CAMERA DI COMMERCIO INDUSTRIA ARTIGIANATO E AGRICOLTURA NAPOLI

determinazione presidenziale
Allegato alla ~~delibera~~ n. 18 del 29-3-2011

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

(ex art. 34, 1° co., lett. g) del D. Lgs. 196/2003
e regola 19 Allegato B del D. Lgs. 196/2003)

(aggiornamento)

Sede: Via S. Aspreno, 2 - 80133 NAPOLI
Borsa Merci: Corso Meridionale, 58 - 80143 NAPOLI
Registro Imprese: Centro Direzionale is. C/2 - 80143 NAPOLI
centralino: 081/7607111 - C.F. 80014190633 - P. IVA 03121650638 - www.na.camcom.it

INDICE

APPENDICE

Riferimenti Normativi Generali

Decreto Legislativo n° 196/2003	**CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI** (Legge delega n. 127/2001) Decreto legislativo 30 giugno 2003, n° 196 (G.U. 29 luglio 2003, Serie generale n. 174, S.O. n. 123/L).
SICUREZZA DEI DATI E DEI SISTEMI	
MISURE DI SICUREZZA	artt. 31-36., D. Lgs. 196/2003
MISURE MINIME (riferimento normativo)	artt. 33-36, D. Lgs. 196/2003 **DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA** (Allegato B del Codice in materia di protezione dei dati personali)
MISURE MINIME (definizione normativa)	Art. 4, 3° c., lett. a): "*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*". Art. 33: "*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*".
OBBLIGATORIETÀ DELLE MISURE MINIME	**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 misure minime elencate nell'art. 34 del Codice.
SANZIONE PENALE	**Art. 169, 1° c.:** "*Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni o con l'ammenda da diecimila euro a cinquantamila euro*".
IL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA	
Art. 34, 1° c., lett. g)	obbligo di tenere un **aggiornato** documento programmatico sulla sicurezza.
Art. 169, 1° c.	*Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni o con l'ammenda da diecimila euro a cinquantamila euro.*
DISCIPLINARE TECNICO - ALLEGATO B	
Regola 19.	*Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:*
Regola 19.1.	***l'elenco** dei trattamenti di dati personali;*
Regola 19.2.	*la **distribuzione dei compiti e delle responsabilità** nell'ambito delle strutture preposte al trattamento dei dati;*
Regola 19.3.	***l'analisi dei rischi** che incombono sui dati;*
Regola 19.4.	***le misure da adottare** per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;*

Regola 19.5.	*la **descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati** in seguito a distruzione o danneggiamento di cui al successivo punto 23;*
Regola 19.6.	***la previsione di interventi formativi** degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. **La formazione è programmata già al momento dell'ingresso in servizio**, nonché **in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti**, rilevanti rispetto al trattamento di dati personali;*
Regola 19.7.	*la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza **in caso di trattamenti di dati personali affidati**, in conformità al codice, **all'esterno della struttura del titolare**;*
Regola 19.8.	*per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, **l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati** dagli altri dati personali dell'interessato.*

1. *Definizioni*

Codice	**DL 196/03**-"Codice di Protezione in materia di dati personali"
CCIAA	**C**amere di **C**ommercio **I**ndustria **A**rtigianato **A**gricoltura
CdC	**C**amera **di C**ommercio, Industria, Artigianato e Agricoltura
U.O.	**U**nità **O**rganizzativa (nelle Camere di Commercio)
Capo Ufficio	dipendente CdC a cui spetta la responsabilità organizzativa della U.O.

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 riferi-

	scono 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) "*chiamata*"	la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale;
c) "*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;
d) "*rete pubblica di comunicazioni*"	una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;
e) "*servizio di comunicazione elettronica*"	i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002;
f) "*abbonato*"	qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate;
g) "*utente*"	qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;

h) "***dati relativi al traffico***"	qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;
i) "***dati relativi all'ubicazione***"	ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;
l) "***servizio a valore aggiunto***"	il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione;
m) "***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.

2. *Generalità*

Dal 1 gennaio 2004 è entrato in vigore il nuovo Codice in Materia di Protezione dei Dati Personali (Decreto legislativo 30 giugno 2003, n. 196) che sostituisce ogni altra precedente norma in tema di privacy.
Tale codice ribadisce il principio che i dati personali oggetto di trattamento debbano essere 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** (cfr. art. 31)
Nel quadro dei più generali obblighi di sicurezza sopra descritti o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare misure di sicurezza volte ad assicurare un livello adeguato di protezione dei dati personali.
Il trattamento di dati personali è consentito solo se sono adottate le seguenti **misure minime di sicurezza**, nei modi previsti dall'apposito disciplinare tecnico.

- Autenticazione informatica;
- Adozione di procedure di gestione delle credenziali di autenticazione;
- Utilizzazione di un sistema di autorizzazione;
- Aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- Protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- Adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- Tenuta di un aggiornato documento programmatico sulla sicurezza.

La Camera di Commercio opera in qualità di Titolare del trattamento per le banche dati ed i trattamenti rientranti nell'ambito delle proprie funzioni istituzionali.

2.1. Riferimenti normativi specifici

La Camera di Commercio, in quanto Titolare di trattamenti di dati personali, è impegnata al rispetto della normativa generale contenuta nel Codice.
In particolare, in quanto ente autonomo di diritto pubblico, ad essa sono applicabili le norme specifiche di cui al Titolo III, capo II, intitolato "*Regole ulteriori per i soggetti pubblici*" di cui al medesimo codice, che si riportano di seguito:

CAPO II
REGOLE ULTERIORI PER I SOGGETTI PUBBLICI

Art. 18 (Principi applicabili a tutti i trattamenti effettuati da soggetti pubblici)

1. Le disposizioni del presente capo riguardano tutti i soggetti pubblici, esclusi gli enti pubblici economici.

2. Qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali.

3. Nel trattare i dati il soggetto pubblico osserva i presupposti e i limiti stabiliti dal presente codice, anche in relazione alla diversa natura dei dati, nonché dalla legge e dai regolamenti.

