentari;
- l'elenco dei trattamenti non occasionali effettuati in **ambito giudiziario o per fini di polizia** (*allegato C*), che in sede di prima applicazione della normativa dovranno essere individuati, entro il 30 giugno 2004, dai Ministeri competenti.

Come utile riferimento, in allegato è riprodotto l'indice completo del decreto legislativo sopra citato, dal quale si può apprezzare come il Garante abbia ha voluto strutturare questo Testo Unico.

1.2 Definizioni

Citando l'art 4 del TU:
a**) "trattamento"**, qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;
b) **"dato personale",** qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
c) **"dati identificativi",** i dati personali che permettono l'identificazione diretta dell'interessato;
d) **"dati sensibili",** i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
e) **"dati giudiziari",** i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;
f) **"titolare",** la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
g) **"Responsabile",** la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;
h**) "Incaricati",** le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal Responsabile;
i**) "interessato",** la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;
l) **"comunicazione",** il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal Responsabile e dagli Incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
m) **"diffusione",** il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
n) **"dato anonimo",** il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
o**) "blocco",** la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;
p) **"banca di dati",** qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

q) **"Garante",** l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

E' opportuno evidenziare che il nuovo codice ha ufficializzato i seguenti punti, che si erano già affermati nella pratica e nelle interpretazioni fornite dal Garante:
-- tra le decisioni che competono al titolare vi sono anche quelle in merito alla delega operativa ai Responsabili e agli strumenti utilizzati per trattare i dati personali;
-- il ruolo di Incaricato del trattamento può essere rivestito solo da una persona fisica; quindi non da società ed enti.

1.3 Due parole sulla natura dei dati personali

Dalla definizione di partenza si desume innanzitutto che il dato personale è una **informazione su un soggetto**, sia esso una persona fisica, una persona giuridica, un ente od una associazione: ciò porta ad escludere dalla definizione la semplice combinazione di nome, cognome, luogo e data di nascita di una persona.

La frase Mario Rossi, nato il 25 febbraio 1958 a Milano non è un dato sensibile, in quanto prende oggettivamente atto dell'esistenza dell'individuo Mario Rossi, senza fornire alcuna informazione in merito alla vita del suddetto. Lo stesso può dirsi per la semplice denominazione di una società.
Ma ciò è sempre vero? Per i Mario Rossi di tutto il mondo sicuramente sì. E per Abramo Levi, nato a Tel Aviv il 12 febbraio 1958?

In questo caso la semplice combinazione di elementi anagrafici "di base" può svelare una precisa informazione in merito alla religione ed al gruppo etnico di appartenenza del soggetto: informazione che, per inciso, è definita dalla legge come "sensibile", e quindi meritevole di particolare tutela.
Questo esempio induce a formulare una prima riflessione: in taluni casi il confine tra ciò che è "dato sensibile" e ciò che non lo è sfuma, e la risposta in merito dipende in ultima analisi dalle **concrete finalità** perseguite da chi possiede e tratta i dati.

Se, ad esempio, il fine fosse semplicemente di annotare i dati anagrafici di Abramo Levi per fargli gli auguri di compleanno, non si sarebbe nel campo dei dati sensibili. Se invece tale dato fosse utilizzato da un commerciante di oggettistica religiosa, l'informazione assurgerebbe al rango di dato sensibile, in quanto in tale contesto non rileverebbero i dati anagrafici dell'individuo, ma la sua appartenenza ad una religione.

Nella frase *Abramo Levi è di religione ebraica* il vero dato sensibile è cioè costituito dalla appartenenza del soggetto ad una precisa categoria di individui (le persone di religione ebraica). La combinazione di nome e cognome (Abramo Levi) diventa rilevante, solo in quanto essa viene usata come strumento per riferire una situazione o una qualità ad un determinato individuo.

Tornando a Mario Rossi, Mario Rossi, residente in Piazza del Popolo 2, Firenze è invece certamente un dato personale, in quanto fornisce l'informazione su dove il suddetto individuo risieda.
Così come è un dato personale Sigma Spa, con sede in via dell'Industria 2, Milano, poiché la legge estende il proprio ambito di applicazione ai dati che concernono persone giuridiche, enti ed associazioni, con la sola esclusione degli Organi che costituiscono la Pubblica Amministrazione.

La legge trova applicazione anche per i dati che riguardano **soggetti non residenti**: sono quindi ad esempio considerati dati personali, e come tali vanno trattati, quelli di *John Smith di New York*, piuttosto che della *Ford Inc. di Detroit*.
In una decisione presa nel 1999, il Garante ha precisato che l'espressione **qualunque informazione** vuole evidentemente attribuire alla definizione di *dato personale* la massima ampiezza, comprendendo anche ogni notizia, informazione o elemento che abbia un'efficacia informativa tale, da fornire un contributo aggiuntivo di conoscenza rispetto ad un soggetto identificato od identificabile.

E ciò in riferimento sia ad informazioni **oggettivamente caratterizzate**, suscettibili di una verifica e di un sindacato obiettivo (es. indirizzo e numero di telefono; dato relativo alle ore di servizio prestate da un dipendente, in un determinato arco temporale), che a **descrizioni, giudizi, analisi o ricostruzioni di profili personali**, che danno origine a stime ed opinioni di natura soggettiva, finalizzate anche ad una valutazione complessiva del soggetto interessato.
Esempi di **valutazioni di carattere soggettivo**, che sono a tutti gli effetti considerate dati personali, sono:

- le valutazioni, effettuate da una banca, sul grado di affidabilità di un soggetto che richiede un finanziamento, nonché le eventuali motivazioni anche "interne" che sono alla base del rifiuto di concederlo;
- una diagnosi medica, anche per la parte che comprende elementi valutativi o di prognosi di tipo discrezionale;
- le note di qualifica, cioè le valutazioni che contribuiscono a formare il giudizio annuale sul rendimento di un dipendente.
-

Si sono citate le tipologie di dati che, scorrendo i ricorsi decisi dal Garante, più di frequente sono oggetto di contenzioso, che si conclude inevitabilmente con la condanna di chi effettua il trattamento, per avere negato l'accesso ai soggetti cui tali dati si riferiscono.

