Camera di Commercio
Caserta

ALLEGATO B

Istruzioni ai Responsabili ed Incaricati del trattamento dei dati personali comuni, sensibili e/o giudiziari della Camera di Commercio di Caserta

1. INTRODUZIONE

Le presenti istruzioni costituiscono una serie organica di prescrizioni, orientate a garantire la sicurezza dei dati e delle informazioni detenute dagli uffici e dalle strutture della Camera di Commercio di Caserta. Tali prescrizioni devono intendersi come istruzioni impartite dal titolare del trattamento (la Camera di Commercio di Caserta) ai sensi dell'art. 29, comma 5 del decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali (di seguito anche denominato semplicemente Codice). Lo scopo delle prescrizioni è quello di costituire un supporto minimo all'azione dell'apparato burocratico, evitando i rischi di danneggiamento o dispersione dei dati, in ragione di un trattamento non corretto. In ogni caso, il trattamento dei dati presso gli uffici e le strutture della Camera di Commercio deve avvenire:

- **nel rispetto del principio di riservatezza**;
- **in modo lecito e secondo correttezza**;
- **per un periodo di tempo non superiore a quello necessario agli scopi per i quali i dati sono stati raccolti e, successivamente, trattati**;
- **nel rispetto delle misure minime di sicurezza, custodendo e controllando i dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta**.

Nello specifico, deve intendersi per:

- **Tutela della riservatezza**: l'attivazione di procedure di conoscenza delle informazioni detenute, a qualsiasi titolo, dalla Camera di Commercio, tali da consentire l'accesso solo a soggetti identificati e dotati di un adeguato grado di autorizzazione;
- **Integrità**: l'aggiornamento dei dati e delle informazioni realizzato periodicamente da personale autorizzato;
- **Disponibilità:** l'attivazione di procedure che consentano ai soggetti autorizzati di accedere in tempi utili alle informazioni. Il livello di sicurezza in materia di trattamento dei dati raggiungibile mediante la mera applicazione delle procedure ed il corretto uso dei mezzi tecnici è tuttavia limitata. La sicurezza delle informazioni, per arrivare ad i livelli più elevati, richiede la condivisione degli obiettivi da parte del personale dell'Ente. Esiste infatti una relazione tra la sicurezza e il sistema organizzativo: intanto l'ente può perseguire i suoi obiettivi, in quanto il personale impegnato sia motivato ad incrementare la propria produttività, efficienza, efficacia delle attività, in un sistema di flessibilità e di integrazione.

La prima misura di sicurezza è quindi di carattere organizzativo e coinvolge l'esatta definizione dei ruoli e delle responsabilità. A tal fine la Camera di Commercio di Caserta, quale titolare del trattamento dei dati personali, con la determinazione n.272 adottata in data 13.06.2017, ha riconosciuto al Segretario Generale e ai Dirigenti la qualità di responsabili del trattamento dei dati, ai sensi dell'art.29 del d.lgs. 30 giugno 2003, n.196 (c.d. Codice in materia di trattamento dei dati personali). Le presenti istruzioni intendono quindi corroborare l'azione dirigenziale, lasciando comunque intatta l'autonomia dirigenziale per individuare ulteriori modalità operative che rafforzino la sicurezza dei trattamenti, senza, tuttavia, appesantire l'azione amministrativa, in linea con quanto enunciato nella legge 7 agosto 1990, n.241.

1.1 Riferimenti normativi e alle disposizioni aziendali

In relazione al trattamento dei dati deve garantirsi la puntuale applicazione del *Codice in materia di protezione dei dati personali*, decreto legislativo 30 giugno 2003, n. 196 e relativi allegati, in particolare l'allegato B, recante "Disciplinare tecnico in materia di misure minime di sicurezza".

Nell'elaborazione delle presenti istruzioni si è tenuto conto anche delle pronunce del Garante per la protezione dei dati personali, della Direttiva del Dipartimento della Funzione Pubblica dell'11 febbraio 2005, n.1 , recante misure finalizzate all'attuazione nelle pubbliche amministrazioni delle disposizioni contenute nel decreto legislativo 30 giugno 2003, n. 196 .