4. Salvo quanto previsto nella Parte II per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, i soggetti pubblici non devono richiedere il consenso dell'interessato.

5. Si osservano le disposizioni di cui all'articolo 25 in tema di comunicazione e diffusione.

Art. 19 (Principi applicabili al trattamento di dati diversi da quelli sensibili e giudiziari)

1. Il trattamento da parte di un soggetto pubblico riguardante dati diversi da quelli sensibili e giudiziari è consentito, fermo restando quanto previsto dall'articolo 18, comma 2, anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente.

2. La comunicazione da parte di un soggetto pubblico ad altri soggetti pubblici è ammessa quando è prevista da una norma di legge o di regolamento. In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di cui all'articolo 39, comma 2, e non è stata adottata la diversa determinazione ivi indicata.

3. La comunicazione da parte di un soggetto pubblico a privati o a enti pubblici economici e la diffusione da parte di un soggetto pubblico sono ammesse unicamente quando sono previste da una norma di legge o di regolamento.

Art. 20 (Principi applicabili al trattamento di dati sensibili)

1. Il trattamento dei dati sensibili da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite.

2. Nei casi in cui una disposizione di legge specifica la finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili, il trattamento è consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che ne effettuano il trattamento, in relazione alle specifiche finalità perseguite nei singoli casi e nel rispetto dei principi di cui all'articolo 22, con atto di natura regolamentare adottato in conformità al parere espresso dal Garante ai sensi dell'articolo 154, comma 1, lettera g), anche su schemi tipo.

3. Se il trattamento non è previsto espressamente da una disposizione di legge i soggetti pub-

blici possono richiedere al Garante l'individuazione delle attività, tra quelle demandate ai medesimi soggetti dalla legge, che perseguono finalità di rilevante interesse pubblico e per le quali è conseguentemente autorizzato, ai sensi dell'articolo 26, comma 2, il trattamento dei dati sensibili. Il trattamento è consentito solo se il soggetto pubblico provvede altresì a identificare e rendere pubblici i tipi di dati e di operazioni nei modi di cui al comma 2.

4. L'identificazione dei tipi di dati e di operazioni di cui ai commi 2 e 3 è aggiornata e integrata periodicamente.

Art. 21 (Principi applicabili al trattamento di dati giudiziari)

1. Il trattamento di dati giudiziari da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le finalità di rilevante interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili.

2. Le disposizioni di cui all'articolo 20, commi 2 e 4, si applicano anche al trattamento dei dati giudiziari.

Art. 22 (Principi applicabili al trattamento di dati sensibili e giudiziari)

1. I soggetti pubblici conformano il trattamento dei dati sensibili e giudiziari secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato.

2. Nel fornire l'informativa di cui all'articolo 13 i soggetti pubblici fanno espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati sensibili e giudiziari.

3. I soggetti pubblici possono trattare solo i dati sensibili e giudiziari indispensabili per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa.

4. I dati sensibili e giudiziari sono raccolti, di regola, presso l'interessato.

5. In applicazione dell'articolo 11, comma 1, lettere c), d) ed e), i soggetti pubblici verificano periodicamente l'esattezza e l'aggiornamento dei dati sensibili e giudiziari, nonché la loro pertinenza, completezza, non eccedenza e indispensabilità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. Al fine di assicurare che i dati sensibili e giudiziari siano indispensabili rispetto agli obblighi e ai compiti loro attribuiti, i soggetti pubblici valutano specificamente il rapporto tra i dati e gli adempimenti. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per la verifica dell'indispensabilità dei dati sensibili e giudiziari riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni o gli adempimenti.

6. I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.

7. I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. I medesimi dati sono trattati con le modalità di cui al comma 6 anche quando sono tenuti in elenchi, registri o banche di dati senza l'ausilio di strumenti elettronici.

8. I dati idonei a rivelare lo stato di salute non possono essere diffusi.

9. Rispetto ai dati sensibili e giudiziari indispensabili ai sensi del comma 3, i soggetti pubblici

sono autorizzati ad effettuare unicamente le operazioni di trattamento indispensabili per il perseguimento delle finalità per le quali il trattamento è consentito, anche quando i dati sono raccolti nello svolgimento di compiti di vigilanza, di controllo o ispettivi.

10. I dati sensibili e giudiziari non possono essere trattati nell'ambito di test psicoattitudinali volti a definire il profilo o la personalità dell'interessato. Le operazioni di raffronto tra dati sensibili e giudiziari, nonché i trattamenti di dati sensibili e giudiziari ai sensi dell'articolo 14, sono effettuati solo previa annotazione scritta dei motivi.

11. In ogni caso, le operazioni e i trattamenti di cui al comma 10, se effettuati utilizzando banche di dati di diversi titolari, nonché la diffusione dei dati sensibili e giudiziari, sono ammessi solo se previsti da espressa disposizione di legge.

12. Le disposizioni di cui al presente articolo recano principi applicabili, in conformità ai rispettivi ordinamenti, ai trattamenti disciplinati dalla Presidenza della Repubblica, dalla Camera dei deputati, dal Senato della Repubblica e dalla Corte costituzionale.

2.2.Struttura del sistema camerale

Il sistema camerale italiano si articola in 103 CCIAA, 19 Unioni Regionali, una Unioncamere nazionale e numerose agenzie specializzate nazionali.

Unioni Regionali

Ai fini di una più organica iniziativa volta allo sviluppo economico-imprenditoriale dell'area territoriale di competenza, l'art. 6, comma 1, della L. n. 580/1993 le Camere di Commercio possono associarsi, costituendo apposite associazioni prive di personalità giuridica, in Unioni Regionali:

- per lo sviluppo delle attività che interessino, nell'ambito della Regione, più di una circoscrizione territoriale;
- per il coordinamento dei rapporti con gli enti regionali territorialmente competenti.