Con queste considerazioni in mente, è opportuno quindi pensare che qualunque dato aziendale merita attenzione da parte di chi lo tratta, non solo per la sua possibile valenza come dato di natura personale, ma anche per l'importanza che esso riveste per l'azienda stessa.

1.4 L'uso degli strumenti informatici

Avendo introdotto un netto distinguo tra il trattamento effettuato con e senza strumenti elettronici, il legislatore ha ritenuto opportuno scendere nel dettaglio delle modalità di accesso alle informazioni e il trattamento avviene con l'ausilio di strumenti informatici.

L'adozione di adeguate misure di sicurezza è resa obbligatoria per tutti i soggetti che trattano dati personali, con particolare attenzione per quelli sensibili e giudiziari.

Con il DL 196/2003 viene anche esplicitato il quadro delle **misure minime di sicurezza** (art. 33 T.U.), che configurano il livello minimo di protezione richiesto dalla normativa per contrastare i rischi di perdita, di alterazione, di distruzione e di uso improprio dei dati.
Egli ha quindi utilizzato i termini "autenticazione/autorizzazione" per regolamentare l'accesso alle informazioni con l'ausilio di strumenti informatici.
Questo comporta che l'utente (titolare, Responsabile od Incaricato) autorizzato al trattamento debba possedere quelle che sono indicate come "credenziali di autenticazione"

- un **nome utente** ed una **password** di accesso ai sistemi; tali informazioni devono essere note solo ed esclusivamente all'utente autorizzato all'accesso ai dati;
- **dispositivo di autenticazione**; è previto l'impiego di tecnologie che utilizzano dispositivi fisici per l'autenticazione ai sistemi (badge, smart cards, etc.)
- caratteristiche **biometriche**, ovvero utilizzo di dispositivi di rilevazione biometrica (impronta digitale, iride, etc) che possono essere associati ad una password;

Citiamo per maggiore chiarezza altri estratti significativi del decreto legge:

Obblighi di sicurezza : art. 31 del T.U.
"I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati ed alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche

accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta".

Misure minime di sicurezza : art. 33 del T.U.

"Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.

L'adozione delle Misure Minime di Sicurezza è obbligatoria per tutti coloro che effettuano trattamenti di dati personali."

Sanzioni : art. 169 del T.U.

"Chiunque, essendovi tenuto, omette di adottare il misure minime previste dall'art. 33 è punito con l'arresto sino a due anni o con l'ammenda da diecimila euro a cinquantamila euro."

2 L'organizzazione per la sicurezza

L'Azienda Unità Sanitaria 1 di Sassari, nella consapevolezza che un sistema complesso quale la sicurezza può funzionare solo se i suoi meccanismi sono formalizzati e verificabili, nonché posti in essere da personale adeguatamente formato e motivato, per l'applicazione e la gestione della normativa sulla privacy, ha provveduto ad adottare la seguente organizzazione per la sicurezza.

2.1 Titolare del Trattamento

Ai sensi dell'art.4, lett. f) del Codice in materia di protezione dei dati personali, il Titolare dei trattamenti è l'ASL1 di Sassari nella persona del Direttore Generale.

Per Titolare si intende la persona fisica, persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, in piena autonomia, le decisioni in ordine alle finalità e alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza. Il titolare, in quanto tale, è Responsabile dell'analisi e della valutazione dei rischi che incombono sui dati e dell'applicazione delle misure minime di sicurezza.
Il Titolare ha a facoltà di nominare uno o più Responsabili che possono essere interni o esterni, impartendo loro le direttive alle quali essi sono tenuti ad attenersi nella gestione e trattamento dei dati personali che gli sono stati affidati;
Il Titolare verificherà periodicamente che le istruzioni e le norme di legge in tema di privacy vengano correttamente applicate dai Responsabili.

2.2 Responsabili del Trattamento

Il Titolare, nella persona del Direttore Generale dell'Azienda USL N. 1 di Sassari, ha nominato Responsabili dei Trattamenti tutti i Dirigenti di Struttura Semplice o Complessa dell'Azienda.

I compiti dei Responsabili i sono i seguenti:

- nominare gli Incaricati ovvero le persone fisiche ai quali, all'interno della propria struttura, è affidato il compito di trattare i dati personali;
- impartire istruzioni precise e dettagliate agli Incaricati;
- controllare le attività degli Incaricati, procedendo a verifiche periodiche, in conformità alle direttive dei Titolari/Contitolari;
- informare l'interessato (ovvero il soggetto cui i dati si riferiscono) sulle modalità e finalità del trattamento e raccoglierne il consenso, ove previsto dalla normativa;
- rispondere alle istanze avanzate dall'interessato o da un suo Incaricato.

2.3 Responsabile per la Sicurezza Informatica

il Titolare, nella persona del Direttore Generale dell'Azienda USL N. 1 di Sassari, ha nominato Responsabile della Sicurezza Informatica il dirigente Responsabile del Sistema Informativo ed Informatico.

Il Responsabile del Sistema Informativo ed Informatico dell'Azienda USL n°1 di Sassari, è nominato Responsabile della Sicurezza Informatica, ed in tale veste gli viene affidata la pianificazione, l'organizzazione, l'attuazione (anche mediante l'eventuale ricorso a qualificati soggetti esterni) delle infrastrutture informatiche centralizzate, delle procedure e di tutte le iniziative aziendali ritenute necessarie ed opportune per progressivamente migliorare le misure di sicurezza informatica indispensabili a garantire la sicurezza dei trattamenti effettuati con strumenti elettronici.