1.2 Organizzazione del documento

Il presente documento è suddiviso in quattro parti:
Misure di sicurezza: l'insieme delle misure di carattere tecnologico e di natura procedurale ed organizzativa per

garantire un adeguato livello di sicurezza dei dati e delle informazioni;
Istruzioni per il trattamento dei dati: indicazioni utili per la corretta gestione e custodia degli account di accesso ai sistemi informatici utilizzati per il trattamento dei dati;
Sicurezza del software e dell'hardware: norme per la corretta gestione degli apparati informatici e del software installato su di essi.
Sanzioni per inosservanza delle norme: ambito di applicazione e sanzioni a carico dell'incaricato in caso di violazioni delle istruzioni operative

2. Misure di sicurezza

Per misure di sicurezza deve intendersi l'insieme delle prescrizioni di carattere tecnologico, procedurale ed organizzativo finalizzate all'implementazione di un adeguato livello di sicurezza nel trattamento dei dati.

2.1 Criteri tecnici ed organizzativi per la protezione delle aree e dei locali

I dati e le informazioni di carattere sensibile e/o giudiziario devono essere trattati in aree protette, anche fisicamente, dall'accesso di persone non autorizzate. Sono perciò individuate spazi, dotati di un sistema di controllo all'ingresso e di eventuali sbarramenti di sicurezza. Un livello di protezione più elevato deve attivarsi per gli ambiti di trattamento e/o conservazione dei dati sensibili e giudiziari e ove sono ubicati i server di residenza dei dati e delle informazioni. Le barriere fisiche, ove necessario, devono essere configurate in modo tale da impedire l'accesso alle persone non autorizzate. Quando restano vuote, le aree di sicurezza devono restare chiuse e con strumenti di controllo atti ad impedire accessi abusivi. Il personale in servizio presso l'Ente ha accesso ai locali esclusivamente per l'adempimento della prestazione lavorativa. Il personale che espleta servizi strumentali (es.: pulizia dei locali) o si occupa della manutenzione e dei servizi accessori, deve essere espressamente autorizzato ad accedere alle aree di sicurezza. L'assegnazione degli spazi di lavoro deve avvenire secondo criteri tali da impedire la promiscuità di permanenza e di utilizzazione tra:

- personale incaricato del trattamento di dati personali;
- personale non incaricato di trattamento di dati personali;
- soggetti estranei alla Camera di Commercio di Caserta

Il personale dipendente incaricato di trattamento ha accesso ai dati esclusivamente sulla base delle esigenze di servizio, conformemente ai seguenti principi:

- la necessità di trattamento;
- il minimo livello di conoscenza dei dati.

I Responsabili del trattamento devono vigilare affinché venga disciplinato e controllato l'accesso, il transito e la permanenza di persone estranee all'attività lavorativa nelle aree e nei locali adibiti a luoghi di lavoro, con particolare attenzione agli spazi in cui vengono custodite banche di dati o ove vengono trattati dati sensibili o giudiziari. E' altresì compito del Responsabile vigilare sull'introduzione in tali aree di oggetti, apparecchiature, sostanze o materiali che possono favorire il sorgere di rischi. Devono essere previsti procedure, accorgimenti e strumenti per:

- consentire l'accesso alle aree dove vengono custoditi e trattati i dati al solo personale autorizzato, ivi compresi i locali destinati al personale addetto alla video sorveglianza;
- ostacolare l'accesso abusivo ai dati;
- segnalare la presenza di intrusi;

2.1.1 Archivi cartacei temporanei

La gestione degli archivi cartacei temporanei si ascrive alla competenza del Responsabile del trattamento. Lo stesso individua le tipologie dei documenti contenenti i ***dati sensibili*** – cioè intendendo come tali "*i dati personali idonei a rilevare l'origine raziale 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 rilevare lo stato di salute e la vita sessuale*" - e ***dati giudiziari*** – cioè "*i dati personali idonei a rivelare provvedimenti di cui all'art. 3, comma 1, lettere da a) a o) e da r) a u), del DPR 14.11.2002, n. 313, in materia di casellario giudiziario, 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*" - ed i dipendenti incaricati dei relativi trattamenti. Il Responsabile dovrà assicurare che la documentazione venga custodita in armadi dotati di serratura, le cui chiavi dovranno essere conservate in modo appropriato. I documenti contenenti dati sensibili o giudiziari devono essere conservati secondo modalità che precludano la visione, in occasione della consultazione di documenti di altro genere, mediante creazione di sottofascicoli in busta chiusa, con sottoscrizione dello

stesso Responsabile o di un incaricato. Il Responsabile deve garantire l'integrità dei sottofascicoli in occasione dell'accesso all'archivio da parte di soggetti non legittimati alla consultazione dei dati sensibili o giudiziari.

