Camera di Commercio
Caserta

ALLEGATO B
Ordine di Servizio n.2 del 07.01.2019

Istruzioni operative relative al trattamento dei dati personali della Camera di Commercio di Caserta

Regolamento Europeo 2016/679 (GDPR)
Codice Privacy (d.lgs n.101/2018)

Premessa

Le presenti istruzioni costituiscono una serie organica di prescrizioni, orientate a garantire la sicurezza dei dati e delle informazioni detenute e trattate 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 del *Regolamento Europeo GDPR 2016/679* relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito Regolamento), nonché del *Codice in materia di protezione dei dati personali*, adeguato, per effetto del decreto legislativo n.101 del 10.08.2018, alle nuove disposizioni regolamentari europee, in vigore dalla data del 25 maggio 2018.

Lo scopo di queste prescrizioni è quello di costituire un supporto minimo all'azione dell'apparato burocratico, al fine di garantire la correttezza e conformità a legge dei trattamenti di dati personali posti in essere, evitando i rischi di danneggiamento o dispersione dei dati, in ragione di un trattamento non corretto. Le presenti istruzioni intendono quindi corroborare l'azione dirigenziale, lasciandone comunque intatta l'autonomia per individuare ulteriori modalità operative che rafforzino la sicurezza dei trattamenti, contemperando i principi fondamentali di trasparenza e di accessibilità dell'azione amministrativa con quello di tutela della riservatezza, senza, tuttavia, che questa ne risulti appesantita, in linea con quanto enunciato nella legge 7 agosto 1990, n.241.

In ogni caso, il trattamento dei dati presso gli uffici e le strutture della Camera di Commercio deve avvenire:

- **nel rispetto dei diritti e delle libertà fondamentali delle persone, in particolare del diritto alla protezione dei dati personali**;
- **nel rispetto del principio di liceità e secondo correttezza e trasparenza**;
- **per un periodo di tempo non superiore a quello necessario rispetto agli scopi per i quali i dati sono stati raccolti e, successivamente, trattati**;
- **nel rispetto di adeguate misure 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 presidenziale n.6, adottata in data 28.08.2018, ha riconosciuto al Segretario Generale la qualità di Responsabile del trattamento dei dati personali, ai sensi dell'art.28 del Regolamento UE. Il Segretario Generale, atteso il livello di complessità della struttura e tenuto conto della numerosità ed eterogeneità dei procedimenti di cui è titolare la Camera di commercio di Caserta, ha proceduto, a sua volta, alla designazione, quali ulteriori Responsabili del trattamento, ciascuno per l'area e le materie di relativa pertinenza, dei Dirigenti dell'ente.

Sono, inoltre, stati nominati, quali responsabili esterni del trattamento di dati personali della Camera di commercio:

Infocamere s.c.p.a., , società consortile delle camere di Commercio, quale responsabile esterno per tutto quanto attiene ai trattamenti di dati personali effettuati con l'ausilio di strumenti informatici ed all'archiviazione dei documenti cartacei in banche date centralizzate.

ASIPS – Azienda Speciale della Camera di Commercio di Caserta relativamente alle attività ad essa affidate, sulla base di specifica convenzione;

IC Outsourcing s.c.r.l. - Azienda del sistema camerale per attività, oggetto di specifica convenzione, svolte per conto della Camera di Commercio di Caserta

Da segnalare, infine, che, con provvedimento presidenziale n.2 del 22.05.2018, ratificato dalla Giunta camerale con delibera n.30/GC del 28.05.2018, la Camera di Commercio di Caserta ha proceduto alla nomina del Responsabile della protezione dei dati personali di cui all'art.37 e seguenti, del Regolamento UE.