In particolare, al Responsabile per la Sicurezza Informatica sono assegnati i compiti di:

- raccogliere le informazioni da ciascun Responsabile per elaborare la mappa dei trattamenti di dati personali, effettuati dall'Azienda, combinando la tipologia dei dati trattati con gli strumenti che vengono impiegati per il trattamento;
- sulla base di tale mappa, effettuare una analisi dei rischi che gravano sui dati informatizzati e sugli strumenti, identificando di conseguenza gli elementi da proteggere e le minacce cui essi sono sottoposti;
- sulla base dell'analisi dei rischi, definire i requisiti di sicurezza da adottare, per proteggere il complesso degli archivi elettronici di dati personali, delle procedure e dei sistemi informativi esistenti, osservando quanto prescritto dal Dlgs 196/2003 e dal relativo disciplinare tecnico allegato sub B);
- progettare, implementare e progressivamente migliorare il sistema di sicurezza dei sistemi informativi e dell'infrastruttura informatica aziendale, in base ai requisiti definiti nel punto precedente, mediante l'adozione delle opportune misure centralizzate e decentrate:
    - organizzative, che si sostanziano nella definizione di una serie di norme e procedure, miranti a regolamentare l'aspetto organizzativo del processo di sicurezza dei trattamenti effettuati con strumenti elettronici;
    - fisiche, il cui scopo è di proteggere le aree, le apparecchiature informatiche e i dati da eventi di natura accidentale e da intrusioni di personale non autorizzato o di terzi;
    - logiche, il cui campo di applicazione riguarda la protezione delle informazioni, con particolare riferimento a quelle gestite con i sistemi informativi (dati, applicazioni, sistemi e reti);
- pianificare e curare l'attuazione, anche a cura di soggetti specializzati esterni, degli interventi di monitoraggio della sicurezza e dei test di penetrazione e predisporre un piano di controlli periodici, da eseguirsi con cadenza almeno annuale, dell'efficacia delle misure di sicurezza adottate;
- assicurarsi che siano adeguatamente predisposti e mantenuti in efficienza sistemi e procedure di ripristino dei dati, nel caso in cui essi siano colpiti da eventi che possano danneggiarli o addirittura distruggerli, con l'obiettivo di renderli nuovamente disponibili entro un lasso di tempo ragionevole, avendo riguardo all'efficienza dell'organizzazione;
- garantire che sia effettuata la manutenzione del sistema di sicurezza informatica, per assicurarne la costante efficienza e disponibilità, nonché procedere al suo aggiornamento periodico, per renderlo sempre adeguato alle nuove minacce;
- programmare e curare la realizzazione del piano di formazione del personale dell'organizzazione, in tema di sicurezza, finalizzato anche alla emanazione ed al rispetto di procedure interne inerenti la sicurezza (regolamentazione degli accessi fisici e logici agli archivi ed ai sistemi informativi, norme operative di utilizzo e gestione dei sistemi, gestione delle password, ecc…..);
- verificare che i soggetti esterni, cui l'Azienda dovesse affidare il trattamento di dati personali informatizzati, adottino misure di sicurezza conformi a quelle minime, previste dagli articoli da 33 a 35 Dlgs 196/2003 e dal relativo disciplinare tecnico, allegato sub B) al Dlgs 196/2003 stesso;
- procedere alla redazione e/o all'aggiornamento annuale (eventualmente avvalendosi di qualificati soggetti specializzati esterni), entro il 31 marzo di ogni anno, del Documento Programmatico sulla Sicurezza, che provvederà a firmare per approvazione.

Il Responsabile per la Sicurezza ha il compito di progressivamente definire e consolidare le "linee guida" e le istruzioni generali in merito ai seguenti punti, aventi specifica attinenza con la sicurezza nell'uso degli strumenti informatici:

- procedure da seguire per la classificazione dei dati, al fine di distinguere quelli sensibili e giudiziari, per garantire la sicurezza dei quali occorrono maggiori cautele, rispetto a quanto è previsto per i dati di natura comune;
- modalità per elaborare e custodire le password, necessarie per accedere agli elaboratori elettronici ed ai dati in essi contenuti, nonché per fornirne una copia al preposto alla custodia delle parole chiave;
- procedure da seguire per non lasciare incustoditi e accessibili gli strumenti elettronici, mentre è in corso una sessione di lavoro;
- procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi;
- procedure per il salvataggio dei dati e verifica della loro ripristinabilità;
- modalità di custodia ed utilizzo dei supporti rimuovibili, contenenti dati personali.

Ai soggetti incaricati della gestione e manutenzione del sistema informativo, siano essi interni o esterni all'Azienda, viene prescritto di non effettuare alcun trattamento, sui dati personali contenuti negli strumenti elettronici, fatta unicamente eccezione per i trattamenti di carattere temporaneo strettamente necessari per effettuare la gestione o manutenzione del sistema.

2.4 Incaricati

Il Titolare, nella persona del Direttore Generale dell'Azienda USL N. 1 di Sassari, ha assegnato ai Responsabili la delega per la designazione obbligatoria degli Incaricati, avvalendosi della modalità semplificata introdotta dall'art. 30, comma 2, del Codice per individuare l'ambito di trattamento consentito agli addetti alle strutture e alle unità organizzative di pertinenza.

L'Incaricato assume, in ordine al trattamento, funzioni operative in aderenza a specifiche istruzioni ricevute dal Titolare o dal Responsabile.
La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito; si considera tale, secondo la normativa anche la documentata preposizione della persona fisica ad una unità organizzativa ove viene individuato l'ambito del trattamento consentito agli addetti all'unità medesima.
Le operazioni di trattamento di dati personali possono essere effettuate solo dagli Incaricati che operano sotto la diretta autorità del Titolare o dei Responsabili.
Oltre alle istruzioni generali, su come devono essere trattati i dati personali, agli Incaricati vengono fornite esplicite istruzioni in merito ai seguenti punti, aventi specifica attinenza con la sicurezza:

- procedure da seguire per la classificazione dei dati, al fine di distinguere quelli sensibili e giudiziari, per garantire la sicurezza dei quali occorrono maggiori cautele, rispetto a quanto è previsto per i dati di natura comune;
- modalità di reperimento dei documenti, contenenti dati personali, e modalità da osservare per la custodia degli stessi e la loro archiviazione, al termine dello svolgimento del lavoro per il quale è stato necessario utilizzare i documenti;
- modalità per elaborare e custodire le password, necessarie per accedere agli elaboratori elettronici ed ai dati in essi contenuti, nonché per fornirne una copia al preposto alla custodia delle parole chiave;
- prescrizione di non lasciare incustoditi e accessibili gli strumenti elettronici, mentre è in corso una sessione di lavoro;
- procedure e modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi;
- procedure per il salvataggio dei dati;

- modalità di custodia ed utilizzo dei supporti rimuovibili, contenenti dati personali;
- dovere di aggiornarsi, utilizzando il materiale e gli strumenti forniti dal Titolare, sulle misure di sicurezza.