2.1.2 Archivi cartacei di deposito

L'archivio cartaceo di deposito deve essere controllato in considerazione della circostanza che l'accesso a siffatta documentazione non è pubblico. La consultazione potrà avvenire esclusivamente da parte del personale autorizzato o da parte di estranei autorizzati dal Responsabile. Il Responsabile dell'archivio cartaceo deve annotare su apposito registro gli estremi di ogni consultazione, precisando la data, la struttura richiedente, l'identità del soggetto che procede alla consultazione, l'oggetto della consultazione, le operazioni effettuate. I documenti contenenti dati sensibili o giudiziari devono essere conservati secondo modalità che precludano la visione, in occasione della consultazione di documenti di altro genere, mediante creazione di sottofascicoli in busta chiusa, con sottoscrizione dello stesso Responsabile o di un incaricato. Il Responsabile deve garantire l'integrità dei sottofascicoli in occasione dell'accesso da parte di soggetti non legittimati alla consultazione dei dati sensibili o giudiziari.

2.1.3 Selezione e scarto

La selezione e lo scarto della documentazione deve avvenire nel rispetto delle prescrizioni normative vigenti.

2.1.4 Altre misure per il rispetto dei diritti degli interessati

L'Ente al fine di garantire il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale dovrà:

- predisporre appropriate distanze di cortesia, tenendo conto dell'eventuale uso di apparati vocali o di barriere;
- predisporre soluzioni tali da prevenire, durante colloqui, l'indebita conoscenza da parte di terzi di informazioni idonee a rilevare lo stato di salute;
- predisporre opportuni accorgimenti volti ad assicurare che, ove necessario, possa essere data correttamente notizia o conferma anche telefonica, ai soli terzi legittimati.

3. Istruzioni per il trattamento dei dati

Le operazioni di trattamento possono essere effettuate solo dagli incaricati che operano sotto la diretta autorità del Titolare o del responsabile, nel rispetto delle istruzioni da questi ultimi impartite. Tali operazioni devono essere limitate esclusivamente a quei dati la cui conoscenza sia strettamente necessaria per adempiere ai compiti loto assegnati.

Il trattamento impone di attivare tutte le misure atte a far si che non siano violati i diritti e le libertà fondamentali di ognuno e siano garantiti gli aspetti di riservatezza, di identità personale e di protezione dei dati personali.

Gli incaricati dovranno rispettare le norme di sicurezza per la protezione dei dati personali.
Il Responsabile del trattamento dei dati è tenuto ad effettuare controlli sulle attività degli incaricati del trattamento, al fine di garantire la puntuale applicazione delle disposizioni contenute nel Codice. Ogni Responsabile informa gli incaricati dell'attivazione di sistemi di controlli legati a criteri in parte statistici in parte casuali. I responsabili, preferibilmente, precisano le istruzioni per il corretto trattamento dei dati, in forma scritta. E' sempre ammessa la diffusione di istruzioni in forma orale, in particolare allorquando vi sia l'urgenza di salvaguardare i principi in materia di trattamento dei dati personali. Deve in ogni caso garantirsi l'osservanza delle misure minime di sicurezza, contenute negli artt. 33 – 36 del d.lgs. n. 196 del 2003 e nel relativo allegato B, indifferentemente dalla natura del supporto contenente dati.

L'informativa

Affinché si possa procedere al trattamento di dati personali, è necessario che ai soggetti interessati al trattamento stesso venga resa l'informativa prevista dall'art.13 del d.lgs n.196/2003. Il consenso non è necessario per le attività istituzionali degli enti pubblici. E' invece necessario per raccolta di dati legate ad attività di natura commerciale svolta dagli stessi enti.
Le Pubbliche Amministrazioni possono effettuare un trattamento di dati sensibili e dati giudiziari sulla base di disposizioni specifiche previste dagli artt.20, 21, e 22 del Codice in materia di protezione di dati personali.
Le Pubbliche Amministrazioni non devono richieder il consenso dell'interessato, purché il trattamento sia effettuato nell'ambito dello svolgimento delle proprie funzioni istituzionali.

