CAMERA DI COMMERCIO
BERGAMO

Disciplinare per l'utilizzo degli strumenti informatici, della rete informatica, telematica (internet e posta elettronica) e di telefonia e per il trattamento dei dati derivanti dal loro utilizzo

CAMERA DI COMMERCIO
BERGAMO

Indice

PREMESSA

La Camera di commercio di Bergamo (di seguito “Camera” o “Ente”) utilizza le moderne tecnologie nell'ambito dello svolgimento dell'attività lavorativa, al fine di perseguire con maggior efficacia, efficienza ed economicità le proprie finalità istituzionali, in un'ottica di semplificazione dell'attività amministrativa.

A tal fine la Camera mette a disposizione dei lavoratori un'idonea strumentazione informatica, favorisce l'utilizzo della Rete Informatica e Telematica, con particolare riferimento all'uso di internet, della posta elettronica e del Sistema di telefonia fissa e mobile e ne promuove un utilizzo corretto attraverso l'adozione del presente Disciplinare.

PRINCIPI E CONTESTO NORMATIVO

Le diverse esigenze che emergono nella redazione delle regole a presidio delle nuove tecnologie sono contrastanti. Se da un lato infatti tali tecnologie consentono un accesso quanto più rapido ed efficace alle informazioni – garantendo in tal modo una certa trasparenza nell’operato – esse rischiano, al contempo, di ledere il principio della riservatezza delle relazioni personali e professionali (Deliberazione del Garante, 01 marzo 2007, n. 13, punto 1.1: *“d) l’utilizzo di Internet da parte dei lavoratori può infatti formare oggetto di analisi, profilazione e integrale ricostruzione mediante elaborazione di log file della navigazione da web […] I servizi di posta elettronica sono parimenti suscettibili di controlli che possono giungere fino alla conoscenza da parte del datore di lavoro del contenuto della corrispondenza”).* Per questi motivi, è necessario che tali esigenze siano bilanciate secondo i canoni stabiliti da principi cogenti. Nella disciplina in esame, il Garante per la protezione dei dati personali ha enucleato tre principi guida fondamentali:

1. il principio di necessità, secondo cui i sistemi informativi e i programmi informatici devono essere articolati nel senso di ridurre al minimo l’utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite;
2. il principio di correttezza, in base al quale i lavoratori devono essere messi a conoscenza delle caratteristiche fondamentali del trattamento;
3. il principio di pertinenza e non eccedenza, in virtù del quale:
   - i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime;
   - il datore di lavoro deve trattare i dati nella misura meno invasiva possibile, rispetto alle finalità perseguite.

Ai sensi del Regolamento UE 2016/679 e della vigente normativa nazionale in materia di protezione dei dati personali, i dati possono essere classificati come segue:
a) dati personali “comuni”: dato personale comune è da intendersi qualunque informazione relativa alla persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale. Ad esempio i **dati che permettono l'identificazione diretta** - come i dati anagrafici: nome e cognome, le immagini, ecc. - e i **dati che permettono l'identificazione indiretta**, come un numero di identificazione: il codice fiscale, l'indirizzo IP, il numero di targa.
b) dati particolari ex articolo 9 GDPR: dati personali idonei a rivelare l’origine razziale ed etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l’appartenenza sindacale, nonché i dati genetici, biometrici intesi ad identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all’orientamento sessuale della persona.
c) dati particolari ex articolo 10 GDPR (cd dati giudiziari): dati giudiziari sono quei dati relativi alle condanne penali ai reati o a connesse misure di sicurezza.

Secondo la suddetta normativa in materia di protezione dei dati personali, si comunica a tutto il personale dipendente che per trattamento dei dati si intende “qualsiasi operazione o insieme di operazioni, compiute con o senza l’ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l’organizzazione, la strutturazione, la conservazione, l’adattamento o la modifica, l’estrazione, la consultazione, l’uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l’interconnessione, la limitazione, la cancellazione o la distruzione”. In tale ottica è indifferente che le operazioni vengano svolte con o senza l’ausilio di mezzi elettronici, o comunque automatizzati, per cui anche i trattamenti effettuati su supporto cartaceo devono intendersi assoggettati alla normativa privacy.

Pertanto, le operazioni di trattamento si possono idealmente suddividere in tre macro tipologie, in funzione del fatto che il loro fine sia:

a) Il reperimento delle informazioni.

Tale fase è tecnicamente definita raccolta di dati, ovvero l'acquisizione delle informazioni, in qualunque modo essa avvenga: ad esempio, direttamente dalla persona interessata, presso terzi, o mediante consultazione di elenchi.

b) Il trattamento "interno" delle informazioni.