Unione Italiana delle Camere di Commercio (Unioncamere)

L'Unioncamere è una federazione degli enti camerali avente personalità giuridica di diritto pubblico (riconosciuta con D.P.R. 30 giugno 1954, n. 709).

Alla stessa devono obbligatoriamente aderire tutte le CCIAA operanti sul territorio nazionale, nonché la Regione autonoma Valle d'Aosta per il tramite del competente assessore regionale.

I compiti istituzionali dell'Unioncamere sono i seguenti:

- curare e rappresentare gli interessi delle CCIAA, anche in quanto autonomie funzionali ex lege n. 59/97;
- promuovere, realizzare e gestire, direttamente o tramite proprie aziende speciali, nonché con la partecipazione ad altri organi, anche a carattere associativo, ad enti, a consorzi ed a società anche a prevalente capitale privato, servizi di interesse delle CCIAA e delle categorie economiche.

In base allo statuto Unioncamere provvede altresì a curare i rapporti con le istituzioni nazionali ed internazionali e con le categorie, promuove e realizza iniziative coordinate ed incentiva l'attività del sistema camerale in tutte le sue articolazioni, anche per favorire lo sviluppo a rete. Essa pone in essere ogni iniziativa volta a favorire la presenza delle imprese italiane sui mercati mondiali, coordinando il sistema camerale italiano con i sistemi operanti in ambito comunitario ed extracomunitario. L'Unioncamere inoltre costituisce commissioni, osservatori e centri specializzati, realizza studi, indagini e ricerche, organizza congressi e convegni, partecipa all'attività di enti aventi finalità di interesse per le Camere di Commercio ed è legittimata ad assumere ogni iniziativa, anche giudiziaria, per la tutela della denominazione e delle prerogative delle Camere di Commercio in Italia.

Camera di Commercio, Industria, Agricoltura ed Artigianato

Le Camere di Commercio, ai sensi dell'art. 1 della legge 29 dicembre 1993, n. 580, sono enti autonomi di diritto pubblico che svolgono, nell'ambito della circoscrizione territoriale di competenza, funzioni di interesse generale per il sistema delle imprese curandone lo sviluppo nell'ambito delle economie locali.

Le Camere di Commercio hanno sede in ogni capoluogo di provincia e la loro circoscrizione territoriale coincide, di regola, con quella della provincia o dell'area metropolitana.

InfoCamere S.C.p.A.

InfoCamere S.C.p.A. è la società consortile di informatica delle Camere di Commercio. In base allo statuto la società "non ha scopo di lucro ed ha per oggetto il compito di approntare, organizzare e gestire nell'interesse e per conto delle CCIAA e con criteri di economicità gestio-

nale, un sistema informatico in grado di trattare e distribuire in tempo reale, anche a soggetti terzi, atti, documenti e informazioni che la legge dispone siano oggetto di pubblicità legale o di pubblici notizia o che comunque scaturiscano da registri, albi, ruoli, elenchi e repertori tenuti dalle CCIAA.

Aziende Speciali

Ai sensi dell'art. 2, secondo comma, della legge n. 580/1993, le Camere di Commercio per il raggiungimento dei loro scopi promuovono, realizzano e gestiscono strutture ed infrastrutture di interesse economico generale a livello locale, regionale e nazionale, direttamente o mediante la partecipazione, secondo le norme del codice civile, con altri soggetti pubblici e privati, ad organismi anche associativi, ad enti, a consorzi e a società. Possono inoltre costituire aziende speciali operanti secondo le norme del diritto privato.

Le Aziende Speciali operano in qualità di autonomi Titolari dei trattamenti da esse effettuato.

2.3. Funzioni delle Camere di Commercio

Tali funzioni sono definite dettagliatamente dall'art. 2, commi 1, 4, 5 e 6 della legge n. 580/1993 e successive modificazioni ed integrazioni.

Ai sensi della norma citata le funzioni istituzionali che le CCIAA sono chiamate a svolgere riguardano:

- il supporto e la promozione degli interessi generali delle imprese;
- le materie amministrative ed economiche relative al sistema delle imprese, fatte salve le specifiche attribuzioni di competenza delle amministrazioni statali e delle regioni;
- specifiche funzioni delegate dallo Stato e dalle regioni o da convenzioni internazionali;
- funzioni di regolazione del mercato con possibilità per le CCIAA di:
  - > promuovere la costituzione di commissioni arbitrali e conciliative per la risoluzione delle controversie tra imprese, e tra queste ed i consumatori ed utenti;
  - > predisporre e promuovere contratti-tipo tra imprese, loro associazioni e associazioni di tutela degli interessi dei consumatori e degli utenti;
  - > promuovere forme di controllo sulla presenza di clausole inique inserite nei contratti.

Tra le funzioni sopra richiamate quella il cui esercizio implica in misura più rilevante il trattamento di dati personali è la funzione amministrativa, consistente nella tenuta di registri (variamente denominati) in cui sono iscritti i soggetti che svolgono le più svariate attività nei settori del commercio, industria, agricoltura ed artigianato.

Detti registri si dividono in registri anagrafici ed in registri abilitanti.

L'istituzione di ciascun registro, albo, ruolo od elenco, i requisiti professionali e morali che gli operatori economici devono possedere per l'iscrizione negli stessi, la tenuta e gestione dei medesimi da parte delle Camere di Commercio, sono indicati nelle varie normative specifiche che li disciplinano.

La lista dei trattamenti svolti in tali ambiti è contenuta nell'apposita sezione del presente documento.

3. *Obblighi previsti dalla legge*

Per la CdC, in base al Codice, l'emissione del Documento Programmatico sulla Sicurezza è obbligatoria. L'emissione di questo documento deriva dalle prescrizioni di cui alle Misure minime di Sicurezza previste nell'Allegato B del Codice.

3.1 Campo di applicabilità

Il presente Documento Programmatico sulla Sicurezza si applica alla Camera di Commercio di Napoli.

