ALLEGATO A

CCIAA di NAPOLI

NOME FILE	VERSIONE	DATA CREAZIONE	DATA STAMPA
ManOp_1_0.doc	2011-02	22/03/2011	23/03/2011
AUTORE DOCUMENTO:	CCIAA di NAPOLI		

MANUALE OPERATIVO PRIVACY

1. Introduzione al documento

La procedura regola i comportamenti da tenersi ai fini del rispetto di quanto previsto dal Decreto legislativo 30 giugno 2003, n.° 196 recante "Codice in materia di protezione dei dati personali".

1.1. Novità introdotte rispetto alla precedente emissione

Versione/Release n° :	01	**Data Versione/Release :**	/ /
Descrizione modifiche:	nessuna modifica		
Motivazioni :			

Versione/Release n° :	01	**Data Versione/Release :**	/ /
Descrizione modifiche:	Nessuna		
Motivazioni :	Prima Emissione		

1.2. Scopo e campo di applicazione del documento

La procedura intende garantire che:

- vengano date le corrette informazioni ai soggetti di cui sono trattati i dati personali
- vengano gestite correttamente le richieste di conoscenza e modifica dei dati personali presenti nelle diverse banche dati
- vengano prese le adeguate misure di sicurezza per garantire che i dati gestiti dalla CCIAA di Napoli non vengano utilizzati al di fuori degli scopi e delle finalità per cui sono stati raccolti
- siano rispettate le "misure minime di sicurezza" ai sensi del Disciplinare Tecnico in Materia di Misure Minime di Sicurezza, di cui all'Allegato "B" del D.L.vo n. 196/2003
- i dati gestiti dalla CCIAA di Napoli non possano essere manipolati da persone non autorizzate
- siano effettuati tutti gli adempimenti previsti dalla legge, in particolare provvedendo dove necessario alle nomine di Responsabili e Incaricati ed alle informative.

La procedura si applica a tutti i trattamenti di dati personali effettuati dalla CCIAA di Napoli, quindi sia ai dati gestiti per conto di altri soggetti/clienti, sia ai dati relativi alla gestione interna.

La procedura deve essere rispettata da tutti i dipendenti della CCIAA di Napoli nei ruoli previsti dalla legge di Incaricato o Responsabile del Trattamento

1.3. Revisione del documento

Il presente documento è valido per un anno. Trascorso tale termine deve essere oggetto di revisione per adeguarlo ad eventuali variazioni del livello di rischio a cui sono soggetti i dati personali e ad eventuali modifiche della tecnologia informatica.

Nell'attesa dell'adeguamento conservano validità le regole in vigore.

2. Il contesto del D.L.vo n. 196/2003 nella CCIAA di Napoli

2.1. Tipologia dei Trattamenti di dati personali effettuati nella CCIAA di Napoli

Schematicamente i trattamenti di dati personali effettuati nella CCIAA di Napoli sono riconducibili a 3 diverse tipologie:

a) dati personali contenuti nelle **banche dati interne** trattati esclusivamente dalla CCIAA di Napoli (esempi: gestione personale; procedure interne);

b) dati personali contenuti nella **banche dati interne** trattati da soggetti esterni per conto della CCIAA di Napoli (esempi: procedure registro imprese; servizi tecnologici, ecc.);

Di seguito si indicano i trattamenti affidati a strutture esterne:

InfoCamere S.C.P.A.	Gestione di vari trattamenti inerenti il registro delle imprese ed altri albi, ruoli ed elenchi. L'elenco completo è presente in Tabella 7. del DPS
InfoCert	Gestione del Protocollo informatico e dei certificati CNS. L'elenco completo è presente in Tabella 7. del DPS
IC Outsourcing	Gestione archiviazione ottica atti del registro imprese. L'elenco completo è presente in Tabella 7. del DPS

Tali enti operano nella figura di "Responsabile" dei trattamenti a loro contrattualmente affidati.

2.2. Ruoli e Responsabilità D.L.vo n. 196/2003 nella CCIAA di Napoli

Titolare del Trattamento

Ai sensi dell'art. 28 del D.L.vo n. 196/2003, **il Titolare** dei Trattamenti dei dati personali contenuti nelle banche dati della CCIAA di Napoli è la Camera di Commercio, rappresentata organicamente, per tale materia, dal Presidente.

Responsabile del Trattamento

Al Responsabile del Trattamento, che viene nominato dal Titolare, viene affidata, in base alle competenze tecniche e alle specifiche esperienze, la gestione delle banche dati nel pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

Il Responsabile ha la funzione di coordinare tutte le operazioni di trattamento dei dati effettuate dagli incaricati sulle banche dati di sua competenza e la responsabilità del procedimento di rettifica dei dati stessi.

Il Responsabile deve garantire il pieno rispetto delle disposizioni in materia di trattamento di dati personali e deve attenersi alle direttive impartite dal Titolare.

La CCIAA di Napoli è articolata in Aree, che espletano la loro missione sotto il controllo di dipendenti con grado di Dirigente.

Tutti i trattamenti svolti all'interno della CCIAA sono funzionali alla missione di un'Area ed all'espletamento delle funzioni pubbliche dell'ente.

Sono stati nominati Responsabili del trattamento dei dati personali con determina n. 6 del 31/03/2009, i dirigenti **dr.ssa Teodora Ferrara** e **dr. Mario Esti** incaricando altresì, per le rispettive aree, i dirigenti a svolgere attività di sostegno e orientamento nei confronti degli incaricati del trattamento dei dati personali e di collaborazione con la Giunta Camerale e con il Segretario Generale, rispettivamente per l'esercizio dei diritti e doveri e delle funzioni del titolare nonché per la predisposizione delle misure gestionali e organizzative necessarie alla piena attuazione presso la Camera di Napoli del Decreto Lg.vo n.196/2003.

Incaricati del Trattamento

Il ruolo di Incaricato è definito dall'art. 30 del Codice in materia di protezione dei dati personali

Art. 30 (Incaricati del trattamento)

1. Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del Titolare o del Responsabile, attenendosi alle istruzioni impartite.
2. La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima.

L'attività della CCIAA di Napoli comporta che tutti i dipendenti della stessa gestiscono e trattano i dati contenuti nelle banche dati della CCIAA di Napoli; di conseguenza le attività di trattamento di dati personali devono essere opportunamente regolamentate in modo da rispettare tutti i requisiti di legge.

Si tratta quindi di:

a) individuare i trattamenti di dati personali, presso le varie aree;

b) individuare le persone che effettuano tali trattamenti;

c) nominare tali persone Incaricati del Trattamento;

d) predisporre documenti che contengano precise istruzioni indicanti le modalità con cui si effettuano i trattamenti.

L'ultima esigenza da soddisfare è mantenere il quadro di cui sopra flessibile e facile da mantenere, affinché cambiamenti nelle attività delle persone siano facilmente gestibili in relazione ai requisiti espressi.

A seguito di queste esigenze si è provveduto a redigere il presente Manuale Operativo Privacy, il quale ha lo scopo di impartire le istruzioni a cui devono attenersi tutti gli incaricati del trattamento (ossia tutti i dipendenti della CCIAA di Napoli) nello svolgimento delle operazioni richieste nell'attività lavorativa.

A tal fine, viene di seguito evidenziato il seguente testo.

INCARICO
al trattamento dei dati personali nello svolgimento dell'attività lavorativa ai sensi del D. L.vo n.° 196/2003 (Codice in materia di protezione dei dati personali)

Il Presidente, in rappresentanza del "Titolare" CCIAA di Napoli, considerato che ai sensi dell'art 30 del D.L.vo 196/2003, le operazioni di trattamento dei dati personali svolte all'interno della CCIAA di Napoli possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite e che la designazione degli incaricati è effettuata per iscritto, con la consegna del presente Manuale Operativo Privacy provvede a formalizzare nei confronti dei dipendenti della CCIAA di Napoli l'incarico di trattare i dati personali su cui avranno occasione di operare nell'espletamento dell'attività lavorativa.
Si ricorda che le operazioni di trattamento devono essere svolte nella misura necessaria e sufficiente alle finalità proprie di ciascuna banca dati nonché, in generale, per la realizzazione delle funzioni istituzionali della CCIAA di Napoli e comunque essere eseguite in modo lecito e secondo correttezza (art. 11 del D. L.vo n.° 196/2003).
I trattamenti devono essere eseguiti in base alle istruzioni e le procedure di lavoro contenute nel presente Manuale Operativo Privacy ed in osservanza delle misure di sicurezza adottate all'interno della CCIAA e delle eventuali istruzioni integrative che saranno eventualmente impartite dal Titolare e/o dai Responsabili e/o dai Dirigenti di Area.
I dipendenti, infine, sono tenuti a mantenere la massima riservatezza sui dati personali dei quali vengano a conoscenza nello svolgimento dell'attività lavorativa.
Il presente documento, il testo del D. L.vo n.° 196/2003 e le eventuali istruzioni integrative sono disponibili sul sistema Intranet.
Nel caso in cui per esigenze di servizio si verifichi un cambio di Area di appartenenza, il nuovo Dirigente impartirà le specifiche istruzioni.
L'incarico può essere revocato in ogni momento, con effetto immediato e senza obbligo di preavviso.