MISURE DI SICUREZZA

Adempimenti degli incaricati – Principi generali

In applicazione del principio di *accountability,* il titolare del trattamento deve mettere in atto tutte le misure tecniche ed organizzative adeguate per garantire e documentare la conformità del trattamento al Regolamento e alle vigenti disposizioni in materia di tutela dei dati personali. Per misure di sicurezza deve, quindi, intendersi il complesso delle prescrizioni di carattere tecnologico, procedurale ed organizzativo finalizzate all'implementazione di un adeguato livello di sicurezza nel trattamento dei dati, in termini di disponibilità, integrità ed autenticità delle informazioni.
Tali misure devono essere distinte in relazione alla tipologia di dati trattati nonché allo strumento o supporto utilizzato dai soggetti autorizzati nelle diverse operazioni di trattamento di dati personali
In via generale, ciascun incaricato del trattamento deve:

- rispettare i principi generali del Regolamento (Ue) 2016/679 (GDPR), con particolare riferimento alla liceità e correttezza del proprio agire, all'obbligo di procedere alla raccolta e alla registrazione dei dati per scopi determinati, espliciti e legittimi;
- rendere l'informativa agli interessati in sede di raccolta dei dati;
- rispettare l'obbligo di riservatezza e segretezza e conseguentemente il divieto di comunicazione e diffusione dei dati trattati nel corso dell'incarico svolto;
- utilizzare i dati, cui abbia accesso, solamente per finalità compatibili all'esecuzione delle proprie mansioni o dei compiti affidati, per cui è autorizzato ad accedere alle informazioni e ad utilizzare gli strumenti aziendali;
- rispettare le misure di sicurezza idonee adottate dalla società, atte a salvaguardare la riservatezza e l'integrità dei dati;
- segnalare eventuali malfunzionamenti di strumenti elettronici, perdite di dati o esigenze (sia di natura organizzativa, sia tecnica), che possano migliorare lo svolgimento delle operazioni affidate;
- accedere ai dati strettamente necessari all'esercizio delle proprie funzioni e competenze;
- in caso di interruzione del lavoro, anche temporanea, verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- mantenere riservate le proprie credenziali di autenticazione;
- svolgere le attività previste dai trattamenti secondo le direttive del responsabile del trattamento dei dati; non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento dei dati;
- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- informare il responsabile in caso di incidente di sicurezza che coinvolga dati particolari e non;
- raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli di studio e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;
- eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge.

Trattamento di dati personali tramite utilizzo di strumenti informatici - Istruzioni

Come principio generale, sia i dispositivi di memorizzazione del proprio PC sia le unità di rete, devono contenere informazioni strettamente professionali e funzionali alle attività lavorative alle quali si è preposti e non possono essere utilizzate per scopi diversi (immagini, video e documenti personali). L'accesso ai dati non può avere luogo da parte di soggetti estranei all'organizzazione o non specificamente autorizzati.
Di seguito sono riportate le indicazioni per la gestione dei diversi strumenti informatici per il trattamento dati:
Gestione strumenti elettronici (pc fissi e portatili)
Ciascun incaricato è responsabile del corretto utilizzo e della custodia degli strumenti elettronici in dotazione (a titolo esemplificativo personal computer, periferiche, lettori di smart card). Si devono adottare le misure di sicurezza per la tutela della riservatezza, consistenti nell'evitare che l'accesso ai dati possa avvenire da parte di soggetti estranei

all'organizzazione o non specificamente autorizzati. Al fine di verificare il corretto utilizzo degli strumenti in dotazione potranno essere svolti controlli a campione mediante la raccolta e l'analisi di dati aggregati e anonimi. Inoltre, nel caso di provato o constatato uso illecito o non consentito degli strumenti elettronici, risultante dalla verifica delle informazioni in modalità aggregata e anonima, può essere necessario procedere alla verifica delle registrazioni delle sessioni di lavoro, al fine di sanzionare condotte illecite, anche su richiesta dell'autorità giudiziaria, cui le informazioni potranno essere comunicate, senza alcuna ulteriore informativa all'interessato.
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.
Per la gestione della sessione di lavoro sul pc (fisso e portatile), è necessario che:

• al termine delle ore di servizio, il PC deve essere spento, a meno che non stia svolgendo elaborazioni particolari. In tal caso gli uffici debbono tassativamente essere chiusi a chiave;