Si raggruppano in tale macro-tipologia le varie operazioni, poste in essere da chi raccoglie informazioni per organizzarle e renderle agevolmente usufruibili. Esse sono:

- la registrazione dei dati, cioè il loro inserimento in supporti, automatizzati o manuali, al fine di rendere i dati disponibili per i successivi trattamenti;
- la organizzazione dei dati in senso stretto, cioè il processo di lavorazione che ne favorisca la fruibilità attraverso l'aggregazione o la disaggregazione, l'accorpamento, la catalogazione eccetera;
- la elaborazione, ovvero le operazioni che attribuiscono significatività ai dati in relazione allo scopo per il quale essi sono stati raccolti;
- la selezione, la estrazione ed il raffronto, specifiche che rientrano nella ipotesi più generale della elaborazione;
- la modificazione dei dati registrati, in relazione a variazioni o a nuove acquisizioni;
- la interconnessione, ovvero la messa in relazione di banche dati diverse e distinte tra loro al fine di compiere ulteriori processi di elaborazione, selezione, estrazione o raffronto;
- il blocco, ovvero la conservazione dei dati con sospensione temporanea dei trattamenti;
- la conservazione dei dati, alla quale la legge dedica particolari attenzioni sotto il profilo della sicurezza;
- la cancellazione o la distruzione dei dati, anch'esse operazioni il cui compimento fa sorgere l'obbligo di effettuare taluni adempimenti.

c) L'uso delle informazioni nei rapporti con l'esterno.

Alle operazioni di utilizzo dei dati personali la legge dedica le maggiori attenzioni, in quanto sono potenzialmente più lesive della privacy; sono quelle operazioni, infatti, attraverso le quali si mettono a disposizione di terzi i dati personali. Esse sono:

- **la comunicazione,** cioè il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- **la diffusione**, cioè il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Sezione I
DISPOSIZIONI GENERALI

Art. 1
FINALITA'

1. Il presente Disciplinare è diretto a:
   a) porre in essere, unitamente al Piano Generale in materia di misure di sicurezza dell'Ente, ogni opportuna misura organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri degli strumenti informatici, della Rete Informatica e Telematica e del Sistema di telefonia fissa e mobile, nel rispetto dei diritti dei lavoratori e del diritto alla riservatezza;
   b) informare coloro che utilizzano per lavoro gli strumenti informatici, la Rete Informatica e Telematica e il Sistema di telefonia messi a disposizione dalla Camera delle misure adottate e che si intendono adottare al fine di:
      - garantire il diritto alla riservatezza degli utenti interni ed esterni della Rete Informatica, Telematica e di Telefonia;
      - assicurare la funzionalità ed il corretto impiego delle strumentazioni informatiche e telematiche da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa;

- prevenire rischi alla sicurezza del sistema;
- responsabilizzare gli utilizzatori sulle conseguenze di un uso improprio delle strumentazioni;
- definire in maniera trasparente le modalità di effettuazione dei controlli e le conseguenze, anche disciplinari, di un utilizzo indebito.

Art. 2
PRINCIPI GENERALI

1. La Camera promuove il corretto utilizzo degli strumenti informatici, della Rete Informatica e Telematica, con particolare riferimento all'uso di internet, alla posta elettronica, e del Sistema di telefonia quali strumenti utili a perseguire con efficacia, efficienza ed economicità le proprie finalità istituzionali, in un'ottica di semplificazione dell'attività amministrativa, nel rispetto dei principi e delle linee guida delineati dalla normativa vigente.

2. La titolarità dei beni e degli strumenti informatici, telematici e di telefonia è in capo all'Ente. Tali strumenti sono messi a disposizione del personale, degli addetti che operano in outsourcing e per coloro che per lo svolgimento dell'attività lavorativa in ambito camerale ne facciano espressa richiesta. La dotazione degli strumenti e delle risorse informatiche, telematiche e di telefonia non costituisce titolo per l'acquisizione di alcun diritto in capo ai predetti soggetti e può essere ridotta, sospesa o eliminata qualora ne sussistano le motivazioni.

3. Ogni soggetto identificato al precedente punto 2, dopo aver ricevuto le relative istruzioni, è responsabile, sotto i profili amministrativi, civili e penali, del corretto uso degli strumenti informatici, telematici e di telefonia e del contenuto delle comunicazioni effettuate. Risponde dei danni, anche all'immagine dell'Ente, che possono derivare da comportamenti illeciti.

4. La Camera privilegia l'attività di prevenzione rispetto a quella di controllo, indicando ed attuando, in un'ottica di reciproco affidamento, appropriate misure di tutela e promuovendo misure di autotutela da parte dei fruitori, nonché assicurando la massima diffusione al contenuto del presente Disciplinare.

5. Nello svolgimento dell'attività di monitoraggio e controllo la Camera agisce nel rispetto della normativa vigente, con particolare riguardo alla tutela dei diritti dei lavoratori e alle garanzie in materia di protezione dei dati personali, nell'osservanza dei principi di ragionevolezza, correttezza, trasparenza e proporzionalità.