L'individuazione dei trattamenti è stata effettuata mediante la redazione del Documento Programmatico sulla Sicurezza della CCIAA di Napoli, la cui Tabella 1 riporta l'elenco dei trattamenti svolti dal Titolare suddivisi per area di competenza. La Tabella 2 individua i compiti e le responsabilità di ciascuna struttura.

Ciascun dipendente opera nella qualità di Incaricato, secondo la nomina sopra riportata, per i trattamenti svolti nella propria area di competenza.

L'eventuale mutamento di area organizzativa e/o di mansioni comporta automaticamente la modifica dell'ambito di trattamento consentito all'Incaricato, che sarà quello relativo ai trattamenti svolti nella nuova struttura di competenza o nelle nuove mansioni assegnate.

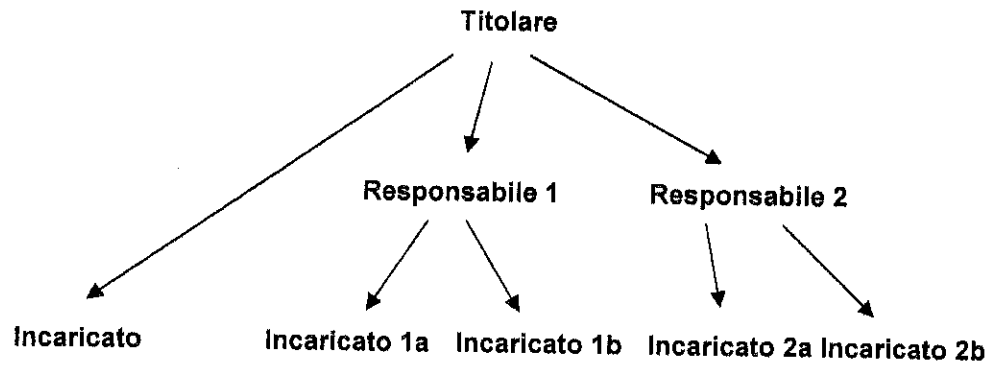
Nel riassumere gli obblighi dell'Incaricato si ricorda che lo stesso dovrà:

- procedere alla raccolta di dati personali solo se incaricati dal titolare o dal responsabile e comunque limitatamente ai soli dati indicati da detti soggetti, anche mediante l'approvazione di appositi moduli di raccolta;
- consegnare agli interessati, nel caso che procedano alla raccolta dei dati personali ed al momento della medesima, il modulo contenente l'informativa di cui all'art. 13 del D.L.vo n. 196/2003, salvo che l'informativa medesima sia stata fornita direttamente dal titolare o dal responsabile;
- trattare i dati personali esclusivamente per le finalità proprie di ciascuna banca dati nella quale vengono inseriti;
- effettuare il trattamento nel rispetto del presente Manuale Operativo Privacy e delle eventuali istruzioni integrative specificate dal proprio responsabile gerarchico;
- adottare, nel trattamento dei dati, tutte le misure di sicurezza che siano indicate, oggi o in futuro, dal titolare o dal responsabile, oltre a quanto di seguito precisato:
  a) 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;
  b) per qualsiasi banca dati, riporre i supporti informatici e/o cartacei contenenti i dati personali nei luoghi indicati a tale scopo (armadi, cassetti), in modo da evitare che detti documenti siano accessibili a persone non autorizzate al trattamento dei dati medesimi;
  c) 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;
  d) in caso si constati o si sospetti un incidente di sicurezza deve essere data immediata comunicazione al responsabile del trattamento;
  e) nel caso si debba accedere, a fini di trattamento anche a dati considerati particolari dalla normativa rilevante, cioè a dati sensibili, si sottolinea l'esigenza di una particolare attenzione e diligenza, nell'osservanza delle disposizioni di cui sopra in relazione a tale tipo di dati;
- 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;
- effettuare la comunicazione e la diffusione dei dati esclusivamente ai soggetti indicati dal titolare o dal responsabile e secondo le modalità stabilite dai medesimi;
- mantenere, salvo quanto precisato al punto precedente, la massima riservatezza sui dati personali dei quali vengano a conoscenza nello svolgimento dell'incarico, per tutta la durata del medesimo ed anche successivamente al termine di esso;

- svolgere, in ogni caso, il trattamento dei dati personali per le finalità e secondo le modalità stabilite, anche in futuro, dal titolare e dal responsabile e, comunque, in modo lecito e secondo correttezza;
- 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;
- 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'incarico nel rispetto della normativa vigente.

Riepilogo dei Ruoli

L'articolazione dei ruoli e delle relative possibilità di nomina previste dalla norma è la seguente:



In base allo schema precedente si riporta nella Tabella seguente lo schema riassuntivo di quanto finora elencato nel presente Capitolo:

Trattamenti Ruolo d.l.vo n. 196/2003	Banche Dati Interne	Banche Dati Interne in outsourcing
Titolare	CCIAA di Napoli	CCIAA di Napoli
Responsabile	dr.ssa Teodora Ferrara dr. Mario Esti	InfoCamere S.C.p.A. InfoCert S.p.A.
Incaricato	Tutti i dipendenti CCIAA di Napoli	Dipendenti CCIAA di Napoli che secondo le mansioni svolte effettuano il trattamento Personale atipico a tempo determinato che secondo le mansioni svolte effettuano il trattamento Dipendenti dei Responsabili esterni che effettuano il trattamento

TRATTAMENTI DI DATI PERSONALI E SANZIONI

Nel trattamento di dati personali si può incorrere in **responsabilità civile e responsabilità penale.**

Il primo tipo di responsabilità comporta l'obbligo di risarcire gli eventuali danni cagionati da un trattamento illegittimo. Il regime di responsabilità civile è particolarmente gravoso, in quanto oltre ad essere risarcibile anche il danno morale, l'art. 15 prevede che, al fine di esimersi dalla responsabilità, è necessario provare "*di aver adottato tutte le misure idonee ad evitare il danno*", ponendo così in capo al danneggiante un onere probatorio altrimenti non richiesti nelle altre ipotesi di illecito civile.

E' necessario sottolineare che, in caso di eventuali danni cagionati per trattamenti svolti all'interno della CCIAA, il primo soggetto ad esserne chiamato a risponderne sarà la CCIAA stessa, ai sensi dell'art. 2049 del codice civile. Essa, qualora condannata al risarcimento, ha diritto a rivalersi sul dipendente che ha posto in essere la condotta illecita.

Con riferimento alla **responsabilità penale**, invece, è opportuno ricordare il principio secondo cui la responsabilità penale **è personale**. Chi commette un reato dovrà risponderne in prima persona, non valendo la responsabilità della società.

I reati penali previsti in materia di protezione dei dati personali sono di varia natura. Si tratta:

1) del Trattamento illecito di dati personali, previsto dall'art. 167 del d.l.vo n. 196/2003;
2) della Falsità nelle dichiarazioni e notificazioni al Garante (art. 168);
3) nella mancata adozione delle Misure minime di sicurezza (art. 169);
4) dell'inosservanza dei provvedimenti del Garante;
5) di altre fattispecie.

Oltre alle sanzioni penali, infine, sono previsti i seguenti illeciti amministrativi che comportano l'applicazione di sanzioni pecuniarie.

1) Omessa o inidonea informativa all'interessato (art. 161);
2) Omessa o incompleta notificazione (art. 163);
3) Omessa informazione o esibizione al Garante (art. 164).

3.1. ISTRUZIONI AGLI INCARICATI DEL TRATTAMENTO

Le seguenti istruzioni, che integrano quelle sinteticamente riportato nel capitolo 2.2. del presente Manuale Operativo Privacy, riportano quanto previsto nel Documento Programmatico sulla Sicurezza approvato dalla CCIAA di Napoli.

Le stesse devono essere osservate da tutti soggetti che all'interno della CCIAA di Napoli operano in qualità di "Incaricati" del trattamento dei dati personali, nonché da ogni "Responsabile" del trattamento.

Ad integrazione delle previsioni contenute nel Documento Programmatico sulla Sicurezza si riportano ulteriori istruzioni in merito alle misure di sicurezza che i singoli Incaricati devono rispettare nel trattamento di dati personali nello svolgimento dei compiti loro affidati.

3.2. TRATTAMENTO SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Per quanto riguarda i locali e gli archivi che contengono dati personali di questa tipologia, vale quanto prescritto dal D.L.vo n. 196/2003 (art. 35) e la CCIAA di Napoli si è organizzata per l'attuazione di quanto ivi prescritto.