Si tenga presente che tutto il personale medico e amministrativo dell'Azienda USL (medici, paramedici ed impiegati amministrativi) che in qualche misura svolge attività che implicano il trattamento di dati personali, con particolare attenzione per quelli sensibili e giudiziari, dovrà essere designato quale Incaricato dei trattamenti di competenza.

3 Le misure di sicurezza

3.1 Non c'è privacy senza sicurezza

La questione sicurezza non riguarda infatti i soli dati trattati elettronicamente. Tale aspetto è oggi certo di primaria importanza, ma non è l'unico. La sicurezza si ottiene anche con l'uso delle tradizionali chiavi e con la vigilanza delle strutture esterne e dei locali.
Ma non basta ancora, perché si è finora parlato delle ***misure di sicurezza fisiche***, accennato a quelle ***logiche legate all'informatica***, ma non si deve dimenticare l'aspetto più importante: le ***misure organizzative***, il cui fine è di fare in modo che l'intera struttura adotti comportamenti conformi ai principi della sicurezza e, più in generale, della privacy.

A nulla serve essere estremamente scrupolosi nel trattamento dei dati, inviando informative, acquisendo consensi ed autorizzazioni, aggiornandoli con maniacale puntualità, se si lasciano poi i supporti contenenti i dati incustoditi sulla scrivania, alla mercé di chiunque possa entrare nell'ufficio.

3.2 L'insieme delle misure di sicurezza

La sicurezza non deve essere intesa solo come protezione da eventi negativi, accidentali o intenzionali, ma anche come limitazione degli effetti causati dall'eventuale verificarsi di tali eventi di:

- **distruzione o perdita, anche accidentale, dei dati**: ossia si deve impedire che dati, informazioni e risorse siano resi irreperibili da persone, mediante processi non autorizzati, o da eventi accidentali. Nel mondo mondo informatico si ricorre la concetto di ***disponibilità del dato,*** in tale ambito assume inoltre una particolare valenza il requisito della ***integrità del dato***, che deve essere quello originario o legittimamente modificato, in relazione alla relativa facilità di procedere fraudolentemente a modifiche senza lasciare indizi;
- **accesso non autorizzato ai dati**: nel mondo fisico è immediato pensare ad estranei, che nella notte si introducono in un'azienda per rubare dei dati o farne delle copie, piuttosto che a personale dell'azienda stessa che viola determinati archivi durante l'orario di lavoro. Nel mondo informatico si parla di ***confidenzialità*** o ***riservatezza,*** con ciò intendendosi che un determinato dato deve essere accessibile solo a chi è autorizzato: si dovrà quindi fare in modo che il personale non possa consultare files che non lo riguardano; che estranei non possano accedere abusivamente al sistema informativo; che durante la trasmissione di dati da un computer ad un altro, dei malintenzionati non intercettino i messaggi per violare le informazioni in essi contenuti. Correlato a tali aspetti vi è il requisito della ***autenticità*** dei dati, che concerne la garanzia e certificazione della loro provenienza;
- trattamento non consentito o non conforme alle finalità della raccolta.

Si noti che la legge parla realisticamente di "riduzione al minimo", non di eliminazione dei rischi, nella consapevolezza che il raggiungimento di tale assoluto obiettivo è di fatto quasi impossibile, di fronte a tentativi reiterati e sofisticati di violazione della sicurezza delle informazioni da parte di soggetti maleintenzionati .

Un'importante osservazione concerne il fatto che viene preteso un *diverso grado di diligenza*, che varia in funzione della *natura dei dati* e delle *specifiche caratteristiche* del trattamento.

E' ovvio che, per custodire un banale elenco di dati anagrafici di taluni abitanti di una città, non è necessario l'uso di una cassaforte con dieci combinazioni, né l'adozione di altro accorgimento, che non sia di riporre l'elenco nel cassetto dotato della solita serratura.

Chi custodisce un elenco contenente nomi cognomi ed indirizzi di persone affette da gravi problemi di salute, con dovizia descritti, è invece tenuto ad adottare più efficaci accorgimenti, a salvaguardia della sicurezza.

L'insieme delle misure di sicurezza viene quindi concettualmente suddiviso in tre sottoinsiemi, distinguendo le ***misure***:

- ***organizzative***, che si sostanziano nella definizione di una serie di norme e procedure, miranti a regolamentare l'aspetto organizzativo del processo di sicurezza;
- ***fisiche****,* il cui scopo è di proteggere le aree, le apparecchiature, i dati e le persone da eventi di natura accidentale (es. incendi) e da intrusioni, di personale non autorizzato o di terzi;
- ***logiche***, il cui campo di applicazione riguarda la protezione delle informazioni, con particolare riferimento a quelle gestite con i sistemi informativi (dati, applicazioni, sistemi e reti), sia in relazione al loro corretto utilizzo, che in relazione alla loro gestione e manutenzione nel tempo.

3.3 Cosa richiede il Codice

L'obbligo di adottare le misure di sicurezza è ribadito dall'articolo 31 del nuovo codice, che disciplina quelle che sono comunemente definite le ***misure idonee di sicurezza***, in merito alle quali sottolinea che "la norma impone al titolare e al Responsabile, se designato, l'obbligo di custodire e controllare i dati personali oggetto di trattamento mediante l'adozione di idonee e preventive misure di sicurezza, individuabili alla luce delle conoscenza acquisite in base al progresso tecnico in relazione alla natura dei dati ed alle specifiche caratteristiche del trattamento, in grado di ridurre al minimo i rischi".
Si tratta in sostanza dell'obbligo di operare in concreto al fine di ridurre al minimo i rischi mediante l'utilizzazione di sistemi di sicurezza *costantemente adeguati nel tempo*".
Le misure idonee sono quindi "…*non individuate*, ma *individuabili* sulla base delle soluzioni tecniche concretamente disponibili, e la loro mancata predisposizione comporta la Responsabilità per i danni eventualmente cagionati….".
In questo contesto, il Codice fa la distinzione tra:

- le cosiddette ***misure idonee*** (*Capo I del Titolo V della parte I*), che consistono in generale nell'insieme degli accorgimenti che il soggetto che tratta i dati deve adottare, in relazione alla sua specifica situazione, in modo da 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. Dalla mancata adozione, di tali misure, consegue l'obbligo di risarcimento dei danni eventualmente causati;
- le ***misure minime*** (Capo II del Titolo V della parte I), che il comma 3, lettera a) dell'articolo 4 definisce come il complesso delle misure tecniche, informatiche, organizzative, logistiche (leggasi logiche, NdR) e procedurali di sicurezza che configurano il livello minimo di protezione, richiesto in relazione ai rischi previsti nell'articolo 31. La loro adozione è imposta dalla norma, che provvede a descriverle analiticamente, con la conseguenza che sono previste sanzioni di natura penale, in caso di mancata adozione.