Le prescrizioni contenute in questo documento vanno applicate in generale a qualunque trattamento di Dati Personali effettuato nell'Ente, quindi ai Trattamenti di Dati:

- dei quali l'Ente è direttamente Titolare
- dei quali l'Ente è co-titolare, insieme ad altro ente od organizzazione
- dei quali l'Ente ha affidato alcune operazioni del trattamento ad apposito Responsabile
- dei quali l'Ente opera in qualità di Responsabile.

Va precisato che con riferimento ad alcuni trattamenti e banche dati gestiti nel Sistema Informatico Camerale l'Ente ha provveduto, con **delibera G.C. n. 22 del 31.03.1999**, a nominare la società InfoCamere S.C.p.A. quale Responsabile del trattamento, rinnovando tale nomina, in conseguenza dell'entrata in vigore del Codice, con atto del **21.05.2008 Prot. 21519/08**.

L'Ente Camerale, inoltre, ha provveduto alla nomina di "Responsabile del trattamento" della società InfoCert S.p.A., relativamente ai trattamenti di dati effettuati a mezzo del "Protocollo Informatico", informaticamente gestito da tale società, ed alle attività inerenti alla Carta Nazionale dei Servizi.Per tali attività il titolare del trattamento provvederà all'integrazione della nomina relativamente alle funzioni di Amministratore di Sistema.

Per il trattamento di tali dati, delle relative banche dati, e per le misure di sicurezza inerenti agli stessi la CdC verifica l'operato dei Responsabili attraverso l'esame dei Documenti Programmatici sulla sicurezza adottati da questi ultimi.

Il Titolare del trattamento inoltre ha provveduto, con apposito atti, a nominare la InfoCamere S.C.p.A. ed i sig.ri Mario Rosario De Marco, Angelo Raffaele Caprioli, Giuseppe Passaro, dipendenti dell'ente camerale, nella veste di "Amministratore di Sistema", in osservanza del provvedimento del 27 novembre 2008, pubblicato in G.U. n. 300 del 24 dicembre 2008, con cui l'Autorità garante della protezione dei dati personali ha dettato apposite *"Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema".*

In tale veste gli amministratori di sistema provvedono a:

- assicurare la custodia delle credenziali per la gestione dei sistemi di autenticazione e di autorizzazione in uso;
- predisporre e rendere funzionanti le copie di sicurezza (operazioni di backup e recovery) dei dati e delle applicazioni di competenza;
- predisporre sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione ed agli archivi elettronici da parte dell' "amministratore di sistema"; tali registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

3.2 Obbligo dell'osservanza delle disposizioni del DPS in Camera di commercio

Le prescrizioni contenute nel presente documento vanno rispettate e fatte rispettare all'interno della CdC, per le competenze di ciascuno. Tutti i dipendenti della CdC, devono essere edotti sulla sua esistenza e informati sui contenuti.

Eventuali situazioni di deviazione accertate rispetto a quanto prescritto nel presente documento dovranno essere rimosse nel più breve tempo possibile.

Il presente documento deve essere aggiornato, almeno annualmente, entro il 31 marzo di ogni anno.

4. *Titolare del trattamento*

Ai sensi dell'art. 4, 1° comma, lett. f) del Codice, per titolare s'intende "*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*".

Art. 28 del Codice – Titolare del trattamento. "*Quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo, **titolare del trattamento è l'entità nel suo complesso** o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza*".

Nel presente Documento Programmatico sulla Sicurezza, il ***titolare del trattamento*** dei dati personali è:

Camera di Commercio Industria Artigianato ed Agricoltura di Napoli.

Via S. Aspreno n. 2 - 80133- Napoli

http://www.na.camcom.it/

Ulteriori sedi:

Borsa Merci
Corso Meridionale, 58 - 80143 Napoli

Registro delle Imprese
Centro Direzionale di Napoli - Isola C/2 - 80143 Napoli

5. *Elenco dei trattamenti di dati personali effettuati*

Riferimento normativo: ***D.L.vo n. 196/2003 – Allegato "B", Disciplinare tecnico in materia di misure minime di sicurezza. (Regola 19.1)***

Nel presente paragrafo sono individuati i trattamenti effettuati dalla CdC, direttamente o attraverso collaborazioni esterne, con l'indicazione della natura dei dati e della struttura interna od esterna operativamente preposta, nonché degli strumenti impiegati.

Per ciascun trattamento è indicato un apposito numero/codice identificativo, valido nell'ambito del presente Documento Programmatico sulla Sicurezza, al fine di una più agevole individuazione nelle tabelle del trattamento considerato.

Vedere in Appendice:

Tabella 1.1. ***ELENCO DEI TRATTAMENTI DI DATI PERSONALI***

5.1. *TRATTAMENTI CARTACEI DI DATI SENSIBILI O GIUDIZIARI*

I trattamenti cartacei effettuati nell'ambito della Camera sono indicati in tabella 1.1.

In particolare, relativamente alle varie aree si segnalano trattamenti che possono riguardare dati sensibili 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

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

6. *Competenze e responsabilità delle strutture preposte ai trattamenti*

Riferimento normativo: ***D.L.vo n. 196/2003 – Allegato "B", Disciplinare tecnico in materia di misure minime di sicurezza. (Regola 19.2)***

L'articolazione delle competenze e delle responsabilità delle singole strutture preposte ai trattamenti discende primariamente dall'organigramma dell'Ente.

In tale ambito è possibile distinguere i trattamenti effettuati dalla CdC in due grandi categorie:

1) trattamenti effettuati nello svolgimento delle funzioni istituzionali;
2) trattamenti, previsti dalla legge, effettuati per esigenze organizzative dell'Ente.

Tipicamente i trattamenti rientranti nel secondo tipo hanno ad oggetto:

a) Dati contabili
Inerenti ai dati necessari per la gestione della contabilità dell'Ente.
Detti dati vengono utilizzati esclusivamente per rapporti di carattere commerciale e non vengono trattati da personale non autorizzato né ceduti o comunque comunicati e/o diffusi a terzi.

b) Dati retributivi e del personale
Inerenti ai dati necessari per l'amministrazione del personale della CdC.
Detti archivi vengono utilizzati esclusivamente per rapporti di carattere amministrativo e non vengono trattati da personale non autorizzato né ceduti o comunque comunicati e/o diffusi a terzi, fatti salvi gli obblighi di legge.