> Art. 35 (Trattamenti senza l'ausilio di strumenti elettronici)
> 1. 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.

Con specifico riferimento alla CdC di Napoli sono individuate le seguenti aree in cui vengono effettuati trattamenti cartacei di dati sensibili e/o giudiziari:

Area S.1. – Area gestione del personale e della sicurezza

- **Servizio Gestione del personale: dati sensibili e giudiziari**
- **Servizio Sicurezza e relazioni sindacali – Ufficio sicurezza e prevenzione: dati sensibili**

Area S.2. – Area Gestione Risorse

- **Servizio Acquisti e patrimonio – Ufficio Appalti e contratti: dati giudiziari**

Area S.3. – Area Programmazione e affari generali

- **Servizio Affari Generali – Ufficio Protocollo e archivio: dati sensibili e giudiziari**

Area S.4. – Area Anagrafe Economica

- **Servizio Registro Imprese – Ufficio Diritto Annuale e procedure concorsuali nonché Ufficio polifunzionale per il Commercio: dati giudiziari**
- **Servizio Registro Imprese – Ufficio di qualificazione imprese di impiantistica, autoriparatrici, di pulizia e di facchinaggio: dati giudiziari**
- **Servizio Registro Imprese – Ufficio Segreteria del Conservatore: dati giudiziari**
- **Servizio Albi, Ruoli e Attività – Ufficio Segreteria Albo Imprese Artigiane: dati giudiziari**

- **Servizio Albi, Ruoli e Attività – Ufficio Licenze e concessioni speciali: dati giudiziari**
- **Servizio Albi, Ruoli e Attività – Ufficio Ruoli, Elenchi ed Albi: dati giudiziari**
- **Servizio Albi, Ruoli e Attività – Ufficio Albo Promotori Finanziari: dati giudiziari**

Area S.5. – Area Studi

- **Servizio Regolazione del mercato e tutela del consumatore – Ufficio conciliazione e segreteria Corte Arbitrale: dati sensibili e giudiziari**

Area S.6 – Area Promozione

- **Servizio promozione ed incentivi: dati sensibili**

Le strutture in cui sono effettuati i trattamenti sopra riportati sono definite "aree ad accesso controllato".

Le aree ad accesso controllato devono essere all'interno di locali sotto la responsabilità della CCIAA di Napoli.

Per tali aree:

- Il locale deve essere chiuso anche se presidiato, le chiavi o le abilitazioni di diversi dispositivi sono custoditi a cura del Responsabile dell'ufficio.
- L'accesso deve essere consentito solo alle persone autorizzate.
- L'accesso deve essere possibile solo dall'interno dell'area sotto la responsabilità della CCIAA di Napoli.

Il Responsabile dell'ufficio mantiene un effettivo controllo sull'area di sua responsabilità.

- Possono accedere all'area solo le persone appartenenti all'ufficio.
- I visitatori occasionali devono essere accompagnati.
- Gli ingressi fuori orario devono essere controllati.

I documenti cartacei contenti dati personali sensibili e/o giudiziari sono riposti in armadi muniti di serratura. Le chiavi degli armadi sono conservate dal Responsabile dell'ufficio e/o dai singoli incaricati appartenenti allo stesso.

I locali in cui sono collocati gli armadi sono muniti di porte con serrature. Le chiavi dei locali sono sotto la responsabilità del Responsabile dell'ufficio e/o degli incaricati operanti nell'ambito dello stesso.

La protezione dei locali da eventi ambientali è assicurata utilizzando le medesime procedure già attuate nell'ambito dell'Ente ai sensi del d.l.vo n. 81/2008.

4.2.2. ISTRUZIONI SCRITTE PER GLI INCARICATI FINALIZZATE AL CONTROLLO E LA CUSTODIA DEGLI ATTI E DOCUMENTI CONTENENTI DATI PERSONALI PER L'INTERO CICLO NECESSARIO ALLO SVOLGIMENTO DELLE OPERAZIONI DI TRATTAMENTO

Istruzioni particolareggiate applicabili al trattamento di dati personali effettuato nell'ambito dello svolgimento delle mansioni svolte all'interno della CCIAA di Napoli:

- La CCIAA di Napoli ha messo a disposizione locali ad accesso controllato ed armadi muniti di serratura ove sono di norma custoditi i documenti contenenti dati personali sensibili e/o giudiziari; come regola generale, tali documenti non devono essere asportati da tale luogo sicuro e, ove ciò avvenga, la asportazione deve essere ridotta al minimo tempo necessario per effettuare le operazioni di trattamento.
- Dai luoghi sopra citati devono essere asportati solo i documenti strettamente necessari per le operazioni di trattamento e non intere pratiche, se ciò non è necessario.
- Al termine delle operazioni di trattamento, i documenti devono essere immediatamente riposti nel luogo sicuro.
- Per tutto il periodo in cui i documenti sono all'esterno del luogo sicuro, l'incaricato non deve mai perderli di vista, adempiendo ad un preciso obbligo di custodia dei documenti stessi.
- L'incaricato deve inoltre controllare che i documenti, composti da numerose pagine o più raccoglitori, siano sempre completi, verificando che sia il numero dei fogli che l'integrità del contenuto, rispetto a quanto presente, all'atto del prelievo dal luogo sicuro.
- Se si debbono abbandonare, ad esempio di sera, in ufficio o al termine dell'orario di lavoro, gli anzidetti documenti, l'incaricato deve identificare un luogo sicuro di custodia che dia sufficienti garanzie di protezione da accessi non autorizzati (un armadio chiuso a chiave, un cassetto chiuso a chiave, una cassaforte, un armadio blindato, un classificatore chiuso a chiave); ove si utilizzi un contenitore chiuso a chiave, di qualunque natura, occorre accertarsi che non esistano duplicati abusivi delle chiavi e che tutte le chiavi siano in possesso solo di incaricati autorizzati.
- I documenti di cui sopra non devono essere mai lasciati incustoditi sul tavolo durante il giorno.
- Ci si deve in particolare accertare che un visitatore o terzo (addetto alla manutenzione, addetto alle pulizie, collega non autorizzato) possa entrare in ufficio anche non invitato o per cause accidentali, non possa venire a conoscenza dei contenuti dei documenti.
- Si deve limitare al minimo assoluto il numero di fotocopie effettuate, mantenendo una traccia scritta delle copie effettuate e degli incaricati e responsabili, cui le copie sono state inviate.
- Si deve adottare una procedura per la consegna delle copie ai destinatari, che dia tutte le garanzie di sicurezza, in particolare utilizzando buste di sicurezza sigillate, oppure effettuando la consegna personalmente, di modo da ridurre al minimo la possibilità che soggetti terzi non autorizzati possano prendere visione del contenuto, od addirittura fotocopiarlo dall'insaputa del mittente e destinatario.
- Particolare cautela deve essere adottata ove i documenti in questione vengano consegnati in originale a un incaricato o Responsabile, debitamente autorizzato.
- Nel caso la consegna degli originali o delle fotocopie dei documenti avvenga per posta, si utilizzi la spedizione per assicurata convenzionale, che è l'unica che da la garanzia di un

continuo tracciamento del movimento del documento ed offre ben più elevate garanzie di sicura consegna al destinatario, rispetto alle più tradizionale raccomandata.

- Quale che sia il tipo di spedizione adottato, ci si accerti che esso consenta di avere prova certa del fatto che il destinatario ha effettivamente ricevuto i documenti inviati e che essi sono giunti integri, e quindi non manomessi o alterati in fase di trasporto.
- Eventuali fotocopie non riuscite bene debbono essere distrutte in un apposito distruggi-documenti, se disponibile, oppure devono essere strappate in pezzi talmente piccoli, da non consentire in alcun modo la ricostruzione del contenuto, che deve essere comunque illeggibile.
- È tassativamente proibito utilizzare le fotocopie non riuscite come carta per appunti.
- È parimenti tassativamente proibito trasportare all'esterno del posto di lavoro fotocopie non riuscite, da utilizzare altrove come carta per appunti.
- Quando i documenti devono essere trasportati all'esterno del luogo di lavoro, l'incaricato deve tenere sempre con sé la cartella o la borsa, nella quale i documenti sono contenuti; deve inoltre evitare che sia possibile esaminare, da parte di un soggetto terzo non autorizzato, anche solo la copertina del documento in questione.
- Durante il trasporto, la cartella non deve essere mai lasciata incustodita e preferibilmente deve essere tenuta chiusa a chiave o devono essere azionate le serrature a combinazione di presenti sulla cartella o valigia.
- È tassativamente proibito discutere, comunicare o comunque trattare dati personali per telefono, se non si è certi che il corrispondente sia un incaricato, il cui profilo di autorizzazione sia tale da potere trattare i dati in questione.
- Si raccomanda vivamente non parlare mai ad alta voce, trattando dati personali per telefono, soprattutto utilizzando cellulari all'esterno dell'Ente o anche all'interno, in presenza di terzi non autorizzati, per evitare che dati personali possano venire a conoscenza di terzi non autorizzati, anche accidentalmente.
- In caso di dubbio sulle modalità di applicazione di quanto sopra illustrato, o per chiedere ulteriori chiarimenti in merito, l'incaricato deve rivolgersi al Responsabile della propria Divisione/Servizio.