Art. 3
DESTINATARI

1. Il presente Disciplinare si applica ai dirigenti, ai dipendenti, o a questi assimilati, ed in genere a tutti gli autorizzati ad accedere alla rete camerale e agli strumenti informatici, telematici e di telefonia (d'ora innanzi più brevemente denominati "personale") per lo svolgimento della propria attività lavorativa.

2. Le prescrizioni del presente Disciplinare integrano le specifiche istruzioni impartite agli autorizzati al trattamento dei dati personali ai sensi del Regolamento UE n. 679/2016 e del D.Lgs. n. 196/2003 e s.m.i.

3. Il mancato rispetto delle regole e dei divieti di cui al presente Disciplinare costituisce, per i dipendenti, violazione del Codice di comportamento e determina, nel rispetto dei principi di gradualità e proporzionalità, l'applicazione delle sanzioni disciplinari previste dalle disposizioni di legge e dal Contratto Collettivo di Lavoro vigente, fatto salvo comunque il diritto della Camera di Bergamo al risarcimento dei danni eventualmente patiti a causa della condotta del lavoratore. Il mancato rispetto delle regole e dei divieti del presente Disciplinare costituisce, per i collaboratori esterni, violazione degli obblighi contrattuali.

4. Al presente Disciplinare viene data la massima pubblicità, anche mediante pubblicazione sulla intranet camerale a tutti i dipendenti, nonché con l'adeguata formazione anche in relazione alla tutela dei dati personali.

5. Per tutto quanto non espressamente contenuto nel presente Disciplinare si rinvia al Piano Generale in materia di misure di sicurezza dell'Ente.

Sezione II
USO DEGLI STRUMENTI INFORMATICI, TELEMATICI E DI TELEFONIA

Art. 4
CRITERI GENERALI DI UTILIZZO

1. Gli strumenti informatici (personal computer, stampanti, ecc.), telematici (l'accesso ad internet, tramite collegamento fisso o mobile, la posta elettronica), telefonici (telefono fisso, cordless, cellulare) messi a disposizione dalla Camera, costituiscono strumento di lavoro.

2. Pertanto l'utilizzo di essi è consentito per finalità attinenti o comunque connesse con l'attività lavorativa, secondo criteri di correttezza e professionalità, coerentemente al tipo di attività svolta e nel rispetto delle disposizioni normative ed interne e delle esigenze di funzionalità e di sicurezza dei sistemi informativi.

È escluso l'uso per scopi privati e/o personali. In conformità a quanto previsto nel vigente codice di comportamento dei dipendenti della Camera di Commercio di Bergamo, eventuali deroghe nell'utilizzo degli strumenti informatici e di uso comune sono possibili ove ciò non vada a discapito dell'attività lavorativa, del decoro e dell'immagine dell'Ente, ovvero non comporti costi specifici, in linea con i principi di gestione e buon senso e in accordo con il proprio Responsabile.

3. L'utilizzo di tali strumenti messi a disposizione non configura alcuna titolarità, da parte del lavoratore, dei dati e delle informazioni trattate, che appartengono alla Camera ed ai quali l'Ente si riserva, pertanto, il diritto di accedere nei limiti consentiti dalle norme di legge e contrattuali.

4. Il personale deve custodire e utilizzare gli strumenti affidatigli in modo appropriato, con la massima attenzione e diligenza, essendo beni rilevanti anche ai fini della sicurezza del sistema. Gli strumenti sono configurati in modo da garantire il rispetto delle regole descritte nel presente Disciplinare e tale configurazione non deve essere modificata senza la preventiva necessaria autorizzazione dell'amministratore di sistema individuato in Infocamere s.c.r.l. o di chi ne abbia la competenza. Il personale è altresì tenuto ad informare direttamente il proprio responsabile/dirigente della struttura organizzativa di appartenenza, il Servizio Risorse Strumentali e il Responsabile della Protezione dei Dati (DPO), qualora vi sia la possibilità di una violazione di dati personali, fatti salvi gli obblighi di denuncia alle autorità competenti.

5. Le attività connesse al trattamento di dati devono essere svolte di norma attraverso l'ausilio di sistemi informativi centralizzati e non localizzati sul PC in dotazione.

Art. 5
POSTAZIONE DI LAVORO

1. Le postazioni di lavoro (PdL) sono gestite dall'Ufficio Servizi Informatici e Strumentali che le assegna agli Utenti. È vietato qualsiasi utilizzo che deturpi o rovini la PdL e tutti gli accessori/periferiche in assegnazione. La postazione di lavoro è provvista di software di sicurezza (software antivirus, personal firewall, software per aggiornamento automatico delle patch di sistema, etc.). L'utilizzatore della PdL è profilato come utente senza diritti amministrativi, fatti salvi i casi in cui sia necessario fornire l'utente di ulteriori diritti per l'utilizzo di software che richiedono aggiornamenti frequenti.