Nell'ambito dei trattamenti effettuati dalla CdC, con particolare riferimento ai trattamenti effettuati con strumenti elettronici, alle relative banche dati ed alle procedure di archiviazione e ripristino dei dati informatici, assume particolare rilievo la distribuzione dei compiti tra la CdC ed InfoCamere S.C.p.A., essendo quest'ultima la società consortile che per statuto è deputata alla gestione ed amministrazione in maniera informatica dei dati trattati nell'ambito del sistema camerale ed avendo ricevuto la nomina a Responsabile del trattamento.

La stessa, inoltre, provvede a mettere a disposizione in favore delle CdC che ne abbiano fatto espressa richiesta, altre procedure informatiche a supporto delle procedure interne di gestione della contabilità e del personale dell'ente.

6.1 La distribuzione dei compiti tra InfoCamere e Camere di Commercio

6.1.1. InfoCamere

InfoCamere, con riferimento ai Patti Consortili e relativamente ai dati Camerali, ha le seguenti responsabilità:

- determinare le procedure per la sicurezza dei dati e verificare le necessità di aggiornamento delle stesse e delle misure in esse specificate;
- amministrare la sicurezza informatica dell'intero sistema di sua pertinenza e delle componenti di sistema ad essa delegate dalle CCIAA;
- effettuare periodici controlli e verifiche in merito al rispetto delle prescrizioni contenute nel presente Documento Programmatico sulla Sicurezza;
- valutare periodicamente il livello di rischio di sicurezza dei dati;
- predisporre un adeguato piano di formazione dei propri incaricati del trattamento circa i rischi e le contromisure da adottare;
- implementare le misure organizzative e tecniche necessarie a garantire un adeguato *standard* di sicurezza relativamente al trattamento dei dati, nel pieno rispetto degli adempimenti di legge.

6.1.2. CAMERA DI COMMERCIO

La Camera di Commercio è responsabile, per le attività che le competono, di predisporre le opportune procedure per mettere in atto le misure di protezione previste dal presente documento, soprattutto in relazione ai rischi derivanti dalle interconnessioni tra le strutture informatiche proprie del Sistema Camerale ed InfoCamere. È responsabile altresì dei Trattamenti, ancorché riferiti alle Banche Dati Istituzionali, non delegati esplicitamente ad InfoCamere.

Con riferimento alla Camera di Commercio di Napoli risultano definite le seguenti Aree:

S.1.	**AREA GESTIONE DEL PERSONALE E DELLA SICUREZZA** **1)** Servizio gestione del personale: **a)** Ufficio gestione del personale; **b)** Ufficio trattamento economico e di quiescenza; **2)** Servizio organizzazione: **a)** Ufficio organizzazione e metodo; **3)** Servizio sicurezza e relazioni sindacali: **a)** Ufficio relazioni sindacali; **b)** Ufficio sicurezza e prevenzione.
S.2.	**AREA GESTIONE RISORSE** **1)** Servizio Ragioneria e bilancio: **a)** Ufficio contabilità e bilancio; **b)** Ufficio contabilità fornitori e beneficiari; **c)** Ufficio entrate; **d)** Ufficio controllo di gestione; **2)** Servizio Acquisti e patrimonio: **a)** Ufficio economato; **b)** Ufficio tecnico; **c)** Ufficio appalti e contratti.
S.3.	**AREA PROGRAMMAZIONE E AFFARI GENERALI** **1)** Servizio Affari Generali: **a)** Ufficio programmazione e A.A.G.G. e Informazioni; **b)** Ufficio gestione partecipazioni **c)** Ufficio protocollo e archivio; **2)** Servizio Comunicazioni stampa e Relazioni esterne: **a)** Ufficio stampa e relazioni esterne; **b)** Ufficio cerimoniale; **3)** Servizi Ausiliari Tecnici: **a)** Ufficio centralino e informazioni; **b)** Ufficio meccanografico.
S.4.	**AREA ANAGRAFE ECONOMICA** **1)** Servizio Registro Imprese: **a)** Ufficio Diritto Annuale e procedure concorsuali nonché Ufficio polifunzionale per il Commercio; **b)** Ufficio Sezione Ordinaria; **c)** Ufficio Sezione Speciale Registro Imprese – REA; **d)** Ufficio di qualificazione imprese di impiantistica, autoriparatrici, di pulizia e di facchinaggio; **e)** Ufficio di Consulenza e Formazione informatica – Rilascio smart card, etc.; **f)** Ufficio Segreteria del Conservatore; **2)** Servizio Albi, Ruoli ed Attività speciali: **a)** Ufficio Segreteria Albo Imprese artigiane; **b)** Ufficio Licenze e concessioni speciali; **c)** Ufficio Ruoli Elenchi ed Albi; **d)** Ufficio Albo Regionale smaltimento rifiuti (SISTRI).
S.5.	**AREA STUDI** **1)** Servizio Studi prezzi e documentazione: **a)** Ufficio Studi e documentazione; **b)** Ufficio prezzi; **2)** Servizio Statistica: **a)** Ufficio Protesti; **b)** Ufficio Statistica; **3)** Servizio Regolazione del mercato e tutela del consumatore: **a)** Ufficio brevetti e tutela del mercato; **b)** Ufficio Metrico; **c)** Ufficio conciliazione e segreteria corte arbitrale; **d)** Ufficio MUD; **4)** Servizio biblioteca ed emeroteca: **a)** Ufficio biblioteca ed emeroteca.
S.6.	**AREA PROMOZIONE**

	1) Servizio Promozione attività Produttive: **a)** Ufficio Promozione attività produttive; **b)** Ufficio Marketing Territoriale; **2)** Servizio Promozione estera e incentivi finanziari: **a)** Ufficio sostegno al credito (Confidi); **b)** Ufficio Commercio con l'estero, banche dati estere e rapporti comunitari.