• Se l'incaricato si assenta momentaneamente dalla propria postazione deve accertarsi che l'eventuale sessione di lavoro aperta non sia accessibile da altre persone. Pertanto deve chiudere la sessione di lavoro sul PC facendo Logout, oppure attivare la procedura di blocco, protetto dalle credenziali di autenticazione;
• Relativamente all'utilizzo dello screen-saver, occorre osservare le seguenti norme:
  - Non deve mai essere disattivato;
  - Il suo avvio automatico deve essere previsto non oltre i primi 10 minuti di inattività del PC
• Quando si esegue la stampa di un documento contenente dati personali, in particolare su una stampante condivisa, occorre ritirare tempestivamente i documenti stampati per evitare l'accesso a soggetti non abilitati al trattamento.
Per l'utilizzo dei PC portatili valgono le regole elencate per i PC connessi alla rete, con le seguenti ulteriori raccomandazioni:
• prima della riconsegna, rimuovere eventuali file ivi elaborati;
• quando il PC portatile è nei locali dell'Ente, non lasciarlo mai incustodito; in caso di brevi assenze assicurarlo alla scrivania o ad elementi "sicuri" dell'arredamento (maniglie, intelaiature…) utilizzando gli appositi cavi in acciaio dotati di lucchetto;
• quando il PC portatile è all'esterno dell'Ente, evitare di lasciarlo incustodito;
• per assenze prolungate, anche qualora l'ambiente venga ritenuto "affidabile", è necessario custodire il portatile in modo opportuno es. cassaforte;
• in caso di furto di un portatile è necessario avvertire tempestivamente il responsabile del Servizio Informatico, onde prevenire possibili intrusioni ai sistemi aziendali;
• in caso di viaggio aereo trasportare tassativamente il portatile come bagaglio a mano;
• eseguire periodicamente salvataggi dei dati e non tenere tali backup insieme al PC portatile.

Il dipendente ha divieto di utilizzare il cellulare o altri dispositivi personali sulla rete camerale per non mettere a rischio gli strumenti informatici dell'ente, al fine di garantire la massima sicurezza del sistema.
L'incaricato ha obbligo di segnalare al referente informatico qualsiasi episodio anomalo, anche occasionale, che si verifichi al proprio pc.
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.

Gestione username e password
L'accesso al PC, sia esso collegato in rete o meno, è protetto da un sistema di autenticazione che richiede all'Incaricato di inserire sulla videata di accesso all'elaboratore un codice utente (username), associato ad una parola chiave (password). L'adozione ed il corretto utilizzo della combinazione username / password è fondamentale per il corretto utilizzo del PC, in quanto:
• tutela l'utilizzatore ed in generale l'Ente da accessi illeciti, atti di vandalismo e, in generale, violazioni e danneggiamenti del proprio patrimonio informativo;
• tutela l'Incaricato da false imputazioni, garantendo che nessuno possa operare a suo nome e che, con il suo profilo (ossia con le sue user id e password) solo lui possa svolgere determinate azioni;
• è necessario per gestire correttamente gli accessi a risorse condivise.

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. Non è consentito 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 delle unità organizzative sono tenuti ad effettuare una verifica periodica delle abilitazioni ai diversi servizi informatici in uso dai propri collaboratori. In particolare, essi dovranno comunicare al referente informatico dell'ente le abilitazioni occorrenti al personale di nuova assegnazione, chiedendo, la disattivazione delle credenziali di coloro che, per qualsiasi motivo, non siano addetti più alle funzioni per le quali le credenziali erano state assegnate.
Tali abilitazioni saranno dismesse entro un mese dalla comunicazione .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.

Ciascun incaricato deve scegliere le password in base ai seguenti criteri:

- devono essere lunghe almeno otto caratteri;
- non devono fare riferimento ad informazioni agevolmente riconducibili ai soggetti utilizzatori o ai loro congiunti;
- devono contenere una combinazione di numeri e/o segni speciali, lettere, maiuscole e minuscole;
- non deve essere uguali alle precedenti.