I modelli previsti ai fini della richiesta di un qualsiasi provvedimento, compreso il modello di dichiarazione sostitutiva, devono contenere l'informativa prevista dall'art.13 del Codice, diretta ad illustrare all'utente, le finalità e le modalità del trattamento dei dati contenuti nella relativa modulistica.
L'informativa ai sensi del citato art.13 deve contenere le seguenti indicazioni:

a) Le finalità e le modalità del trattamento cui sono destinati i dati;
b) la natura obbligatoria o facoltativa del consenso;
c) le conseguenze di un eventuale rifiuto di rispondere;
d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati e l'ambito di diffusione dei medesimi;
e) i diritti di cui all'art.7;
f) gli estremi identificativi del titolare e, se designato, del responsabile del trattamento. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, precisando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili.

L'informativa, adottata di concerto dai dirigenti e Responsabili di Servizio, dovrà essere adottata dai singoli Servizi/Uffici per le finalità sopra richiamate; dovrà altresì essere affissa nei locali dove accedono gli utenti per richiedere i servizi erogati dall'ente.

3.1 Trattamenti senza l'ausilio di strumenti elettronici
Il trattamento di dati senza strumenti elettronici, coinvolge i dati contenuti in tutti i supporti cartacei o simili che, comunque non richiedano l'uso di elaboratori elettronici. Ove esistano copie o riproduzioni di documenti che contengono dati personali, le medesime devono essere protette con le stesse misure di sicurezza applicate agli originali.

3.1.1 Custodia

- I documenti contenenti dati personali – cioè "*qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale*" - devono essere custoditi in modo da non essere accessibili alle persone non incaricate del trattamento, mediante localizzazione presso spazi con accesso riservato (es. armadi o cassetti chiusi a chiave).
- I documenti contenenti dati personali prelevati dagli archivi per l'attività quotidiana, devono essere ivi collocati al termine della giornata.
- I documenti contenenti dati personali non devono rimanere incustoditi su scrivanie o tavoli di lavoro.

3.1.2 Comunicazione
La diffusione dei dati personali deve avvenire in base al principio dello "stretto indispensabile", talché non devono essere condivisi, comunicati o inviati a soggetti o istituzioni che non ne abbiano bisogno per lo svolgimento delle funzioni lavorative, a prescindere dall'eventuale qualifica di responsabili o incaricati di altra struttura. I dati non devono essere comunicati all'esterno della struttura, e comunque a soggetti terzi, se non previa autorizzazione.

3.1.3 Distruzione
Qualora sia necessario distruggere i documenti contenti dati personali, questi devono essere soppressi mediante apparecchi "distruggi documenti" o, in assenza, attraverso modalità che impediscano qualsiasi ricomposizione.

3.1.4 Istruzioni per il trattamento di dati sensibili e/o giudiziari
I trattamenti dei dati sensibili o giudiziari possono essere effettuati solo qualora siano indispensabili per svolgere attività istituzionali.
I documenti contenenti dati sensibili e/o giudiziari devono essere sottoposti al controllo dei Responsabili i quali, a loro volta, potranno avvalersi degli incaricati per la custodia e/o il trattamento. Il Responsabile deve impedire l'accesso a persone prive di autorizzazione nei luoghi e nei momenti in cui si trattano dati sensibili e/o giudiziari. Conseguentemente, il trattamento di dati sensibili e/o giudiziari contenuti in documenti cartacei deve avvenire per il tempo strettamente necessario al trattamento, con successiva immediata archiviazione dei dati.
I relativi documenti dovranno essere custoditi, anche in fase istruttoria, in appositi armadi al fine di garantirne l'accesso solo a persone all'uopo autorizzate. Gli incaricati non dovranno lasciare le pratiche incustodite sul tavolo, né utilizzare cartelline trasparenti per la conservazione di dati sensibili o giudiziari. I Responsabili dei servizi sono incaricati di impartire apposite istruzioni per individuare la collocazione della suddetta documentazione.