4.3. TRATTAMENTO CON STRUMENTI ELETTRONICI

Di seguito si riportano le regole di sicurezza informatiche applicate all'interno della CCIAA.

********** ********** ********** ********** ********** **********

SISTEMI E STRUMENTAZIONE DI PROTEZIONE DEGLI ACCESSI ALLA RETE

Firewall, antivirus e idonee strumentazioni di allarme e blocco proteggono l'accesso alle risorse interne alla rete CCIAA di Napoli.

PROTEZIONE DA PROGRAMMI PERICOLOSI

I sistemi sensibili ai virus sono protetti con opportuni programmi (antivirus). L'efficacia degli antivirus installati è verificata con frequenza giornaliera.

PROTEZIONE DEI DATI PERSONALI

I dati personali sono messi a disposizione solo delle persone che hanno la necessità di accedervi per fini di trattamento.

L'accesso deve essere esplicitamente autorizzato solo con le modalità previste dal trattamento e limitato ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di trattamento o manutenzione.

La validità delle richieste di accesso è verificata prima che sia concessa l'autorizzazione relativa. Parimenti al cessare delle necessità operative verranno revocate le autorizzazioni precedentemente concesse.

PROTEZIONE DELLE CONNESSIONI CON L'ESTERNO

In un sistema integrato la sicurezza deve essere trattata in modo uniforme, in quanto l'insicurezza di una singola parte si può ripercuotere generando insicurezza in tutto il sistema. Questo vale in particolare per gli aspetti di sicurezza della rete. Per assicurare la sicurezza di una rete è fondamentale controllare gli accessi alla rete stessa.

Sono considerate connessioni con l'esterno i collegamenti con altre reti, in particolare:

- interconnessioni tra i servizi informatici e telematici della CCIAA di Napoli e quelli di altre aziende, incluso Internet.
- accesso remoto da parte di dipendenti della CCIAA di Napoli o intermediari o di altre aziende (clienti, fornitori, consociate, ecc.).

Vale anche in questa sede il principio generale: tutto quello che non è espressamente consentito è negato.

MESSA IN SICUREZZA DEI GATEWAY

È definito Gateway per le interconnessioni esterne l'insieme di hardware, software e applicazioni (es. Firewall o Proxy) che permettono l'interconnessione o l'accesso remoto.

I Gateway di interconnessione esterna sono sotto il controllo diretto della CCIAA di Napoli.

ISOLAMENTO DELLE RETI

La CCIAA di Napoli garantisce che, qualora la parte di rete/LAN sia di sua responsabilità, venga evitato il rischio che personale non autorizzato acceda alla rete, ai sistemi o ai dati personali.

AUTENTICAZIONE INFORMATICA

L'accesso ai dati è protetto da appositi sistemi di identificazione, riconoscimento, autenticazione, abilitazione ad alta affidabilità.

Ciascun incaricato deve avere un proprio profilo di autorizzazione che limiti l'accesso ai soli dati necessari per effettuare le operazioni di trattamento e compatibili con le proprie mansioni.

FUNZIONE DI IDENTIFICAZIONE

Tale funzione assicura che ad ogni potenziale utente dei sistemi o delle banche dati sia associato un identificativo unico e univoco, gestito mediante specifici privilegi d'accesso determinati (user-id).

L'user-id sono riconducibili ad un singolo individuo.

FUNZIONE DI RICONOSCIMENTO

Quando un utente accede al sistema, alla banca dati o alla rete ne viene verificata l'identità mediante un successivo livello di controllo delle informazioni appositamente fornite (es. password).

Tali informazioni sono definite Credenziali.

FUNZIONE DI AUTENTICAZIONE

Le Credenziali presentate dall'utente sono verificate mediante un confronto con quelle presente negli archivi della CCIAA di Napoli.

Agli utenti non riconosciuti o che presentino Credenziali errate viene negato l'accesso senz'altra motivazione.

ABILITAZIONE

L'accesso ai sistemi, alle banche dati contenenti informazioni personali, o alla rete è basata sulle effettive necessità del trattamento. Le informazioni relative (Profili di autorizzazione associati alle Credenziali) sono conservate negli archivi della CCIAA di Napoli. L'utilizzo di user-id non personali non è consentito se non per necessità sistemistiche, la gestione di questi user-id di sistema viene regolamentata secondo specifiche direttive conosciute e accettate dai dipendenti che sono in possesso delle relative credenziali di autenticazione.

ASSEGNAZIONE E REVOCA DELLE USER-ID ED ABILITAZIONI

La CCIAA di Napoli gestisce la procedura per l'assegnazione delle user-id che permettono l'accesso ai sistemi, alle banche dati e alla rete.

Ad ogni incaricato del trattamento è assegnato un (eventualmente più di uno) codice di identificazione personale.

Tale codice deve consentire l'univoca identificazione dell'incaricato: non sono consentiti codici di identificazione collettivi.

Deve essere previsto che:

- Quando un utente non ha più la necessità di accedere ad una banca dati o lascia l'ente, il capo ufficio dell'utente interessato chiede alla CCIAA di Napoli di disabilitare l'utenza non più necessaria.
- Le user-id inutilizzate per più di 6 mesi siano disattivate.
- Non sia consentito il riutilizzo di una user-id personale già assegnata ad altro utente.

In caso di una prolungata assenza o impedimento dell'incaricato stesso, il suo dirigente diretto deve informare tempestivamente l'incaricato del trattamento nel caso in cui fosse indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema.

CREDENZIALI PER L'AUTENTICAZIONE

Sono predisposte opportune modalità per il **riconoscimento univoco dell'utente e l'accesso alle risorse ad esso abilitate**. I criteri fondamentali attualmente utilizzati nei sistemi di autenticazione sono riconducibili prevalentemente a due tipologie

- autenticazione forte basato su utilizzo di Smart-Card e certificati digitali
- quello più tradizionale di riconoscimento dell'utente tramite user-id e password.

PASSWORD E REGOLE RELATIVE

La password è un elemento fondamentale per la sicurezza delle informazioni. La robustezza delle password è il meccanismo più importante per proteggere i dati; un corretto utilizzo della password è a garanzia dell'utente.

Le regole di seguito elencate sono vincolanti per tutti i sistemi e le workstation tramite le quali si può accedere alla rete e alle banche dati contenenti dati personali.

Le password assegnate inizialmente e quelle di default dei sistemi operativi, prodotti software, ecc.

devono essere immediatamente cambiate dopo l'installazione e al primo utilizzo.

In particolare:

- Tutte le password di default (ad es. "system", "administrator") devono essere cambiate al momento dell'installazione del prodotto o del sistema e devono essere successivamente cambiate almeno ogni tre mesi.
- Le password non devono essere scritte.
- Le password non devono essere inserite in messaggi e-mail o in altre forme di comunicazione elettronica.
- Le password non devono essere comunicate a terzi. In caso di necessità devono essere immediatamente cambiate.
- Nel caso in cui ci si debba assentare dalla postazione di lavoro durante una sessione di trattamento è fatto obbligo attivare uno screen saver con password.
- La lunghezza minima della password è di 8 caratteri o comunque il massimo previsto dalla tecnologia o sistema specifico (se non può raggiungere gli 8 caratteri ed il sistema è preesistente all'emissione del presente documento).
- La password non deve essere riconducibile ai dati anagrafici dell'incaricato.

Inoltre la password :

- deve contenere almeno un carattere alfabetico ed uno numerico.
- non deve contenere più di due caratteri identici consecutivi.
- non deve essere simile alla password precedente.
- non deve contenere l'user-id come parte della password.
- deve essere cambiata almeno ogni 6 mesi.
- non deve essere comunicata ad altri utenti.

Dove la tecnologia lo permette tali regole sono rese obbligatorie dal software altrimenti è responsabilità dell'utente rispettarle, attività di informazione e responsabilizzazione a riguardo sono svolte periodicamente nell'ambito del Programma di formazione sulla Sicurezza, di cui al paragrafo relativo.

REGOLE DI COSTRUZIONE DELLE PASSWORD

Le password devono essere ricordabili facilmente ma devono essere al contento robuste. Un modo per ottenere ciò è costruire password che si basino sul titolo di una canzone, su di una frase storica o su di una poesia e assemblarne i pezzi.

Ad esempio, la poesia potrebbe essere: "Mi illumino di immenso" ed una password ricavabile da quella poesia potrebbe essere: "MiIlDiIm".