Sono servizi in staff al Segretario Generale:

1) Segreteria Organi; **2)** U.R.P. **3);** Segreteria Nucleo di Valutazione; **4)** Ufficio legale; **5)** Ufficio Controllo interno.

Vedere in Appendice:

Tabella 2. **La distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati**

7. *Analisi dei rischi che incombono sui dati*

Riferimento normativo: ***D.L.vo n. 196/2003 – Allegato "B", Disciplinare tecnico in materia di misure minime di sicurezza. (Regola 19.3)***

Ai fini della redazione del presente Documento Programmatico sulla sicurezza la CdC ha provveduto ad effettuare un'analisi dei rischi che incombono sui dati e sulle loro elaborazioni e fruibilità.

Giova richiamare quanto disposto a tal proposito dall'art. 31 del Codice, che detta il principio generale in materia di obblighi di sicurezza:

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***:
1 – di distruzione o perdita, anche accidentale, dei dati stessi
2 – di accesso non autorizzato
3 – di trattamento non consentito o non conforme alle finalità della raccolta

In conformità alle previsioni dell'Allegato "B", Disciplinare tecnico in materia di misure minime di sicurezza, nonché alla "Guida operativa per redigere il Documento programmatico sulla sicurezza (DPS)" emanata dall'Autorità Garante per la protezione dei dati personali in data 11.06.2004, la CdC ha provveduto a rilevare, coadiuvata da InfoCamere, i principali eventi potenzialmente dannosi per la sicurezza dei dati, con le relative possibili conseguenze e la gravità di ciascuna di esse.

L'analisi dei rischi è stata estesa sia al trattamento di dati attraverso strumenti elettronici, sia ai trattamenti cartacei ed in considerazione del contesto fisico – ambientale in cui i trattamenti vengono effettuati.

Con specifico riferimento ai trattamenti con strumenti elettronici, in considerazione della distribuzione dei compiti sopra esaminata, l'analisi dei rischi e l'adozione delle misure di sicurezza necessari a contrastarli viene demandata ad InfoCamere, per i trattamenti di competenza di quest'ultima in base agli accordi consortili ed alla sua funzione di Responsabile.

L'analisi dei rischi viene riveduta almeno annualmente e comunque tenuta aggiornata rispetto all'evoluzione delle tecnologie e/o a mutamenti organizzativi dell'ente.

In merito alla sicurezza dei locali si rinvia agli adempimenti attuati dalla CdC in osservanza delle previsioni del D.Lgs. n. 81/2008.

SISTEMA DI MISURAZIONE: l'analisi dei rischi è stata effettuata adottando un sistema di misurazione di tipo qualitativo (rischio alto/medio/basso). La valutazione è eseguita considerando il contesto operativo in cui il rischio viene collocato, il livello del rischio del fattore umano commisurato al grado di consapevolezza da parte del singolo operatore, e il livello di protezione assicurato dagli strumenti adottati.

METODO DI VALUTAZIONE: il metodo di valutazione tiene conto ed esprime un valore di rischio per ciascuna minaccia tenuto conto della natura del dato trattato, della finalità del trattamento, della destinazione o meno del dato ad essere reso pubblico nell'ambito delle funzioni istituzionali esercitate dall'Ente.

Vedere in Appendice:

Tabella 3. Analisi dei rischi che incombono sui dati

8. Misure in essere e da adottare

Riferimento normativo: ***D.L.vo n. 196/2003 – Allegato "B", Disciplinare tecnico in materia di misure minime di sicurezza. (Regola 19.4)***

Nell'ambito della CdC i trattamenti che coinvolgono e/o possono coinvolgere dati sensibili o giudiziari sono effettuati sia con strumenti informatici sia senza l'ausilio di strumenti informatici.

Con riferimento alla prima tipologia di trattamenti la CdC si avvale delle procedure informatiche messe a disposizione dalla InfoCamere S.C.p.A., e meglio precisate nella ***"Tabella 1.1. Elenco dei trattamenti"*** presente in Appendice.

La InfoCamere S.C.p.A. è stata nominata Responsabile di tali trattamenti, ed essi ricomprendono l'elaborazione, l'organizzazione, la conservazione, la consultazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, la comunicazione, la diffusione, la cancellazione e la distruzione dei dati.

Il Responsabile è impegnato a porre in essere le operazioni di trattamento in conformità alla tipologia di dato trattato ed alle finalità perseguite con il trattamento stesso.

Ogni procedura informatica realizzata da InfoCamere è strutturata secondo un'architettura client/server. In tale contesto la CdC provvede alla raccolta ed alla registrazione dei dati, alla loro estrazione, utilizzo comunicazione e diffusione.

Le misure in essere e da adottare con riferimento a dette procedure sono pertanto a carico del Responsabile del trattamento, che provvede a definire i sistemi di autenticazione ed autorizzazione, le procedure per il salvataggio dei dati e quelle per il loro ripristino.

Per quanto riguarda i trattamenti effettuati con strumenti elettronici posti in essere direttamente dalla CdC, ossia senza avvalersi delle procedure informatiche messe a disposizione da InfoCamere o da altro soggetto esterno, l'ente provvede direttamente ad adeguarsi alle prescrizioni in materia di misure minime di sicurezza.

Relativamente ai trattamenti per cui si è proceduto a nominare la società InfoCert S.p.A. in qualità di responsabile, sono adottate regole di sicurezza uniformi a quelle applicate da InfoCamere.

E' stata confermata, con determina n. 6 del 31/03/2009, la dr.ssa Teodora Ferrara nella qualità di Responsabile del trattamento dei dati personali, ed è stato nominato come ulteriore Responsabile del trattamento, in sostituzione del dr. Lucio Tisi, il 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.