L'archiviazione dei documenti cartacei contenenti dati sensibili e/o giudiziari deve avvenire in locali ad accesso controllato, utilizzando armadi o cassetti chiusi a chiave.
Per accedere agli archivi contenenti dati sensibili e/o giudiziari fuori orario di lavoro è necessario ottenere una preventiva autorizzazione da parte del Responsabile oppure procedere all'identificazione su un apposito registro.
Le chiavi degli arredi contenenti i suddetti dati dovranno essere conservate in modo da escludere la loro accessibilità da parte di quegli incaricati che non gestiscono il procedimento nel quale risulti necessaria l'acquisizione del dato.

L'accesso agli archivi contenenti dati sensibili o giudiziari deve essere controllato e, terminato l'orario di lavoro, i dati devono essere custoditi in apposite strutture. Gli archivi contenenti dati sensibili o giudiziari, al termine dell'orario di lavoro, non potranno essere consultati, salvo specifiche autorizzazioni.

3.1.5 Trattamenti con l'ausilio di mezzi elettronici
Per trattare i dati mediante dispositivi informatici, deve seguirsi una procedura di autenticazione che consenta l'identificazione del Responsabile o dell'Incaricato, mediante "credenziali di autenticazione". Le "credenziali di autenticazione" consistono in un user-ID, associato ad una parola chiave segreta password.
Le user-ID e password individuali per l'accesso alle applicazioni non devono essere mai condivise con altri soggetti, anche se incaricati del trattamento. Nel caso in cui occorre permettere l'accesso da parte di altri utenti, è necessario richiedere la generazione di una nuova password.
Per i PC collegati in rete, i Responsabili e gli Incaricati devono superare le procedure di identificazione, quali formalità preliminari per accedere alle risorse presenti nella rete aziendale; nel caso di utilizzo di applicazioni esterne a quelle fornite da InfoCamere, i responsabili e gli incaricati devono provvedere anche alla propria identificazione sul sistema applicativo, secondo le modalità e le regole previste dall'applicativo stesso.

3.2.1 Gestione delle password
La password è assegnata ai Responsabili ed agli Incaricati mediante sistemi meccanici che consentano l'enucleazione di password conformi alle prescrizioni contenute nell'Allegato B del d.lgs. n.196 del 2003 (almeno 8 caratteri). Essa non deve contenere riferimenti a dati personali e deve preferibilmente contenere punti, trattini, minuscole e maiuscole. I Responsabili devono garantire l'esclusività dell'uso della password, in particolare impedendo che incaricati, o altri, si avvalgano di credenziali di autenticazione a qualunque titolo percepite.
Ogni incaricato deve adottare le necessarie cautele per tutelare la segretezza della propria password e custodire diligentemente i propri dispositivi, utilizzandoli esclusivamente nei modi e per le finalità necessarie allo svolgimento ella propria funzione. L'accesso ai sistemi, alle banche dati contenenti informazioni personali o alla rete, deve essere basato sulle effettive necessità di trattamento, tramite user-id riconducibile ad un singolo individui, senza che sia possibile accedere contemporaneamente da due postazioni differenti con il medesimo account. Nessuno deve annotare la propria password su supporti facilmente rintracciabili e, soprattutto, in prossimità della postazione di lavoro utilizzata. Gli applicativi utilizzati, gestiti da InfoCamere, prevedono il cambio della password ogni sei mesi.
I responsabili dei servizi dovranno tempestivamente richiedere la disattivazione delle credenziali di coloro che, per qualsiasi motivo, non siano addetti più alle funzioni per le quali le credenziali erano state assegnate.
Le credenziali di autenticazione non utilizzate da almeno 6 mesi sono disattivate su richiesta dei responsabili dei servizi i quali procederanno a verificare le user-id non attive, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

3.2.2 Custode delle password
In caso di assenza od impedimento dell'incaricato e contestuale esigenza di accedere ai dati detenuti presso banche dati o p.c. in uso all'incaricato, i responsabili devono attivare procedure di accesso temporaneo, mediante generazione di nuove credenziale di autenticazione. Le nuove credenziali di autenticazioni devono essere disattivate al termine della sessione straordinaria di lavoro. Conformemente a quanto previsto nel punto 10 dell'all. "B - Disciplinare tecnico" del Codice, il responsabile deve accertarsi che sia fornita adeguata comunicazione all'incaricato del sopravvenuto accesso al p.c. o alla banca dati da parte di altro incaricato.