Nel seguito sono descritte le caratteristiche delle password robuste e le caratteristiche delle password deboli. **Dove la tecnologia lo permette tali regole sono rese obbligatorie dal software altrimenti è responsabilità dell'utente rispettarle.**

Il ripristino della password deve essere fatta solo a fronte di una positiva identificazione del richiedente e dovrà essere cambiata subito dopo a cura del richiedente.

Password robuste

Una password intrinsecamente robusta ha le seguenti caratteristiche:

- Contiene sia caratteri maiuscoli sia caratteri minuscoli
- Contiene cifre, caratteri di interpunzione e lettere
- È lunga almeno otto caratteri
- Non è una parola di una qualunque lingua, dialetto o linguaggio specialistico
- Non si basa su informazioni personali

Password deboli

Una password intrinsecamente debole ha una o più delle seguenti caratteristiche:

- è una parola che si trova sul vocabolario;
- è una parola di uso comune come, ad esempio: nomi propri, cognomi, personaggi di fantasia (es. Mario, Rossi, Pluto, ...);
- è il nome dell'ente o dell'azienda;
- è una data di nascita, un indirizzo, un numero di telefono, una targa automobilistica

- è una sequenza banale di caratteri come, ad esempio: aaabbb, qwerty, 123456...;
- è una qualsiasi password precedentemente menzionata scritta a rovescio;
- è una qualsiasi password precedentemente menzionata preceduta o seguita da una cifra.

AZIONI DA EVITARE NELL'UTILIZZO DELLA PASSWORD

- Non far conoscere la password al telefono a nessuno
- Non far conoscere la password in un messaggio di posta elettronica
- Non parlare della password
- Non dare indicazioni sulla password
- Non far conoscere la password ai familiari
- Non far conoscere la password ai colleghi durante i periodi di assenza dal lavoro
- Non utilizzare l'opzione "ricorda la password" disponibile su alcune applicazioni
- Non scrivere la password in nessun luogo
- Non registrare le password in un file di computer

RIPRISTINO DELLA PASSWORD

Il ripristino della password deve essere fatta, mediate apposita procedura, solo a fronte di una positiva identificazione del richiedente, previa autorizzazione del diretto Responsabile, e dovrà essere cambiata subito dopo a cura del richiedente stesso.

********** ********** ********** ********** ********** **********

A maggior garanzia del rispetto delle previsioni in merito alla gestione delle credenziali di autenticazione da parte dei singoli incaricati si riportano di seguito le linee guida che debbono necessariamente essere rispettate all'interno dell'Ente per la selezione e gestione sicura delle parole chiavi utilizzate:

4.3.1.Linee guida per la selezione e gestione sicura della parola chiave da parte degli Incaricati

Generalità

Tutte le parole chiave a livello di sistema, come ad esempio quelle dell'amministratore di un sistema operativo NT e simili, devono essere cambiate con una frequenza più elevata, rispetto a quella attribuita a parole chiave conferite ad utenti con profilo di accesso di minore rischio (indicare la frequenza, ad esempio 15 giorni).

Tutte le parole chiave utilizzate a livello di sistema devono essere inserite nel database globale di gestione delle parole chiave.

Tutte le parole chiave attribuite ai singoli incaricati per accedere alla posta elettronica, al proprio computer, ad Internet, eccetera, devono essere cambiate almeno ogni sei mesi. Questo intervallo di tempo deve essere ridotto a tre mesi, se queste parole chiave vengono utilizzate per accedere a dati personali sensibili e giudiziari.

È fatto assoluto divieto di inserire parole chiave in messaggi di posta elettronica od altre forme di comunicazione elettronica.

Linee guida per la costruzione delle parole chiave

Le parole chiave possono essere utilizzate per accedere a differenti profili di autorizzazione, nell'ambito del sistema informativo.

Gli utilizzi più frequenti sono ad esempio: contabilità di utente, accesso ad Internet, accesso a sistemi di posta elettronica, accesso a screen saver, accesso a sistemi di casella elettronica vocale, e simili.

Poiché sono molto rari i sistemi informativi che possono utilizzare parole chiave dinamiche, che vengono usate una volta sola, è indispensabile che ogni incaricato prenda buona nota delle modalità con cui è possibile selezionare parole chiave di difficile individuazione.

Parole chiave deboli

Le parole chiave di facile individuazione hanno le seguenti caratteristiche:

- La parola chiave contiene meno di 8 caratteri, anche se il sistema può accettare parole chiave di 8 caratteri ed oltre
- La parola chiave si può trovare in una comune dizionario italiano, in inglese od altra lingua comune
- La parola chiave è una parola di uso comune, come ad esempio il nome di qualche membro della famiglia, di animali da salotto, di amici, di collaboratori o di caratteri di fantasia.
- Sono da ritenere insoddisfacenti anche parole chiave legate a espressioni informatiche, hardware e software, come pure quelle legate a date di nascita od altre informazioni personali, come l'indirizzo, il numero telefonico e simili.
- Sono inoltre da scartare parole o sequenze numeriche del tipo aaaaaaaa, bbbb, 121212, 123456, eccetera. Sono da scartare parole come sopra, digitate alla rovescia
- E' da scartare una qualsiasi delle parole chiave precedentemente indicata come debole, preceduta o seguita da una cifra come ad esempio giovanni1, oppure 1giovanni.

Parole chiave sicure

Per contro, sono da ritenere parole chiave di soddisfacente sicurezza quelle che hanno le seguenti caratteristiche:

- Sono composte da caratteri maiuscoli e minuscoli
- Utilizzano anche caratteri di interpunzione, come; [,] , * " , ed una miscela di numeri e lettere
- Devono avere una lunghezza minima di 8 caratteri alfanumerici, se il sistema consente raggiungere questa lunghezza
- Non devono rappresentare una parola in una qualsiasi lingua o dialetto sufficientemente diffuso
- Non devono essere basate su informazioni personali, come nomi di membri della famiglia e simili
- Un altro importante accorgimento riguarda la selezione di parole chiave, che possano essere facilmente digitate sulla tastiera, senza doverla guardare, per ridurre al minimo

il tempo di digitazione ed evitare che la digitazione possa essere osservata surrettiziamente da terzi nelle vicinanze

Le parole sicure non devono mai essere scritte o archiviate in linea.

Ecco qualche indicazione per creare delle parole chiave sicure ma facili da ricordare:

- Un primo suggerimento è quello di creare una parola chiave, basata sul titolo di una canzone o su un'altra frase, debitamente sintetizzata - ad esempio "tea for two" diventa "teax2"
- La parola chiave può essere formata abbreviando una intera frase come ad esempio "che gelida manina" diventa "chegemani"

Attenzione: non usare mai alcuna degli esempi sopra illustrati come parola chiave

Raccomandazione per la protezione della parola chiave

Non utilizzare la stessa parola chiave per sistemi di autenticazione interni all'ente e per sistemi di autenticazione esterni, come ad esempio l'accesso al proprio conto corrente bancario ed altre attività, non legate all'attività lavorativa.

Ove ad un incaricato vengano attribuiti diversi profili di autorizzazione, non deve essere usata la stessa parola chiave in relazione a differenti profili (ad esempio, deve essere scelta una parola chiave per l'accesso all'area tecnica del sistema, ed una parola chiave separata per l'accesso alla contabilità)

La parola chiave prescelta non deve essere condivisa con alcun soggetto, interno o esterno all'ente, ivi inclusi i superiori, a qualsiasi livello.

Tutte le parole chiavi che sono state generate da un incaricato devono essere trattate come informazione strettamente riservata.

In particolare, ecco un elenco delle cose che non bisogna fare:

- Non rivelate una parola chiave attraverso il telefono a chicchessia
- Non scrivete una parola chiave in un messaggio di posta elettronica
- Non rivelate la parola chiave al vostro superiore
- Non parlate di parole chiave di fronte di terzi
- Non date alcun indicazioni in merito al formato ed alla lunghezza della parola chiave, che utilizzate
- Non svelate la parola chiave su questionari o su formulari di sicurezza
- Non rivelate la parola chiave a membri della famiglia
- Non rivelate la parola chiave ad un vostro collega di lavoro, mentre voi siete in vacanza

Se qualcuno insiste per conoscere la vostra parola chiave, dapprima fate riferimento a questo documento e successivamente informate immediatamente il vostro Titolare, Responsabile o Dirigente.

Non utilizzare mai la caratteristica, offerta da parecchi applicazioni, di ricordare la parola chiave

Non scrivete la parola chiave su un qualsiasi documento e non nascondetelo in alcuna parte del vostro ufficio

Non archiviate la parola chiave in un qualsiasi tipo di sistema di elaborazione, incluso un telefono cellulare, un computer palmare e simile, senza utilizzare un algoritmo di cifratura.