Per la corretta gestione della password è necessario:

- Ogni password ricevuta va modificata al primo utilizzo;
- La password venga conservata in un luogo sicuro;
- Non rivelare o condividere la password con i colleghi di lavoro, famigliari e amici, soprattutto attraverso il telefono;
- Non memorizzare la password sulle diverse applicazioni né lasciarle scritte su etichette accessibili a tutti;
- Non utilizzare la password d'ufficio per applicazioni informatiche personali e cambiarle periodicamente, ed al massimo ogni sei mesi, qualora non sia automaticamente previsto dal sistema, il cambio password periodico;
- Non utilizzare la funzione, offerta da alcuni software, di salvare automaticamente la password per successivi utilizzi delle applicazioni.

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, il referente informatico, su richiesta del responsabile dell'unità organizzativa, deve 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. 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.

Installazione di hardware e software
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"). L'installazione di hardware e software, nonché la modifica dei parametri di configurazione, possono essere eseguiti solamente dalle persone del Servizio Informatico su autorizzazione del Responsabile del trattamento. 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. Pertanto si raccomanda agli utenti dei PC di rispettare i seguenti divieti:
Non utilizzare sul PC dispositivi personali, o comunque non aziendali, quali lettori dispositivi di memorizzazione dei dati;
Non installare sistemi per connessione esterne (es : modem, wifi); tali connessioni, aggirando i sistemi preposti alla sicurezza della rete aziendale, aumentano sensibilmente i rischi di intrusioni e di attacchi dall'esterno;
non utilizzare il cellulare o altri dispositivi personali sulla rete camerale per non mettere a rischio gli strumenti di lavoro informatici dell'ente, al fine di garantire la massima sicurezza del sistema;
Non installare programmi, anche in versione demo. In particolare, è vietata l'installazione di giochi, programmi in prova (shareware), programmi gratuiti (freeware), programmi pirata, e in generale tutti i software non autorizzati dal Servizio Informatico;
Non modificare i parametri di configurazione del proprio PC senza espressa autorizzazione del responsabile dell'unità

organizzativa, che anche per questo aspetto si coordinerà con il referente informatico, sentito il responsabile del trattamento. InfoCamere provvederà all'aggiornamento automatico dei software in uso.
La condivisione di aree e di risorse del proprio PC viene effettuata dal referente informatico, su richiesta del responsabile dell'unità organizzativa. In questi casi devono essere adottate password di lettura e scrittura e la condivisione deve operare solo su singole directory del PC, e non sull'intero disco rigido.

Gestione posta elettronica aziendale
Il servizio di posta elettronica viene fornito per permettere la comunicazione con soggetti terzi interni ed esterni per le finalità dell'Ente e in stretta connessione con l'effettiva attività e mansioni del dipendente che utilizza tale funzionalità.
Al fine di non compromettere la sicurezza dell'Ente e di prevenire conseguenze legali a carico della stessa, bisogna adottare le seguenti norme comportamentali:

- Se si ricevono mail da destinatari sconosciuti contenenti file di qualsiasi tipo, procedere alla loro immediata eliminazione;
- È fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list, salvo diversa ed esplicita autorizzazione;
- La casella di posta elettronica assegnata deve essere mantenuta in ordine, cancellando i documenti inutili;
- quando si riceve un link di collegamento, non cliccare sul link ma riscriverlo sulla barra dell'indirizzo oppure scriverlo sul motore di ricerca. Ciò al fine di evitare che tale link possa consentir il collegamento ad una piattaforma indesiderata o illecita.

Nell'ipotesi in cui la email debba essere utilizzata per la trasmissione di dati particolari (ex dati sensibili), si raccomanda di prestare attenzione a che:

- l'indirizzo del destinatario sia stato correttamente digitato,
- l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile;
- nel corpo del messaggio sia presente un'intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio;

Gestione del salvataggio dei dati

.