3.2.3 Presenza di estranei all'Ente
I Responsabili devono garantire che le attività degli incaricati non vengano espletate alla presenza o secondo modalità che consentano ad estranei, di acquisire dati e/o informazioni detenute dall'Ente. A tal fine i Responsabili devono impartire istruzioni finalizzate ad evitare che personale estraneo o visitatori restino negli spazi ove si trattano dati

personali. In ogni caso, gli incaricati sono tenuti a riporre i documenti contenenti dati personali secondo modalità che ne impediscano la visione a qualunque soggetto non legittimato. In caso di allontanamento dal p.c. si invita l'incaricato ad attivare la procedura di "blocco" p.c., al fine di evitare la visione dei documenti in lavorazione. Lo sblocco può avvenire soltanto con l'inserimento delle proprie credenziali.

3.2.4 Istruzioni per il trattamento di dati sensibili e/o giudiziari

I trattamenti dei dati sensibili o giudiziari possono essere effettuati solo qualora siano indispensabili per svolgere attività istituzionali.

I dati anagrafici devono essere conservati separatamente da quelli sanitari che, invece, se contenuti in elenchi, registri o banche dati devono essere trattati con "tecniche di cifratura o codici identificativi che consentano di identificare gli interessati solo in caso di necessità".

Le smart card dovranno essere parimenti custodite personalmente da ogni responsabile del trattamento, in modo da non risultare accessibili né a terzi né a colleghi.

I dati idonei a rivelare lo stato di salute non possono in alcun modo essere diffusi.

Nella stesura delle determinazioni e delle delibere non devono essere riportati dati sensibili o giudiziari se non nei casi in cui tali riferimenti siano indispensabili ai fini dell'emanazione dell'atto.

Non devono essere utilizzati supporti removibili ai fini della conservazione dei dati sensibili e giudiziari.

I documenti che sono cestinati, qualora contengano anche solo dati personali, devono essere distrutti in modo da non renderli riutilizzabili.

I dati sensibili non potranno in ogni caso essere archiviati otticamente per la diffusione. Pertanto non sono oggetto di archiviazione ottica i documenti inerenti lo stato di salute, i permessi di soggiorno ed i documenti d'identità dove siano riportati particolari stati fisici (ad esempio, patente con riferimento ad handicap o lenti). Dovrà pertanto procedersi all'oscuramento degli stessi rispettivamente con il codice " documento interno" o allegando il cartaceo alla pratica telematica come allegato con visione solo interna. Inoltre, deve essere esclusa l'archiviazione ottica di qualsiasi dato giudiziario (esempio certificati del casellario giudiziale) qualora ciò renda impossibile la distruzione del documento decorso il periodo di tempo necessario alla conservazione del documento.

E' fatto divieto, ai sensi del codice della privacy, di pubblicare e divulgare con qualsiasi mezzo notizie e immagini idonee a consentire l'identificazione di un minore. (es. permessi di soggiorno con foto di minori).

3.2.5 Distruzione dei dati

I supporti magnetici od ottici contenenti dati personali devono essere cancellati prima di essere riutilizzati. Se ciò non è possibile, essi devono essere distrutti secondo modalità che ne impediscano la ricomposizione.

4. Sicurezza del software e dell'hardware

Le norme riportate in questa sezione sono finalizzate ad aumentare la sicurezza dei singoli sistemi informatici utilizzati per il trattamento dei dati. Il rispetto di tali norme garantisce anche che non vengano compromesse le misure di sicurezza del sistema informativo ad opera di un utente regolarmente autorizzato, che, inconsapevolmente, adotti comportamenti in grado di violare l'integrità del sistema (installazione inconsapevole di virus o di "trojan horse"). I Responsabili devono assicurare che gli incaricati non installino sulla postazione di lavoro programmi non attinenti alle attività di ufficio, ovvero programmi senza la preventiva autorizzazione. I Responsabili, qualora non siano in grado di apprezzare l'impatto dei programmi per i quali si è chiesta l'installazione, si coordinano con il referente informatico dell'Ente per concordare la linea di condotta. Gli incaricati non devono modificare le configurazioni hardware e software, senza l'autorizzazione del Responsabile del trattamento, che anche per questo aspetto si coordinerà con il referente informatico. InfoCamere provvederà all'aggiornamento automatico dei software in uso.