Ricordatevi di cambiare la parola chiave almeno una volta ogni sei mesi; questo intervallo viene ridotto a tre mesi in caso la parola chiave consenta l'accesso alla trattamento di dati sensibili e giudiziari.

Se avete anche solo il minimo sospetto che la vostra parola chiave sia stata in qualche modo compromessa o venuta a conoscenza di terzi, provvedete immediatamente alla sostituzione della parola chiave e riferite l'accaduto al Titolare od al Responsabile del trattamento di dati personali.

Si faccia attenzione che, nell'ambito delle misure di controllo del livello di sicurezza del sistema informativo, è possibile che il Responsabile effettui tentativi di violazione della vostra parola chiave. Nel caso il tentativo abbia esito positivo, vi verrà chiesto di sostituire immediatamente la parola chiave.

Istruzioni speciali per analisti programmatori

Gli analisti programmatori devono accertarsi che i loro programmi siano dotati delle seguenti caratteristiche di sicurezza:

- Le applicazioni devono essere in grado di autenticare i singoli individui e non i gruppi
- Le applicazioni non devono archiviare le parole chiave in chiaro od in una forma facilmente intelligibile
- Le applicazioni devono avere la possibilità di introdurre la figura di un gestore di livello superiore, di modo che un utente possa subentrare alle funzioni di un altro, senza dover conoscere la sua parola chiave

Frasi chiave

Le frasi chiave possono essere utilizzate per l'autenticazione remota di un utente, utilizzando gli algoritmi con chiave pubblica e privata.

Un sistema con chiave pubblica e privata definisce una relazione matematica tra la chiave pubblica, nota a tutti, e la chiave privata, che conosciuta soltanto all'utente.

Senza la parola frase che permette di decifrare la chiave privata, l'utente non può ottenere l'accesso al sistema.

Questa architettura di sicurezza è spesso usata in Italia nella gestione di applicativi di firma digitale.

Le frasi chiave non sono la stessa cosa delle parole chiave.

Una frase chiave è una versione più lunga di una parola chiave e quindi più sicura.

Una frase chiave è tipicamente composta da molte parole ed è questa la ragione, per cui essa più sicura contro i cosiddetti "attacchi del dizionario".

Una frase chiave sicura è relativamente lunga e contiene una combinazione di lettere maiuscole e minuscole, nonché numeri e segni di interpunzione. Ecco un esempio di una soddisfacente frase chiave:

"la mattina e' BELLA"

Tutte le regole prima illustrate, che si applicano alla selezione delle parole chiave, si applicano anche alle frasi chiave.

Disattivazione del profilo di autenticazione

Nel caso l'incaricato non utilizzi il proprio codice identificativo personale e parola chiave per un periodo superiore a sei mesi, il suo profilo di autenticazione viene automaticamente disattivato. Per riprendere la operatività, l'incaricato deve prendere contatto con il proprio Dirigente.

Disattivazione del profilo di autorizzazione

Per esplicita prescrizione di legge, il profilo di autorizzazione concesso ad un incaricato deve essere verificato almeno una volta l'anno.

È possibile che l'incaricato, pure debitamente autenticato, si trovi impossibilitato ad utilizzare il proprio profilo di autorizzazione, per scadenza dello stesso e mancato rinnovo.

Per riprendere la operatività, l'incaricato deve prendere contatto con il proprio DIirgente.

Interventi di emergenza

Il disciplinare tecnico in materia di misure minime di sicurezza prevede esplicitamente che sia possibile, per il Titolare od il Responsabile del trattamento di dati personali, di accedere alla parola chiave di un incaricato, ove per una qualunque ragione egli non sia presente sul posto di lavoro e sorga una urgente esigenza di accedere a dati personali, che sono accessibili soltanto con il suo profilo di autorizzazione.

Giova sottolineare che, ove il profilo di autorizzazione sia condiviso con altri soggetti, la procedura di emergenza appresso illustrata non ha ragione di essere utilizzata, in quanto agli stessi dati si può accedere grazie ad un altro incaricato, che utilizza la propria parola chiave.

Nel caso il profilo di autorizzazione rientri nella categoria soprariportata, è fatto obbligo all'incaricato di trascrivere la propria parola chiave su un foglio di carta, che deve essere inserito in una busta debitamente sigillata e controfirmata, meglio se chiusa con sigilli inviolabili a numerazione univoca.

Tale busta deve essere consegnata al Titolare od al Responsabile del trattamento dei dati personali e il suo contenuto deve essere costantemente aggiornato, ogniqualvolta l'incaricato decide di sostituire la propria parola chiave.

È facoltà del Titolare o del Responsabile, in presenza dell'incaricato, aprire la busta sigillata e verificare che la parola chiave presente sul foglio di carta corrisponde a quella effettivamente in uso.

È fatto obbligo al Titolare od al Responsabile del trattamento i dati personali di verbalizzare in apposito registro, con controfirma di garanzia da parte di terzi (precisare), l'avvenuta apertura della busta e la presa di conoscenza della parola chiave.

Resta inteso che dal momento in cui il Titolare od il Responsabile hanno preso conoscenza della parola chiave, all'incaricato che l'ha selezionata non compete più alcuna ulteriore responsabilità, in merito a trattamenti non autorizzati od accessi non consentiti ai dati personali, di cui al suo profilo di autorizzazione.

La sua responsabilità verrà pienamente rimessa in essere, non appena l'incaricato avrà avuto la possibilità di selezionare una nuova parola chiave ed assumersene quindi la piena responsabilità di corretto utilizzo. In tale occasione ci si rammenti di inserire la nuova parola chiave della busta sigillata, come precedentemente illustrato.

Sanzioni

Un incaricato che abbia violato queste linee guida di sicurezza potrebbe essere sottoposto ad azioni disciplinari di vario livello, per i possibili riflessi che la sua negligenza potrebbe avere avuto sulla sicurezza del sistema informativo.

4.3.2. ISTRUZIONI ORGANIZZATIVE E TECNICHE PER LA CUSTODIA ED USO DEL SUPPORTO RIMOVIBILE

Un ulteriore aspetto di sicurezza che gli Incaricati della CCIAA di Napoli sono tenuti a rispettare concerne la custodia e l'uso di supporti rimovibili su cui vengano conservati dati personali sensibili e/o giudiziari.

In linea generale, non viene raccomandata la copia supporti removibili di dati sensibili e giudiziari, per ridurre al minimo il rischio di perdita o distruzione anche accidentale dei dati stessi.

Non si deve inoltre dimenticare che un supporto rimovibile smarrito e o accidentalmente lasciato incustodito, anche per breve periodo, può essere rapidamente letto e copiato, senza lasciare alcuna traccia dell'accaduto, trovandosi davanti un rischio concreto di accesso non autorizzato o copia abusiva dei dati sensibili e giudiziari

Ciò premesso, ove nello svolgimento della normale attività assegnata all'incaricato, nell'ambito del suo profilo di autorizzazione, sia indispensabile effettuare una copia di dati sensibili e giudiziari su supporto removibile, occorre attenersi alle seguenti cautele:

- Accertarsi che il supporto sia debitamente formattato e privo di altri file, che potrebbero essere infetti. Nel dubbio, è sempre bene provvedere alla formattazione *ex novo* del supporto, prima di registrare dati sensibili e giudiziari;
- Per evitare l'alterazione dei dati in questione, dopo la copia su supporto, si attivi la protezione contro possibili nuove scritture, che potrebbero alterare i dati stessi;
- Il supporto removibile deve essere contrassegnato da un'etichetta, con una indicazione in chiaro od in codice, tale da permettere all'incaricato di riconoscere immediatamente il contenuto del supporto in questione, ed evitare che egli possa confonderlo con altri supporti in suo possesso;
- Il supporto contenente dati sensibili e giudiziari deve essere sempre direttamente e personalmente custodito dall'incaricato che ha realizzato la copia;
- In caso di spedizione ad altro incaricato, occorre accertarsi che il destinatario abbia lo stesso profilo di autorizzazione del mittente e che il supporto venga spedito in una busta sigillata, intestata personalmente all'incaricato, con controfirma sul lembo di chiusura; ove i dati siano particolarmente sensibili, si deve utilizzare una apposita busta, dotato di sigillo in plastica non duplicabile e con numerazione univoca, per mettere in evidenza qualsiasi tentativo di violazione;
- Non si deve spedire un supporto, contenente dati sensibili e giudiziari ad un destinatario, senza aver prima concordato con il destinatario stesso le modalità e tempi di consegna ed aver stabilito la procedura, che permette di confermare l'avvenuta consegna al destinatario del supporto;
- Se sul supporto sono registrati dati relativi all'identità genetica, la creazione del supporto deve essere effettuata all'interno di un locale protetto e debitamente autorizzato dal responsabile o dal titolare; inoltre la registrazione dei dati sul supporto deve avvenire in forma cifrata, indipendentemente dal rispetto delle istruzioni di spedizione sopra illustrate;