In merito alle misure che si devono in concreto adottare, il testo legislativo si limita genericamente a prevedere che si debbano applicare gli strumenti e le conoscenze resi disponibili dal progresso tecnico: non è quindi sufficiente impiantare una serie di misure di sicurezza una volta per tutte, ma ci si deve preoccupare di aggiornarle costantemente.

Tale principio, che è generale e vale quindi per tutte le misure di sicurezza, incluse quelle *fisiche* in senso stretto, assume particolare rilievo per le misure logiche legate al mondo informatico, in relazione al continuo progresso cui esso è soggetto, anche per quanto riguarda la creazione e circolazione di programmi concepiti per violare la altrui sicurezza.

3.4 Gli interventi formativi-informativi degli Incaricati

Gli interventi formativi degli Incaricati del trattamento devono essere programmati in modo tale, che essi abbiano luogo *almeno* al verificarsi di una delle seguenti circostanze:

- già al momento dell'ingresso in servizio;
- in occasione di cambiamenti di mansioni, che implichino modifiche rilevanti rispetto al trattamento di dati personali;
- in occasione della introduzione di nuovi significativi strumenti, che implichino modifiche rilevanti rispetto al trattamento di dati personali.

Gli interventi formativi, che possono avvenire all'interno e/o presso soggetti esterni specializzati, devono essere finalizzati a rendere gli Incaricati edotti dei seguenti aspetti:

- profili della disciplina sulla protezione dei dati personali, più rilevanti in rapporto alle relative attività, e conseguenti Responsabilità che ne derivano;
- rischi che incombono sui dati;
- misure disponibili per prevenire eventi dannosi;
- modalità per aggiornarsi sulle misure minime di sicurezza, adottate dal titolare.

Gli interventi formativi sono una importante componente della più vasta cultura della sicurezza, nel trattamento del patrimonio informativo dell'organizzazione, con particolare riferimento ai dati personali.

3.4.1 Sensibilizzazione e corresponsabilizzazione

La *sensibilizzazione* alle tematiche della sicurezza, ed a costanti comportamenti coerenti con le disposizioni date in merito, deve interessare tutte le risorse umane dell'organizzazione, ad ogni livello di Responsabilità ed attività: ciò al fine di diffondere una cultura generalizzata della sicurezza, che consenta tra l'altro di favorire la miglior efficacia ed efficienza delle misure prese, oltre che di sopperire ad eventuali mancanze delle stesse.

I Responsabili devono tenere presente che le attività relative alla sicurezza non rappresentano un appesantimento del lavoro quotidiano, ma una volta che entrano nel ciclo standard delle operazioni da compiere, contribuiscono a garantire il personale dal rischio di perdere, o comunque compromettere, parte del lavoro fatto.

A titolo di esempio, presentazioni, opuscoli, seminari, riunioni dei dirigenti con i propri collaboratori possono rappresentare opportunità per raggiungere quest'obiettivo.
Per la corresponsabilizzazione, si deve prevedere di:

- coinvolgere i dirigenti e le rappresentanze degli addetti, in tutte le fasi di definizione del piano per la sicurezza
- effettuare interventi di richiamo, e se necessario adottare gli adeguati provvedimenti disciplinari, in caso di inadempienze e/o superficialità in tema di sicurezza.

Analoghi processi devono essere previsti con eventuali partner e per i collaboratori esterni, privati e pubblici, persone fisiche e giuridiche, che interagiscono in modo significativo con l'organizzazione.

3.4.2 Formazione

L'introduzione di un sistema di sicurezza, come di qualunque altro elemento che modifichi le modalità lavorative all'interno di una qualsiasi realtà, ha sicuramente un forte impatto sull'organizzazione.

La formazione interviene in due momenti ben precisi del processo di introduzione di un sistema di sicurezza:

- sensibilizzazione sulle problematiche della sicurezza e sulla loro importanza;
- conoscenza delle misure di sicurezza da adottare, e da gestire ai diversi livelli di Responsabilità.

La formazione, se ben orientata, progettata e realizzata, può essere lo strumento più efficace per realizzare la diffusione delle politiche, degli obiettivi e dei piani dell'organizzazione in tema di sicurezza e per minimizzare quella componente, sempre presente, che consiste nella resistenza al cambiamento.

3.5 La protezione di aree e locali

E' l'insieme delle misura di sicurezza che hanno il compito di prevenire accessi fisici non autorizzati, danni o interferenze con lo svolgimento del lavoro con gli strumenti automatizzati: la protezione delle aree e dei locali, in cui sono situati gli elaboratori, deve essere quindi attivata sia contro eventi dannosi imprevedibili (inondazioni, corti circuiti, ecc.), che contro tentativi di intrusione.
Le contromisure si riferiscono alle protezioni perimetrali dei siti, ai controlli fisici all'accesso, alla sicurezza delle aree dove sono collocati computer (con particolare riferimento a servers) rispetto a danneggiamenti accidentali o intenzionali, alla protezione fisica dei supporti.
Tale obiettivo viene raggiunto attraverso misure di controllo crescenti, correlate ai rischi e al valore dei beni e delle informazioni presenti nell'ambiente. Ne fanno parte le seguenti componenti:

- la classificazione delle aree aziendali (es: aree riservate, aree interne, aree pubbliche);
- l'accesso controllato alle aree considerate critiche;
- la sicurezza fisica (impianti) e la sorveglianza di queste aree;
- la tempestiva rilevazione di eventuali incidenti di sicurezza.