8.1. SICUREZZA FISICA

I controlli istituiti per limitare l'accesso fisico ad alcuni dati personali, sensibili e/o giudiziari sono indispensabili anche al fine di evitare il furto o la diffusione o distruzione non autorizzata di informazioni personali che possono esporre la CdC al rischio di violare la legge in particolare il D.Lgs. 196/03, che riprende comunque disposizioni già in vigore, oltre a metterla nella condizione di non garantire servizi essenziali eventualmente ad essa affidati.

8.1.1. SICUREZZA FISICA DEI DATI ELABORATI 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 TU D.Lgs. 196 (art 35) e la CdC 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.

Sono definite aree ad accesso controllato quei locali che contengono dati personali, sensibili e/o giudiziari, conservati su supporti non informatici (documenti cartacei, microfilms, etc.).

Le aree ad accesso controllato devono essere all'interno di aree sotto la responsabilità della Camera di Commercio.

Per tali aree:

- Il locale deve essere chiuso, salvo eventuali accessi autorizzati da parte di singoli incaricati e/o imprese di pulizia o sorveglianza.
- L'accesso deve essere consentito solo alle persone autorizzate.
- L'accesso deve essere possibile solo dall'interno dell'area sotto la responsabilità della Camera di Commercio.

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 della D. L.vo 81/2008.

Con determinazione segretariale n. 741 del 27.09.2010 la CdC ha provveduto ad attivare il sistema di videosorveglianza e videoregistrazione lungo il perimetro degli edifici delle sedi, con funzioni che attivano il funzionamento nei periodi di chiusura degli uffici.

8.1.2. SITUAZIONI SPECIFICHE:

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

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

I locali in cui vengono effettuati i trattamenti sopra citati sono muniti di armadi chiusi a chiave ove vengono riposti i fascicoli. I locali sono chiusi a chiave.

I trattamenti sono svolti unicamente dai soggetti appositamente incaricati nell'ambito di ciascun ufficio.

8.2. SICUREZZA INFORMATICA

Come già sopra evidenziato la gran parte dei trattamenti con strumenti elettronici effettuati dall'Ente avviene avvalendosi dei servizi forniti dalla InfoCamere, e tramite le procedure informatiche dalla stessa messe a disposizione.

Di seguito si riportano pertanto le policy di sicurezza adottate dalla medesima InfoCamere per i trattamenti ad essa demandati dalla CdC. Al termine dell'esposizione saranno evidenziate le specifiche misure adottate dall'Ente per i trattamenti con strumenti informatici effettuati senza l'ausilio delle procedure InfoCamere.

8.2.1. 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 InfoCamere e Camerale ove InfoCamere la gestisce.

8.2.2. PROTEZIONE DA PROGRAMMI PERICOLOSI

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

8.2.3. 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.

8.2.4. 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. IC-Rete, rete geografica del Sistema Informatico Camerale, è gestita da InfoCamere e InfoCamere stessa ha il compito di assicurarne la sicurezza nella sua funzione di Responsabile del trattamento.

Per assicurare la sicurezza di una rete è fondamentale controllare gli accessi alla rete stessa.

Sono considerate connessioni con l'esterno i collegamenti di IC-Rete con altre reti, in particolare:

- interconnessioni tra i servizi informatici e telematici di InfoCamere e quelli di altre aziende, incluso Internet.
- accesso remoto da parte di dipendenti di Camere, di InfoCamere 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.

8.2.5. 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 o sotto il controllo diretto di InfoCamere o comunque approvati da InfoCamere.

8.2.6. ISOLAMENTO DELLE RETI

La CCIAA 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.

L'architettura delle interconnessioni tra la rete interna delle CCIAA e la rete InfoCamere viene concordata con InfoCamere stessa.

8.2.7. 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.

8.2.8. 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) o smart-card (Identificativo Univoco dell'Utente in essa contenuto)

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

8.2.9. 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 o certificato presente su smart-card).

Tali informazioni sono definite Credenziali.

8.2.10. FUNZIONE DI AUTENTICAZIONE

Le Credenziali presentate dall'utente sono verificate mediante un confronto con quelle presente negli archivi Aziendali di InfoCamere.

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

8.2.11. 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 aziendali di InfoCame-

re. 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.

8.2.12. ASSEGNAZIONE E REVOCA DELLE USER-ID ED ABILITAZIONI

InfoCamere gestisce la procedura per l'assegnazione delle user-id che permettono l'accesso ai sistemi, alle banche dati e alla rete del Sistema Informatico Camerale.

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'azienda/CdC, il capo ufficio dell'utente interessato chieda ad InfoCamere 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, i soggetti eventualmente incaricati della custodia delle copie delle credenziali di accesso devono 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.

8.2.13. 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 InfoCamere 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.

8.2.14. 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.

8.2.15. 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.

8.2.16. 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

8.2.17. 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

8.2.18. CERTIFICATI DIGITALI /SMART-CARD

L'accesso alle applicazioni InfoCamere e ai dati può essere consentito anche tramite identificazione dell'utente tramite SmartCard. Il token o 'gettone identificativo della 'sessione utente', associato alla presenza di un certificato valido letto dalla SmartCard, permette l'accesso al pari dell'input di username e password a specifiche applicazioni / dati con criteri di sicurezza maggiori.

8.2.19. PERSONAL IDENTIFICATION NUMBER

I certificati Digitali sono quelli emessi da InfoCamere quale Ente Certificatore e soddisfano a tutti i requisiti di sicurezza successivamente espressi. I dispositivi InfoCamere obbligano l'utilizzatore di Smart Card all'inserimento di un PIN di lunghezza variabile da 5 a 8 caratteri. Il PIN è un codice personale e segreto, gestito e conosciuto esclusivamente dall'utente.

8.2.20. SUPPORTI DI MEMORIZZAZIONE

I supporti rimovibili contenenti dati sensibili e/o giudiziari sono resi distrutti o non riutilizzabili e ne è prescritta la formattazione in caso di riutilizzo.