- Qualora i dati contenuti sul supporto non abbiano più ragione di essere, si deve provvedere immediatamente alla formattazione del supporto ed alla asportazione dell'etichetta con la indicazione il contenuto od alla sua cancellazione;
- Poiché i supporto sk sono particolarmente sensibili ai campi magnetici, per evitare la cancellazione o danneggiamento anche accidentale dei dati, il supporto non deve mai essere avvicinato ad un campo magnetico, come ad esempio il magnete di un altoparlante, oppure lasciato abbandonato nelle vicinanze di un trasformatore, come i trasformatori utilizzati nelle lampade da tavolo in quanto i campi dispersi potrebbero danneggiare il contenuto del supporto;
- I supporto contenenti dati sensibili e giudiziari non devono essere esposti ad estremi di temperatura e di umidità; in particolare, esso non deve essere lasciato esposto al sole in un'autovettura chiusa e, qualora debba essere trasportato da un ambiente caldo ad uno freddo, o viceversa, con possibile sbalzo di temperatura significativo, prima dell'utilizzo deve essere lasciato passare un adeguato intervallo di tempo, per permettere all'eventuale condensa di dissolversi;
- Qualora il contenuto del supporto debba essere copiato su un hard disk, od altro strumento elettronico di trattamento, ci si accerti di cancellare il relativo contenuto, al termine dell'operazione di trattamento, in modo che l'asportazione del supporto comporti la asportazione completa dei dati registrati, in via temporanea, sullo strumento elettronico; si presti una particolare attenzione a che nessun dato sia rimasto nella memoria buffer, nella clipboard, negli appunti o all'interno del cestino, in sistemi operativi di tipo windows;
- Se l'operazione è ragionevolmente possibile, si raccomanda vivamente di compilare un registro con l'indicazione numerica, o con altro contrassegno, ove sono riportati tutti i suppori contenenti dati sensibili e giudiziari, la loro ubicazione, le modalità di accesso, gli eventuali estremi di consegna ad altro incaricato autorizzato;
- Il supporto contenente dati sensibili o giudiziari non deve mai essere lasciato abbandonato sul tavolo, ma deve essere immediatamente posto all'interno di una custodia sicura, quando non utilizzato; in funzione della criticità dei dati archiviati, si può andare da un cassetto della scrivania chiuso a chiave, sino ad un armadio blindato od una cassaforte, idonea alla custodia di supporti magnetici.

Informativa ex art. 13 del d. l.vo n. 196/2003

Si riporta qui di seguito il testo dell'informativa per i dipendenti della CCIAA di Napoli relativa ai trattamenti di dati personali degli stessi effettuati dall'ente.

PER I DIPENDENTI

INFORMATIVA AI SENSI DELL'ART. 13 DEL D.L.VO N. 196/2003

La Camera di Commercio, Industria, Agricoltura e Artigianato di Napoli (CCIAA di Napoli), in qualità di titolare delle banche dati **"Amministrazione del Personale" e "Sicurezza del Lavoro"**, con la presente provvede a sintetizzare quanto già oralmente comunicato ai sensi dell'art. 13 del d.l.vo n. 196/2003.

Finalità e modalità del trattamento

1) Per la banca dati **"Amministrazione del Personale"**, le finalità del trattamento attengono:

a) alla costituzione ed alla gestione del rapporto di lavoro con il personale, ivi comprese la custodia dei documenti originali relativi alla conclusione del contratto di lavoro subordinato ed alle successive vicende dello stesso, la determinazione ed il pagamento delle retribuzioni di qualsiasi genere e natura, la determinazione ed il pagamento dei rimborsi delle spese di trasferta, la determinazione degli oneri previdenziali e delle trattenute sindacali e l'adempimento degli obblighi relativi, l'adempimento degli obblighi di natura fiscale (modelli di dichiarazione), l'accertamento delle presenze e delle assenze, la gestione degli accertamenti sanitari obbligatori (esclusi quelli previsti dal D.lgs. 81/2008 e successive modifiche ed integrazioni) o richiesti dai dipendenti.

Il trattamento può riguardare anche dati c.d. sensibili ai sensi dell'art. 26 del d.l.vo n. 196/2003 in quanto idonei a rivelare lo stato di salute degli interessati o la loro appartenenza ad associazioni sindacali.

I dati, che vengono raccolti esclusivamente presso gli stessi interessati, sono conservati su supporto cartaceo e/o informatico ed utilizzati esclusivamente per i fini sopra indicati.

La riservatezza e la sicurezza dei dati sono garantite mediante l'utilizzo di armadi muniti di serratura, le cui chiavi sono custodite dal responsabile del trattamento e/o da persona da lui espressamente incaricata e nei quali vengono conservati, quando non sono utilizzati, sia i documenti cartacei che i supporti informatici contenenti i dati.

Inoltre, per quanto riguarda l'archivio elettronico dei dipendenti, la riservatezza e la sicurezza dei dati sono garantite anche dall'utilizzo di codici di accesso personalizzati per ciascun incaricato del trattamento, codici che vengono periodicamente modificati nei termini di legge.

2) Per la banca dati **"Sicurezza del Lavoro"**, le finalità del trattamento attengono all'effettuazione, nel rispetto di quanto disposto dal D. Lgs. 81/2008 della sorveglianza sanitaria obbligatoria cui sono sottoposti i dipendenti della CCIAA di Napoli nonché alla conservazione dei referti medici, relativi alle visite di idoneità, consegnati, in busta sigillata, dalla struttura specialistica che ha effettuato dette visite.

Il trattamento riguarda anche dati c.d. sensibili ai sensi dell'art. 26 del d.l.vo n. 196/2003 in quanto idonei a rivelare lo stato di salute degli interessati.

I dati personali vengono raccolti presso gli stessi interessati, salvo per quanto riguarda i certificati attestanti l'idoneità allo svolgimento delle mansioni ed i relativi referti medici (questi ultimi conservati sempre in busta sigillata) che vengono acquisiti presso le strutture sanitarie che effettuano le visite mediche. Detti dati, contenuti esclusivamente in documenti cartacei, vengono conservati per attuare la sorveglianza sanitaria disposta dal D. Lgs 81/2008 e successive modifiche ed integrazioni. Ad essi hanno accesso esclusivamente i soggetti incaricati del trattamento.

La riservatezza dei dati è garantita mediante l'utilizzo di armadi muniti di serratura, le cui chiavi sono custodite dal responsabile del trattamento e/o da persona da lui espressamente incaricata e nei quali vengono conservati i documenti quando non sono utilizzati.

Per tutte le banche dati indicate sono adottate le misure di sicurezza previste dall'Allegato "B" del D.L.vo n. 196/2003, e successivi aggiornamenti, nonchè tutte le misure che siano comunque idonee a ridurre al minimo il rischio di distruzione o perdita, anche accidentale, dei dati trattati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Natura del conferimento dei dati e conseguenze di un eventuale rifiuto di rispondere.

1) Banca dati **"Amministrazione del Personale"**

Per quanto riguarda le finalità di cui alla precedente lettera a):

- ai sensi dell'art. 24, comma 1, lett. a) del d.l.vo n. 196/2003, nessun consenso è necessario per il trattamento effettuato in adempimento di un obbligo di legge, di un regolamento o di una normativa comunitaria;
- ai sensi dell'art. 24, comma 1, lett. b) del d.l.vo n. 196/2003, nessun consenso è necessario per il trattamento dei dati personali ai fini dell'esecuzione di obblighi derivanti da contratto e per l'adempimento di un obbligo legale.

2) Banca dati "**Sicurezza del Lavoro**"
Essendo il trattamento e la comunicazione dei predetti dati sensibili necessario per l'adempimento di specifici obblighi di legge, il mancato consenso dell'interessato impedirà l'instaurazione del rapporto di lavoro.

Soggetti o categorie di soggetti ai quali i dati possono essere comunicati e ambito di diffusione dei dati medesimi.
1) Banca dati "**Amministrazione del Personale**"
I dati personali degli interessati potranno essere comunicati, esclusivamente per le finalità predette e limitatamente ai soli dati necessari, ai seguenti soggetti: Servizio ispezione del lavoro, INPS, INPDAP, Ministero delle Finanze, INAIL, Direzione provinciale del lavoro, nonchè, in generale, ad associazioni sindacali, compagnie di assicurazione, banche ed enti previdenziali.
Tali soggetti tratteranno i vostri dati personali in qualità di "titolari".

2) Banca dati "**Sicurezza del Lavoro**"
I dati personali contenuti in tale banca dati non saranno oggetto di comunicazione o diffusione a terzi.

Diritti di cui all'art.7 del D.L.vo n. 196/2003
L'interessato può esercitare in ogni momento i diritti di cui all'art. 7 del d.l.vo n. 196/2003 attraverso apposita istanza da presentare al Titolare o al Responsabile del Trattamento.
Dati del titolare e del responsabile
"Titolare" delle banche dati sopra indicate è la Camera di Commercio di Napoli.