• Per i dati ed i documenti che risiedono sui server gestiti centralmente, come ad esempio cartelle di rete e database, il back-up dei dati viene effettuato centralmente da InfoCamere (il Servizio Informatico) con la possibilità di ripristinare in toto oppure selettivamente eventuali files distrutti, ad esempio per guasti hardware oppure per cancellazioni involontarie.
• Per i dati ed i documenti che risiedono esclusivamente sul PC, ogni Incaricato deve effettuare periodicamente il back up dei dati registrati sul proprio PC sulle apposite cartelle collocate nell'area utenti del server. Questo allo scopo di garantire la disponibilità ed il ripristino dei Dati Personali nel caso di una generica compromissione delle risorse (cancellazioni accidentali, guasti, furti…) e per evitare rischi che soggetti terzi possano crittografare i dati e farne uso illecito.
• Per quanto concerne, in particolare, la posta elettronica, in considerazione della circostanza che il nuovo client di posta elettronica in uso presso l'ente è Gmail, l'incaricato può effettuare le operazioni di salvataggio dei dati, utilizzando le app messe a disposizione da Google (ad. esempio Drive).

Gestione dei supporti rimovibili
I supporti rimovibili, come ad esempio dischi magnetici esterni, penne USB o CD riscrivibili, il cui utilizzo è sempre meno frequente, quando contengono dati personali devono essere custoditi in luogo protetto e non accessibile (cassaforte, armadio chiuso a chiave, etc.). Quando non sono più utilizzati devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri Incaricati non autorizzati al trattamento degli stessi dati, soltanto dopo essere stati formattati. Tali operazioni vengono effettuate a cura del Referente informatico. Il trasferimento di file contenenti dati personali, dati particolari (ex dati sensibili) e giudiziari su supporti rimovibili, è da eseguire unicamente in via transitoria, ponendo la massima attenzione alla destinazione di trasferimento e cancellando i file appena possibile. I dati particolari (ex dati sensibili)/giudiziari devono essere crittografati.

Gestione protezione dai 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. Per prevenire eventuali danneggiamenti al software causati dalla presenza o dall'azione di programmi virus informatici, In fase di predisposizione della postazione di lavoro viene installato l'antivirus, che viene

aggiornato a livello centrale da InfoCamere.
L'antivirus aziendale non deve mai essere disattivato o sostituito con altro antivirus non ufficialmente fornito.
Nel caso il programma antivirus installato sul proprio PC riscontri la presenza di un virus, oppure si sospetti la presenza di un virus non rilevato dal programma antivirus è necessario darne immediatamente segnalazione al Referente informatico.

Si raccomanda di non scaricare e né tantomeno aprire file provenienti via e-mail da mittenti sconosciuti. Tali file, possono essere portatori di virus e compromettere la funzionalità del PC, l'integrità dei dati in essa contenuti e soprattutto l'integrità dei sistemi collegati al PC stesso.
Per quanto concerne la posta elettronica, il client utilizzato dalla Camera "GMail", 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 scaricare da Internet programmi o file non inerenti l'attività lavorativa o comunque sospetti.

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.

Trattamento di dati personali tramite utilizzo di strumenti non elettronici - Istruzioni

Per "non elettronici" si intendono sia documenti cartacei sia documenti di altro tipo come ad esempio microfilm, microfiches e lucidi. I documenti di questo tipo contenenti dati particolari (ex dati sensibili) o dati di natura giudiziaria devono essere protetti in appositi armadi dotati di chiavi. Tutti i documenti contenenti dati particolari (ex dati sensibili) o giudiziari che si ritiene debbano essere eliminati devono essere distrutti e non gettati nei cestini.
Per proteggere i dati personali è opportuno evitare il deposito di documenti di qualsiasi genere negli ambienti di transito o pubblici (corridoi o sale riunioni), come pure l'abbandono in vista sulle scrivanie quando ci si debba assentare dal proprio posto di lavoro. Nel ipotesi si tratti di dati particolari (ex dati sensibili) e/o di dati di carattere giudiziario, il rispetto di queste norme è obbligatorio.