4.1 Protezione da virus informatici

I virus informatici rappresentano una delle minacce principali per la sicurezza dei sistemi informativi e dei dati in esso presenti. Un virus informatico, come è noto, può modificare e/o cancellare i dati in esso contenuti, compromettere la sicurezza e la riservatezza di un intero sistema informativo, rendere indisponibile tutto o parte del sistema, compresa la rete di trasmissione dati. In fase di predisposizione della postazione di lavoro viene installato l'antivirus, che viene aggiornato a livello centrale da InfoCamere. Per quanto concerne la posta elettronica, il client utilizzato dalla Camera "Zimbra", cancella automaticamente gli allegati ritenuti sospetti. In ogni caso, al fine di non aumentare il livello di rischio di contaminazione da virus è opportuno che Responsabili ed incaricati provvedano a:

1 accertarsi che sul computer sia sempre operativo il programma antivirus aggiornato e con la funzione di monitoraggio attiva;
2 accertarsi sempre della provenienza dei messaggi di posta elettronica contenenti allegati; nel caso che il mittente dia origine a dubbi, cancellare direttamente il messaggio senza aprire gli allegati
3 non consentire la trasmissione tra computer in rete di file eseguibili e di sistema;
4 non scaricare da Internet programmi o file non inerenti l'attività lavorativa o comunque sospetti.

4.2 Back-up dei dati
Il back-up dei dati viene effettuato centralmente da InfoCamere.

4.3 Utilizzo della rete Internet
Il sistema informativo ed i dati in esso contenuti possono subire gravi danneggiamenti per un utilizzo improprio della connessione alla rete Internet, anche in conseguenza della diffusione di virus informatici o accessi non autorizzati. I Responsabili vigilano che gli incaricati utilizzino la connessione Internet esclusivamente per lo svolgimento dei propri compiti istituzionali, non diffondano messaggi di posta elettronica di provenienza dubbia, non utilizzino la casella postale assegnata per fini privati e personali, non si avvalgano di servizi di comunicazione e condivisione di files (condivisione P2P "peer-to-peer"). Il Responsabile è tenuto a ricordare, a tutto il personale addetto alla propria struttura, il divieto di violare le prescrizioni di cui agli articoli 615 ter –"Accesso abusivo ad un sistema informatico e telematico", 615 quater – "Detenzione e diffusione abusiva di codici di accesso a sistemi informatici e telematica", 615 quinquies – "Diffusione di programmi diretti a danneggiare ed interrompere un sistema informatico" del codice penale, nonché del Decreto Legge 22 Marzo 2004 n. 72, convertito in legge con modificazioni, dalla Legge 21 Maggio 2004 n. 128 (c.d. "Legge Urbani") diretta a sanzionare la condivisione e/o fruizione di file relativi ad un'opera cinematografica, od assimilata, protetta da diritti d'autore.
È pertanto vietato effettuare il download e l'installazione di programmi dalla rete Internet, a meno che non si tratti di software funzionali all'attività lavorativa, e sempre con l'esplicita autorizzazione da parte del Responsabile del trattamento.

5. Sanzioni per inosservanza delle norme
Le presenti istruzioni saranno comunicate ed osservate anche da coloro che, temporaneamente, a qualunque titolo, prestino lavoro o collaborazioni presso la Camera di Commercio di Caserta (personale con contratto di collaborazione, stagisti, borsisti, personale a tempo determinato).
I responsabili dei servizi nonché i responsabili del procedimento sono tenuti a vigilare sul rigoroso rispetto di quanto previsto nel presente provvedimento, nonché ad adottare e/o proporre al responsabile le ulteriori misure necessarie ed opportune per garantire il rispetto della legge.
Le presenti istruzioni integrano elementi di valutazione della condotta del lavoratore. La violazione delle prescrizioni contenute può generare, oltre che responsabilità penali e civili, l'irrogazione di sanzioni disciplinari, in considerazione della gravità della condotta.