3.6 La custodia e l'archiviazione di atti, documenti e supporti

Per quanto concerne il reperimento, la custodia e l'archiviazione di atti, documenti e supporti removibili di memorizzazione dei dati (ad esempio Tape, CD, dischetti, ecc.), i Responsabili dovranno provvedere ad istruire gli Incaricati, affinché adottino precise procedure atte a salvaguardare la riservatezza dei dati contenuti.

Agli Incaricati verranno date disposizioni di accedere ai soli dati personali, la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati: in caso di dubbi, essi si dovranno rivolgere ad un superiore, o ad un Responsabile del trattamento, o direttamente al titolare.

Agli Incaricati è prescritto di prelevare dagli archivi i soli atti e documenti che vengono loro affidati per lo svolgimento delle mansioni lavorative, che devono controllare e custodire, durante l'intero ciclo necessario per lo svolgimento delle operazioni di trattamento, per poi restituirli all'archivio, al termine di tale ciclo.

Gli Incaricati devono custodire in modo appropriato gli atti, i documenti ed i supporti contenenti dati personali, loro affidati per lo svolgimento delle mansioni lavorative.
Cautele particolari devono essere previste per gli atti, documenti e supporti contenenti dati sensibili e giudiziari: agli Incaricati viene in questi casi prescritto di provvedere al controllo ed alla custodia in modo tale, che ai dati non possano accedere persone prive di autorizzazione. A tale fine, gli Incaricati sono stati dotati di:

- cassetti con serratura;

- armadi e schedari chiudibili a chiave nei quali devono riporre i documenti, contenenti dati sensibili o giudiziari, prima di assentarsi dal posto di lavoro, anche temporaneamente. In tali dispositivi i documenti possono essere riposti anche al termine della giornata di lavoro, qualora l'Incaricato debba continuare ad utilizzarli, nei giorni successivi.

Al termine del trattamento, l'Incaricato dovrà restituire all'archivio gli atti, i documenti ed i supporti, non più necessari per lo svolgimento delle proprie mansioni lavorative.
Gli archivi contenenti dati sensibili o giudiziari devono essere controllati, mediante l'adozione dei seguenti accorgimenti:

- le persone vengono autorizzate preventivamente ad accedere agli archivi, previa richiesta della chiave all'Incaricato che ha il compito di custodirla;
- si procede inoltre ad identificare e registrare le persone che accedono agli archivi, contenenti dati sensibili o giudiziari, dopo l'orario di chiusura degli uffici, mediante (ad esempio) l'adozione del seguente accorgimento:
- la chiave dell'archivio è affidata, dopo l'orario di chiusura, al titolare o ai Responsabili del trattamento, o in alternativa ad uno o più soggetti Incaricati per iscritto, i quali provvedono ad annotare in un apposito registro i nominativi di coloro che hanno richiesto di accedere all'archivio;
- I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri Incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

Per qualsiasi tipo di documento o semilavorato cartaceo che contenga dati sensibili e giudiziari, quando non più utilizzati, è prescritto che vengano definitivamente distrutti in modo che le informazioni in essi contenuti non siano intelligibili.

3.7 Le misure logiche di sicurezza nell'utilizzo degli strumenti elettronici

Per i trattamenti effettuati con strumenti elettronici (elaboratori, programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato), si adottano le seguenti misure:

- utilizzo di un sistema di autenticazione informatica, che ha il fine di accertare l'identità delle persone atte a svolgere un determinato trattamento, in modo che possano accedere ai dati personali le sole persone autorizzate
- utilizzo di un sistema di autorizzazione, che ha il fine di circoscrivere le tipologie di dati ai quali gli Incaricati possono accedere, ed i trattamenti che possono effettuare, a quelli strettamente necessari per lo svolgimento delle proprie mansioni lavorative
- gestione di un sistema di protezione, di strumenti e dati, da malfunzionamenti, attacchi informatici e programmi che contengono codici maliziosi (virus)
- prescrizione delle opportune cautele per la custodia e l'utilizzo dei supporti rimovibili (floppy disk, dischi ZIP, CD….), nei quali siano contenuti dati personali.

3.7.1 Le credenziali di autenticazione informatica

Il sistema di autenticazione informatica viene adottato per disciplinare gli accessi a tutti gli strumenti elettronici, presenti nell'organizzazione del Titolare, fatta unicamente salva l'eventuale eccezione per quelli che:

- non contengono dati personali;

- contengono solo dati personali destinati alla diffusione, che sono quindi per definizione conoscibili da chiunque.

Per tutti gli altri casi, è impostata e gestita una procedura di autenticazione, che permette di verificare l'identità della persona, e quindi di accertare che la stessa è in possesso delle credenziali di autenticazione per accedere ad un determinato strumento elettronico col quale trattare i dati personali.

Per realizzare le credenziali di autenticazione si utilizza il seguente metodo:

- si associa un codice per l'identificazione dell'Incaricato (username), attribuito da chi amministra il sistema, ad una parola chiave riservata (password), conosciuta esclusivamente dall'Incaricato, che provvederà, in piena autonomia, ad elaborarla, mantenerla riservata e modificarla periodicamente.

Per l'attribuzione e la gestione delle credenziali per l'autenticazione si utilizza il seguente criterio:

- esse vengono assegnate ad ogni Incaricato individualmente, per cui non è ammesso che due o più Incaricati possano accedere agli strumenti elettronici utilizzando la medesima credenziale.

Nei casi in cui una componente della credenziale di autenticazione è costituita dal codice per l'identificazione (username), attribuito all'Incaricato da chi amministra il sistema, tale codice deve essere univoco: esso non può essere assegnato ad altri Incaricati, neppure in tempi diversi.
E' invece ammesso, qualora sia necessario o comunque opportuno, che ad una persona venga assegnata più di una credenziale di autenticazione.

3.7.2 La disattivazione delle credenziali di autenticazione

Al verificarsi dei seguenti casi, è prevista la disattivazione delle credenziali di autenticazione:

- immediatamente, nel caso in cui l'Incaricato perda la qualità, che gli consentiva di accedere allo strumento;
- in ogni caso, entro sei mesi di mancato utilizzo, con l'unica eccezione delle credenziali che sono state preventivamente autorizzate per soli scopi di gestione tecnica, il cui utilizzo è quindi sporadico.