Distruzione delle copie cartacee
Coloro che sono preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) ovvero che utilizzando strumenti per la riproduzione cartacea di documenti digitali, sono tenuti a procedere alla relativa distruzione del supporto, qualora si verifichino errori o la riproduzione non sia corretta, evitando di riutilizzare i fogli, salva l'ipotesi di uso esclusivamente personale per eventuali appunti o brutte copie, da distruggere immediatamente quando non più necessarie;

Misure di sicurezza
Il trattamento sicuro di documenti contenenti Dati Personali richiede la presenza di misure di sicurezza con le quali l'Incaricato possa interagire ed una serie di accorgimenti direttamente gestibili dall'Incaricato stesso. In particolare, si richiede:
• la presenza e l'uso tassativo di armadi e cassetti dotati di serratura adeguata;

• la presenza e l'uso tassativo, ove si richieda la distruzione di documenti contenenti dati particolari (ex dati sensibili) e giudiziari, di un tritadocumenti.

Prescrizioni per gli incaricati

L'Incaricato deve attenersi alle seguenti prescrizioni:

• in nessun caso è concesso l'accesso a documentazione contenente Dati Personali per motivi non dettati da esigenze di lavoro strettamente connesse ai trattamenti dichiarati, autorizzati e tutelati dal Titolare;

• la documentazione contenente Dati Personali che, per ragioni di praticità operativa, risiede sulle scrivanie degli Incaricati, deve comunque essere rimossa al termine dell'orario di lavoro;

• l'accesso ai supporti deve essere limitato al tempo necessario a svolgere i Trattamenti previsti;

• i supporti devono essere archiviati in ambiente ad accesso controllato;

• i documenti contenenti dati personali, non devono essere lasciati incustoditi in un ambiente non controllato (ad es. a seguito della stampa dei documenti su stampante di rete);

• il numero di copie di documenti contenenti Dati Personali deve essere strettamente funzionale alle esigenze di lavoro;

• cassetti ed armadi contenenti documentazione riservata debbono tassativamente essere chiusi a chiave fuori dell'orario di lavoro;

• l'accesso fuori orario lavorativo a documenti contenti Dati particolari (ex dati sensibili) /giudiziari può avvenire da parte di personale Incaricato, o tramite autorizzazione di quest'ultimo, unicamente previa registrazione dell'accesso a tali documenti;

• la distruzione di documenti contenenti Dati Personali deve essere operata, ove possibile, direttamente dal personale Incaricato;

• ove non siano disponibili strumenti per la distruzione dei documenti (trita documenti), o il volume di questi sia tale da imporre il ricorso al servizio di macero, il personale Incaricato che avvia al macero la documentazione è tenuto a confezionare tale documentazione in modo che il pacco risulti anonimo e solido;

• quando gli atti e i documenti contenenti dati personali, dati particolari (ex dati sensibili) o giudiziari sono affidati agli Incaricati per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli Incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate;

• l'accesso agli archivi contenenti dati particolari (ex dati sensibili) o giudiziari deve essere controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate.

• è severamente vietato utilizzare documenti contenenti Dati personali, dati particolari (ex dati sensibili) o giudiziari come carta da riciclo o da appunti.

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

I dati e le informazioni di carattere "particolare" (*dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose, filosofiche, dati genetici, dati relativi alla salute e alla vita sessuale*) e quelli di natura giudiziaria *(dati relativi a condanne penali e reati e alle connesse misure di sicurezza*) devono essere trattati in aree protette, anche fisicamente, dall'accesso di persone non autorizzate. Sono perciò individuati 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 particolari 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;

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 particolari*** – intendendo come tali "*i dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose, filosofiche o l'appartenenza sindacale, nonché dati genetici, dati biometrici intesi ad identificare in modo univoco una persona, dati relativi alla salute e alla vita sessuale o all'orientamento sessuale della persona, art.9 del regolamento UE* " - e ***dati giudiziari*** – cioè "*i dati personali relative a condanne penale e a reati o a connesse misure di sicurezza, secondo l'art.10 del regolamento, secondo le modalità ed i principi al riguardo fissati dall'art.2 –octies del codice privacy (introdotto dal decreto n.101/2018)*" - 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 ne 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 particolari o giudiziari.