Appendice A: Termini e definizioni

Codice	**DL 196/03**-"Codice di Protezione in materia di dati personali"
CCIAA di Napoli	Camera di Commercio, Industria, Artigianato e Agricoltura di Napoli

Nel seguito i termini "*Titolare*", "*Responsabile*", "*Incaricato*", "*Trattamento*" e "*Dato personale*" sono usati in conformità alle definizioni contenute nell'art. 4 (Definizioni) del Codice che si riportano per chiarezza.

Ai sensi del 1° comma dell'art. 4 del Codice si intende per:

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.

Ai sensi del 2° comma dell'art. 4 del Codice si intende, inoltre, per:

a) "***comunicazione elettronica***"	ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;
b) "***reti di comunicazione elettronica***"	i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;
c) "***rete pubblica di comunicazioni***"	una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;
l) "***posta elettronica***"	messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

Ai sensi del 3° comma dell'art. 4 del Codice si intende, altresì, 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 previsti nell'articolo 31;
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.

Ai sensi del 4° comma dell'art. 4 del Codice si intende, infine, per:

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

Appendice B: Sintesi della normativa

Il Codice in materia di protezione dei dati personali rappresenta un momento di consolidamento della numerosa produzione legislativa che ha fatto seguito alla pubblicazione della legge n. 675/1996 sul medesimo tema. La norma si applica a chiunque, in Italia, gestisca dati personali; restano esclusi i trattamenti di dati connessi ad attività di polizia, all'amministrazione della giustizia e alla sicurezza dello Stato.

La norma da una definizione di **dato personale** e di **trattamento**, attribuisce responsabilità ai **Titolari, Responsabili** e **Incaricati**; regolamenta i diritti spettanti ai soggetti **Interessati**, indica i criteri per stabilire le misure di **sicurezza dei dati** e disciplina la **comunicazione** e la **diffusione** dei dati stessi.

Il Titolare decide le finalità e le modalità del trattamento, il Titolare può nominare uno o più Responsabili a cui delegare parte dei compiti, il Titolare e il Responsabile possono/devono nominare gli Incaricati, che sono le persone fisiche che effettuano il trattamento.

La legge fornisce poi alcune indicazioni sulle modalità di raccolta e sui requisiti dei dati personali oggetto di trattamento, per cui i dati personali devono essere (cfr. art. 11):

a) trattati in modo lecito e secondo correttezza;

b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini non incompatibili con tali scopi;

c) esatti e, se necessario, aggiornati;

d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;

e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

Il principio generale affermato dalla legge è che il trattamento di dati personali è ammesso solo con il **consenso** espresso dell'Interessato.

Sebbene il principio del consenso sia generale, la legge prevede alcune significative eccezioni con la finalità di semplificare gli adempimenti. Non è necessario quindi il consenso nei seguenti casi principali (cfr. art. 24) quando il trattamento:

a) è necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
b) è necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato;
c) riguarda dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, fermi restando i limiti e le modalità che le leggi, i regolamenti o la normativa comunitaria stabiliscono per la conoscibilità e pubblicità dei dati;
d) riguarda dati relativi allo svolgimento di attività economiche, trattati nel rispetto della vigente normativa in materia di segreto aziendale e industriale;
e) è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal Responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2;
f) con esclusione della diffusione, è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397 (1), o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre

(1) In Appendice.

che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale;
g) con esclusione della diffusione, è necessario, nei casi individuati dal Garante sulla base dei principi sanciti dalla legge, per perseguire un legittimo interesse del Titolare o di un terzo destinatario dei dati, anche in riferimento all'attività di gruppi bancari e di società controllate o collegate, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato;
h) con esclusione della comunicazione all'esterno e della diffusione, è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, in riferimento a soggetti che hanno con essi contatti regolari o ad aderenti, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, e con modalità di utilizzo previste espressamente con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13;
i) è necessario, in conformità ai rispettivi codici di deontologia di cui all'allegato A), per esclusivi scopi scientifici o statistici, ovvero per esclusivi scopi storici presso archivi privati dichiarati di notevole interesse storico ai sensi dell'articolo 6, comma 2, del decreto legislativo 29 ottobre 1999, n. 490 ([2]), di approvazione del testo unico in materia di beni culturali e ambientali o, secondo quanto previsto dai medesimi codici, presso altri archivi privati, oggi art. 11 del d. l.vo n. 42 del 22 gennaio 2004 "Codice dei beni culturali e del paesaggio".

La legge prevede poi una speciale regolamentazione per il trattamento dei cosiddetti "**dati sensibili**" la cui tutela rappresenta uno dei diritti fondamentali del diritto alla riservatezza.

Sono "**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,
- lo stato di salute e la vita sessuale.

Queste tipologie di dati possono essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del Garante; anche in questo caso sono previste eccezioni che esentano dall'autorizzazione del garante e dall'obbligo del consenso.

La maggior parte dei trattamenti di dati di cui la CCIAA di Napoli è Titolare non riguarda dati sensibili e, d'altra parte, vi sono molte ipotesi di applicabilità delle eccezioni: sono infatti necessari ai fini dell'esecuzione di obblighi derivanti da un contratto di cui è parte la CCIAA di Napoli ovvero per adempiere a specifiche richieste dell'interessato; riguardano dati provenienti da pubblici registri, albi o elenchi, atti o documenti conoscibili da chiunque; riguardano dati relativi allo svolgimento di attività economiche; sono necessari per adempiere ad un obbligo di legge di regolamento o da una normativa comunitaria.

Oltre alla tutela della privacy, la legge ha la finalità di garantire la **salvaguardia del diritto all'identità personale**, evitando che circolino informazioni errate su persone (fisiche e giuridiche) e associazioni, per prevenire il rischio che ne venga alterata l'immagine o lesa la reputazione.

([2]) D. Lgs. 29 ottobre 1999, n. 490 (testo unico delle disposizioni legislative in materia di beni culturali e ambientali, a norma dell'art. 1 della legge 8 ottobre 1997, n. 352): «*Art. 6 (Dichiarazione). - 1. Salvo quanto disposto dal comma 4, il Ministero dichiara l'interesse particolarmente importante delle cose indicate all'art. 2, comma 1, lettera a) appartenenti a soggetti diversi da quelli indicati all'art. 5, comma 1.*

2. Il Ministero dichiara altresì l'interesse particolarmente importante delle cose indicate all'art. 2, comma 1, lettera b), l'eccezionale interesse delle collezioni o serie di oggetti indicati all'art. 2, comma 1, lettera c) e il notevole interesse storico dei beni indicati all'art. 2, comma 4, lettera c).

3. Gli effetti della dichiarazione sono stabiliti dall'art. 10.

4. La regione competente per territorio dichiara l'interesse particolarmente importante delle cose indicate nell'art. 2, comma 2, lettera c) di proprietà privata. In caso di inerzia della regione, il Ministero procede a norma dell'art. 9, comma 3, del decreto del Presidente della Repubblica 14 gennaio 1972, n. 3.».

Ai sensi della legge, l'**interessato ha il diritto** di (cfr. art. 7) venire a conoscenza:

a) dell'origine dei dati personali;
b) delle finalità e modalità del trattamento;
c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
d) degli estremi identificativi del Titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

Infine la norma pone particolare attenzione alla sicurezza con cui vengono effettuati i trattamenti. Tale sicurezza infatti dà la misura di quanto la tutela del trattamento sia effettivamente realizzata:

Art. 31 (Obblighi di sicurezza)

1. 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 e 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.

Questo articolo si applica anche al trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali (art. 5, comma 3°).

L'adozione delle regole di sicurezza da parte dei Titolari dei trattamenti viene garantita attraverso la previsione di alcune "misure minime", la cui mancanza determina l'applicazione di una sanzione penale.

Art. 33 (Misure minime)

1. 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'omessa adozione delle misure minime previste da questo articolo costituisce reato ai sensi dell'art. 169.

In tale ambito il Codice in materia di protezione dei dati personali individua le varie misure da adottare in maniera differenziata, a seconda degli strumenti impiegati per lo svolgimento dei trattamenti.

Art. 34 (Trattamenti con strumenti elettronici)

1. 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.

Art. 35 (Trattamenti senza l'ausilio di strumenti elettronici)

1. 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.

L'individuazione concreta delle misure minime da adottare viene effettuata all'interno del Disciplinare Tecnico in Materia di Misure Minime di Sicurezza, di cui all'Allegato "B" del D.L.vo n. 196/2003. In tale documento sono analiticamente indicate le misure nel rispetto della suddivisione tra trattamenti effettuati con strumenti elettronici e trattamenti effettuati senza l'ausilio di tali strumenti.