I trattamenti con strumenti elettronici relativi a dati sensibili e giudiziari effettuati autonomamente dalla Camera sono protetti attraverso appositi software antivirus. Gli accessi alle procedure avviene unicamente da parte degli incaricati, i quali custodiscono le relative password.

Con riferimento alle procedure informatiche gestite da altri soggetti terzi (posta elettronica) si rimanda ai documenti di sicurezza ed alle policy adottate da tali enti.

Vedere in Appendice:

Tabella 4. Le misure di sicurezza adottate e da adottare

9. *Descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati*

Riferimento normativo: ***D.L.vo n. 196/2003 – Allegato "B", Disciplinare tecnico in materia di misure minime di sicurezza. (Regola 19.5)***

Per tutti i trattamenti di dati personali effettuati con strumenti elettronici in cui partecipa il Responsabile InfoCamere sono previste da parte di quest'ultima apposite procedure di salvataggio giornaliero dei dati, nonché procedure di ripristino della loro disponibilità con tecniche di Disaster Recovery.

Per una più approfondita conoscenza delle procedure sopra indicati si rinvia al Documento Programmatico sulla Sicurezza predisposto da InfoCamere, nonché alle procedure ivi descritte e/o richiamate.

Vedere in Appendice:

Tabella 5.1. Criteri per il ripristino della disponibilità dei dati

Tabella 5.2. Criteri per il ripristino della disponibilità dei dati

10. Previsione di interventi formativi degli incaricati del trattamento

Riferimento normativo: ***D.L.vo n. 196/2003 – Allegato "B", Disciplinare tecnico in materia di misure minime di sicurezza. (Regola 19.6)***

Sono stati effettuati interventi formativi generalizzati a tutti i dipendenti della CdC per renderli edotti sui rischi che incombono sui dati, sulle misure disponibili per prevenire eventi dannosi, sui profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, sulle responsabilità che ne derivano, sulle modalità per aggiornarsi sulle misure minime adottate dal titolare.

Sono, altresì, previsti interventi formativi nei confronti di nuovi assunti ovvero in caso delle modalità di trattamento o di trasferimento di mansioni. Detti interventi sono svolti dal capo ufficio dell'incaricato entro 30 gg. dal verificarsi dell'evento che richiede la formazione stabilita.

Inoltre, l'Ente Camerale ha provveduto a distribuire ai dipendenti e collaboratori il "Manuale Operativo Privacy" adottato all'interno dell'Ente medesimo, in cui è contenuta la nomina ad incaricato del trattamento prevista dalla normativa, sono descritti gli accorgimenti e le misure da porre in essere per il trattamento di dati personali, le regole di condotta, nonché la struttura e le relative responsabilità di ogni soggetto coinvolto in detto trattamento.

Vedere in Appendice:

Tabella 6. Pianificazione degli interventi formativi previsti

11. Trattamenti di dati personali affidati all'esterno della struttura del Titolare

Riferimento normativo: ***D.L.vo n. 196/2003 – Allegato "B", Disciplinare tecnico in materia di misure minime di sicurezza. (Regola 19.7)***

I trattamenti informatici affidati all'esterno sono quelli effettuati dal Responsabile InfoCamere nell'ambito dei patti consortili che disciplinano il rapporto tra quest'ultima e la CdC.

Nel paragrafo del presente documento relativo alla struttura del sistema camerale ed alla distribuzione delle responsabilità sono contenute idonee informazioni utili a comprendere l'ambito del trattamento effettuato dal responsabile esterno.

Per gli ulteriori trattamenti affidati all'esterno, evidenziati nella relativa tabella, si è provveduto alla nomina dei soggetti nella qualità di Responsabile del trattamento.

Vedere in Appendice:

Tabella 7. Trattamenti affidati a strutture esterne

12. Cifratura o separazione dei dati personali idonei a rivelare lo stato di salute e la vita sessuale dagli altri dati personali dell'interessato

Riferimento normativo: ***D.L.vo n. 196/2003 – Allegato "B", Disciplinare tecnico in materia di misure minime di sicurezza. (Regola 19.8)***

I trattamenti con strumenti informatici affidati al Responsabile InfoCamere sono svolti applicando tecniche di separazione dei dati sensibili e/o giudiziari dagli altri dati personali degli interessati.

L'architettura dei database realizzati e gestiti da InfoCamere, prevede infatti la separazione in apposite tabelle di tali dati, i quali sono resi disponibili anche agli incaricati solo previa autenticazione e nei limiti del sistema di autorizzazione predisposto.

I database relazionali sono conservati presso la struttura di Padova di InfoCamere.

Con riferimento al trattamento di dati sensibili e/o giudiziari con strumenti non elettronici è prevista la separata conservazione, ove possibile, in armadi chiusi a chiave dei documenti contenenti tali tipologie di dati con quelli contenenti dati di altro genere.

Vedere in Appendice:

Tabella 8. – Cifratura dei dati o separazione dei dati identificativi

13. Individuazione dell'ambito di trattamento consentito agli incaricati

In base alle previsioni di cui agli art. 34, 1° comma, lett. d) e 35, 1° comma, lett. a) del Codice l'ente ha provveduto ad individuare l'ambito di trattamento consentito agli incaricati sia con riferimento ai trattamenti svolti con l'ausilio di strumenti elettronici sia per i trattamenti svolti senza l'ausilio di tali strumenti.

Tale ambito è stato definito per i dipendenti dell'ente camerale nonché per i dipendenti della InfoCamere S.C.p.A., la quale, in forza dei patti consortili, gestisce, in qualità di responsabile del trattamento, gran parte delle procedure informatiche utilizzate in Camera di Commercio.

L'ambito del trattamento è stato definito con particolare riguardo ai permessi di Inserimento, Variazione, Cancellazione o distruzione, Lettura, Stampa o fotocopia dei dati da parte degli incaricati con riferimento alle varie funzioni svolte negli ufficio.

Vedere in Appendice:

Allegato B – Ambito del trattamento consentito agli incaricati