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 particolari 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 particolari o giudiziari.

Selezione e scarto

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

Altre misure per il rispetto dei diritti degli interessati

Al fine di garantire il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, il personale 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.

Addetti alla manutenzione

Le seguenti istruzioni devono essere osservate dai preposti in qualità di addetti alla gestione o manutenzione che trattano dati di titolarità per i quali è nominato un responsabile del trattamento nonché dagli addetti di ditte specializzate che svolgano interventi tecnici di gestione e manutenzione degli strumenti elettronici.
L'accesso degli addetti alla gestione e manutenzione è consentito unicamente ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere alle operazioni di manutenzione dei programmi o del sistema informatico.

A ciascun addetto alla manutenzione, previa sottoscrizione di apposito atto per accettazione, è pertanto consentito eseguire le operazioni strettamente necessarie a tali scopi e/o richieste dal titolare, secondo le istruzioni operative da questi fornite, nel rispetto delle disposizioni vigenti in materia. In particolare:

• Nel caso in cui sia necessario effettuare stampe di prova per controllare il funzionamento di stampanti o per verificare il funzionamento di strumenti o programmi installati, non utilizzare files già esistenti ma creare files di prova.

• Nel caso si renda strettamente necessario accedere a files contenenti dati (ad esempio per il recupero di un testo) limitare l'accesso ai dati per il tempo strettamente necessario all'assolvimento delle operazioni di manutenzione.

• Devono essere adottate le prescrizioni misure di sicurezza minime previste dalla vigente normativa in materia di protezione dei dati personali;

• E' necessario informare al più presto il titolare o il responsabile del trattamento qualora si dovessero riscontrare malfunzionamenti o non conformità.

• Tutti i dati personali contenuti nei data base devono essere protetti da password;

Nel caso in cui sia necessario accedere ai dati attraverso gli strumenti elettronici in dotazione agli incaricati, attenersi alle seguenti indicazioni:

- in presenza dell'incaricato, far digitare la password dall'incaricato stesso evitando di venirne a conoscenza;
- in assenza dell'incaricato rivolgersi alla persona individuata dall'incaricato quale proprio fiduciario il quale provvederà all'inserimento della password.

Nei casi in cui sia necessario accedere ai dati personali attraverso il server, rivolgersi all'Amministratore di sistema o provvedere, in collaborazione con l'amministratore di sistema stesso, alla creazione di credenziali di autenticazione da utilizzarsi esclusivamente per l'accesso da parte degli addetti alla manutenzione/gestione dei sistemi informatici;

L'amministratore di sistema ha facoltà, in qualunque momento di controllare e verificare l'operato degli addetti alla manutenzione;

Qualora si renda necessario prelevare apparecchiature elettroniche per effettuare attività di ripristino o interventi di manutenzione che comportino il reset di password precedentemente individuate, la nuova password di accesso sarà comunicata all'incaricato il quale provvederà a cambiarla al termine delle operazioni di manutenzione;

L'accesso al sistema informatico da parte degli addetti alla manutenzione/gestione del sistema è consentito unicamente previo inserimento di password e ID;

E' assolutamente vietato comunicare o diffondere i dati personali di qualsiasi natura provenienti dai database gestiti dalla società, se non previa espressa comunicazione scritta;

Nel caso in cui ci si avvalga di soggetti esterni per interventi specialistici che comportino trattamento di dati personali deve essere rilasciata una dichiarazione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni in materia di misure minime di sicurezza

Sanzioni per l'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 delle unità organizzative nonché i responsabili del procedimento sono tenuti a vigilare sul loro rigoroso rispetto. La violazione delle presenti prescrizioni può costituire fonte di responsabilità disciplinare, oltre, eventualmente, a quella di natura civile e penale.

Caserta, 07 gennaio 2019

IL RESPONSABILE DEL TRATTAMENTO DI DATI PERSONALI

dr. Luca Perozzi