3.7.3 Le istruzioni agli Incaricati

Agli Incaricati vengono impartite precise istruzioni in merito ai seguenti punti:

- obbligo di custodire i dispositivi, attribuiti agli Incaricati a titolo di possesso ed uso esclusivo, con i quali si può accedere agli strumenti informatici (ad esempio, il tesserino magnetico o la smart card): la custodia deve avvenire in modo diligente, sia nell'ipotesi in cui tali dispositivi siano riposti negli uffici (viene prescritto l'obbligo di utilizzare cassetti con serratura), che in quella in cui l'Incaricato provveda a portare il dispositivo con sé (viene prescritto l'obbligo di custodirlo come se fosse una carta di credito); in ipotesi di smarrimento, l'Incaricato deve provvedere immediatamente a segnalare la circostanza all'amministratore di sistema, o alle altre persone che sono state a tale fine indicate, al momento dell'attribuzione del dispositivo;
- obbligo di non lasciare incustodito e accessibile lo strumento elettronico, durante una sessione di trattamento, neppure in ipotesi di breve assenza;
- obbligo di elaborare in modo appropriato la password e di conservare la segretezza sulla stessa; agli Incaricati è imposto l'obbligo di provvedere a modificare la password, con la seguente tempistica:
  - immediatamente, non appena viene consegnata loro da chi amministra il sistema;

- successivamente, almeno ogni sei mesi. Tale termine scende a tre mesi, se la password dà accesso ad aree in cui sono contenuti dati sensibili o giudiziari.

    - prescrizione di comporre password di **almeno otto caratteri,** oppure, nel caso in cui lo strumento elettronico non permetta una tale lunghezza, da un numero di caratteri pari al massimo consentito dallo strumento stesso;
    - prescrizione di **non utilizzare** per le password, nomi semplici o riferimenti agevolmente riconducibili all'interessato (nomi, cognomi, soprannomi, date di nascita proprie, di figli, ecc.);
    - obbligo di segretezza della password, ossia di non comunicarla a nessuno (non solo a soggetti esterni, ma neppure a persone appartenenti all'organizzazione, siano esse colleghi, Responsabili del trattamento, amministratore del sistema o titolare).

3.7.4 La gestione password in deroga

Nei casi di prolungata assenza o impedimento dell'Incaricato, che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema, potrebbe rendersi necessario disporre della password dell'Incaricato, per accedere agli strumenti ed ai dati. A tale fine, agli Incaricati viene richiesto di:

- scrivere la parola chiave su un foglio di carta, da inserire in una busta che deve essere chiusa e sigillata;
- consegnare la busta alla persona preventivamente preposta allo scopo mediante incarico formale.

Solo al verificarsi delle condizioni, sopra esposte, che rendono necessario accedere allo strumento elettronico, utilizzando la copia della parola chiave, il titolare o un Responsabile potranno richiedere la busta che la contiene, a chi la custodisce. Dell'accesso effettuato si dovrà provvedere ad informare, tempestivamente, l'Incaricato cui appartiene la parola chiave.

3.7.5 I profili di autorizzazione

Per discriminare le tipologie di dati ai quali ciascun Incaricato può accedere, ed i trattamenti che può effettuare, si è impostato un sistema di autorizzazione, che circoscrive la sfera d'azione di ciascun ai dati e ai trattamenti strettamente necessari per lo svolgimento delle proprie mansioni lavorative.

L'unica eccezione si ha nei casi in cui il trattamento riguardi solo dati personali destinati alla diffusione: in questo caso non è necessario predisporre alcun sistema di autorizzazione, poiché i dati trattati sono, per definizione, conoscibili da chiunque.

Al di fuori di questi casi, le autorizzazioni all'accesso vengono rilasciate e revocate dal titolare e, se designato, dal Responsabile della sicurezza, ovvero da soggetti da questi appositamente Incaricati.

> ***Il profilo di autorizzazione non viene studiato per ogni singolo Incaricato, ma è impostato per classi omogenee di Incaricati (ad esempio, attribuendo un determinato profilo di autorizzazione a tutti gli impiegati della contabilità, ed attribuendone un altro a coloro che lavorano nell'ufficio personale).***

L'obiettivo di fondo, in ogni caso, è di limitare preventivamente l'accesso, di ciascun Incaricato o di ciascuna classe omogenea di Incaricati, ai soli dati necessari per effettuare le operazioni di trattamento, che sono indispensabili per svolgere le mansioni lavorative.

3.7.6 La verifica periodica di sussistenza

Periodicamente, e comunque almeno annualmente, viene verificata la sussistenza delle condizioni per la conservazione delle credenziali di autenticazione e dei profili di autorizzazione: ciò per quanto riguarda l'ambito di trattamento consentito sia ai singoli Incaricati, che agli addetti alla manutenzione e gestione degli strumenti elettronici.

3.7.7 La protezione anti-intrusione e anti-virus

Per quanto riguarda la protezione, di strumenti e dati, da malfunzionamenti, attacchi informatici e programmi antivirus che contengono codici maliziosi (virus, trojan, backdoor, etc.), devono essere adottati idonei strumenti elettronici e programmi, che il Dlgs 196/2003 imporrebbe di aggiornare con cadenza almeno semestrale, ma che, in relazione al continuo evolversi dei virus, si è ritenuto opportuno di sottoporre ad aggiornamento, di regola:

- Indicativamente ogni settimana nel caso di strumenti elettronici in rete;
- Indicativamente ogni sei mesi nel caso di strumenti elettronici che non sono in rete.

Tutti gli Incaricati devono essere stati istruiti, in merito all'utilizzo dei programmi antivirus e, più in generale, sulle norme di comportamento da tenere per minimizzare il rischio di essere contagiati: a tale fine, dovrà essere loro distribuito un codice dei comportamenti da tenere e di quelli da evitare.

Occorre provvedere anche alla protezione degli elaboratori in rete dall'accesso abusivo, di cui all'articolo 615-ter del codice penale, ai sensi del quale compie tale reato chi si introduce abusivamente in un sistema informatico o telematico, protetto da misure di sicurezza, ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo.

La protezione da tali accessi avviene mediante l'impiego di idonei strumenti elettronici, comunemente conosciuti come firewall e anti-spyware.

A tale riguardo ASL è dotata di più firewall che limitano l'accesso alla rete aziendale dall'esterno a servizi e utenti non autorizzati.
Inoltre sono impartite istruzioni agli amministratori dei vari sistemi (interni o esterni) di tenersi aggiornati periodicamente sui programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti (fix, patch, service pack, ecc.).

L'aggiornamento è effettuato almeno annualmente ed in caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

3.7.8 La gestione dei supporti fisici rimovibili

Per quanto concerne i supporti fisici rimovibili (es. floppy disk, dischi ZIP, CD….), contenenti dati personali, la norma impone che siano impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.
I Responsabili devono prescrivere agli Incaricati del trattamento quanto segue:

- i supporti devono essere custoditi ed utilizzati in modo tale, da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti: in particolare, essi devono essere conservati in cassetti chiusi a chiave, durante il loro utilizzo, e successivamente formattati o distrutti, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi;
- una volta cessate le ragioni per la conservazione dei dati, si devono in ogni caso porre in essere gli opportuni accorgimenti, finalizzati a rendere inintelligibili e non ricostruibili tecnicamente i dati contenuti nei supporti. Tali dati devono quindi essere cancellati, se possibile, e si deve arrivare addirittura a distruggere il supporto, se necessario per i fini in esame.

4 L'affidamento di dati personali all'esterno

Nei casi in cui i trattamenti di dati personali vengano affidati, in conformità a quanto previsto dal Dlgs 196/2003, all'esterno della struttura del Titolare, si adottano i seguenti criteri, atti a garantire che il soggetto destinatario adotti misure di sicurezza conformi a quelle minime, previste dagli articoli da 33 a 35 Dlgs 196/2003 e dal disciplinare tecnico, allegato sub b) al codice.
Per la generalità dei casi, in cui il trattamento di dati personali, di qualsiasi natura, venga affidato all'esterno della struttura del titolare, sono impartite istruzioni per iscritto al terzo destinatario, di rispettare quanto prescritto per il trattamento dei dati personali:

- dal Dlgs 196/2003, se il terzo destinatario è italiano;
- dalla direttiva 95/46/CE , se il terzo destinatario non è italiano.

4.1 Dichiarazione di assunzione di Responsabilità

In ogni caso, il soggetto cui le attività sono affidate dichiara:

- di essere consapevole che i dati che tratterà, nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali, sono soggetti all'applicazione della normativa per la protezione dei dati personali;
- di ottemperare agli obblighi previsti dalla normativa per la protezione dei dati personali;
- di attenersi alle istruzioni specifiche, eventualmente ricevute per il trattamento dei dati personali, conformando ad esse anche le procedure eventualmente già in essere;
- di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate, e di avvertire immediatamente il proprio committente in caso di situazioni anomale o di emergenze;
- di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

Nell'ipotesi in cui il trattamento, di dati sensibili o giudiziari, avvenga con strumenti elettronici, si esige inoltre che il destinatario italiano:

- rilasci la dichiarazione di avere redatto il documento programmatico sulla sicurezza, nel quale abbia attestato di avere adottato le misure minime previste dal disciplinare tecnico.
-

Nei casi in cui ciò si renda opportuno, per ragioni operative legate anche alla tutela dei dati personali, il destinatario esterno viene nominato dal Titolare come Responsabile del trattamento dei dati, mediante apposita lettera scritta.

4.2 Trasferimento di dati a soggetti in paesi extra-UE

Qualora il trasferimento dovesse avvenire verso soggetti residenti in Paesi extra-Ue, che non sono considerati sicuri per il trattamento di dati personali, si stipulano con il destinatario clausole contrattuali conformi, per quanto concerne le misure di sicurezza, a quanto previsto dalla decisione 2002/16/CE: eccezione può essere fatta nei casi, previsti dall'articolo 43 Dlgs 196/2003, in cui il trasferimento può avvenire senza che vengano stipulate tali clausole.
Nei casi in cui il trattamento affidato all'esterno abbia per oggetto dati **sensibili o giudiziari**, si procede alla stipula di clausole contrattuali, con il destinatario, che disciplinano gli aspetti legati alla gestione dei dati personali: se il destinatario è residente in Paesi extra-Ue, che non sono considerati

sicuri per il trattamento di dati personali, tali clausole sono conformi, per quanto concerne le misure di sicurezza, a quanto previsto dalla decisione 2002/16/CE.

5 Il controllo generale sullo stato della sicurezza

Al Responsabile della Sicurezza Informatica è affidato il compito di aggiornare le misure di sicurezza, al fine di adottare gli strumenti e le conoscenze, resi disponibili dal progresso tecnologico, che consentano di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito.
Al fine di verificare l'efficacia delle misure di sicurezza adottate, il Responsabile o i suoi Incaricati provvederanno periodicamente, anche con controlli a campione, ad effettuare una o più delle seguenti attività, rilevando le eventuali non conformità riscontrate:

- verificare l'accesso fisico ai locali dove sono situati i sistemi informatici e le stazioni di lavoro utilizzati per i trattamenti;
- verificare la correttezza delle procedure di archiviazione e custodia di atti, documenti e supporti contenenti dati personali;
- monitorare l'efficacia ed il corretto utilizzo delle misure di sicurezza adottate per gli strumenti elettronici, mediante l'analisi dei log file, nei quali i software di sicurezza installati, i sistemi operativi e le applicazioni scrivono le operazioni svolte dagli Incaricati per il loro tramite. Attraverso questa analisi è possibile individuare i tentativi, riusciti o meno, di accesso al sistema e l'esecuzione di operazioni non corrette, o sospette;
- verificare l'integrità dei dati e delle loro copie di backup;
- verificare la sicurezza delle trasmissioni in rete;
- verificare che i supporti magnetici, che non possono più essere riutilizzati, vengano distrutti;
- verificare il livello di formazione degli Incaricati.

Almeno ogni sei mesi, si procederà ad una sistematica verifica del corretto utilizzo delle parole chiave e dei profili di autorizzazione che consentono l'accesso agli strumenti elettronici da parte degli Incaricati, anche al fine di disabilitare quelli che non sono stati mai utilizzati in sei mesi.
Dell'attività di verifica svolta sarà redatto un verbale, che sarà messo a disposizione del Titolare.

6 Appendice

6.1 Indice completo del TU