2. L'accesso alla stazione di lavoro è condizionato al corretto inserimento delle credenziali di autenticazione (user e password). Per l'uso, la scelta, la modifica e la custodia delle credenziali si rinvia a quanto previsto dal Piano Generale in materia di misure di sicurezza.

3. L'Utente assegnatario della postazione di lavoro è responsabile del suo corretto utilizzo nel rispetto delle seguenti regole comportamentali:

a) è fatto obbligo al dipendente di verificare che sul proprio personal computer sia sempre attivata la funzione di screen saver protetto da password o comunque il blocco riattivabile con inserimento password qualora si allontani dalla propria postazione;

b) la PdL non deve essere accessibile a soggetti non autorizzati;

c) tutto il personale ha l'obbligo di salvare la documentazione relativa alla propria attività lavorativa sugli spazi della rete aziendale;

d) al termine della giornata lavorativa, soprattutto per motivi di sicurezza, deve essere effettuato lo spegnimento delle PdL.

4. È vietato:

a) installare sulla stazione di lavoro software, anche se gratuiti (freeware o shareware) non distribuiti e/o comunque non espressamente autorizzati dalla Camera e collegare alla stazione di lavoro periferiche hardware o dispositivi non messi a disposizione dall'Ente;
b) alterare, disattivare o modificare le impostazioni di sicurezza e di riservatezza del sistema operativo, del software di navigazione, del software di posta elettronica e di ogni altro software installato sulle attrezzature e sugli strumenti, fissi e mobili (postazione di lavoro, notebook, tablet, cellulari, altri supporti, ecc.), forniti in dotazione al personale. Inoltre, l'incaricato ha il dovere di usare e gestire le attrezzature e gli strumenti ricevuti in dotazione con attenzione e diligenza, nonché quello di segnalare tempestivamente all'Ufficio Servizi Informatici e Strumentali e/o al proprio responsabile/dirigente ogni anomalia o disfunzione al fine di ripristinare il corretto funzionamento degli stessi;
c) accedere al *Bios* delle stazioni di lavoro e impostare protezioni o password ulteriori rispetto a quelle contemplate nel Piano Generale in materia di misure di sicurezza dell'Ente che limitino l'accesso alle stazioni di lavoro stesse;
d) caricare o detenere nelle postazioni di lavoro e/o stampare materiale di contenuto non attinente allo svolgimento dell'attività lavorativa, quando questi comportamenti interferiscano con le mansioni attribuite, ovvero aggravino i rischi connessi all'utilizzo dei relativi strumenti;
e) in ogni caso, caricare, detenere e/o stampare materiale informatico:
   - il cui contenuto (a mero titolo esemplificativo: testo, audio, video) sia chiaramente tutelato da diritto d'autore. Nel caso in cui ciò sia necessario per la propria attività lavorativa, il lavoratore è tenuto ad attivare preventivamente gli adempimenti previsti dalla legge;
   - il cui contenuto sia contrario a norme di legge.

5. Le modifiche alla configurazione delle stazioni di lavoro possono essere effettuate unicamente da soggetti espressamente e formalmente autorizzati dalla Camera. Il personale non è autorizzato a modificare il sistema neppure se si tratta della postazione di lavoro assegnata.

6. A titolo esemplificativo, ma non esaustivo, sono considerate modifiche del sistema:

a) modificare i collegamenti di rete esistenti;
b) usare dispositivi removibili (CD, dvd, hard disk, floppy etc.) per alterare la procedura di avvio del dispositivo ed in particolare per effettuare l'avvio di un sistema operativo diverso da quello fornito dalla Camera;
c) aprire la struttura esterna (case) dell'elaboratore e procedere alla modifica (eliminazione o aggiunta) di componenti dello stesso;
d) installare, senza l'assistenza di personale autorizzato, un qualsiasi software, inclusi quelli scaricati da Internet, o comunque alterare la configurazione della stazione di lavoro assegnata.

7. Le cartelle presenti nei server della Camera sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in questa unità. Su tale unità vengono svolte regolari attività di verifica, amministrazione e back up da parte del personale incaricato.

8. Il personale incaricato può in qualsiasi momento procedere alla rimozione di file o applicazioni che riterrà essere pericolosi per la sicurezza sia sulle stazioni di lavoro sia sui server di rete.

9. Con regolare periodicità, secondo quanto previsto dalle indicazioni del Disciplinare per gli autorizzati al trattamento dei dati della Camera di Commercio ciascun dipendente deve provvedere alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili.

Art. 6
POSTAZIONE DI LAVORO PORTATILE

1. Per quanto riguarda la postazione portatile, valgono tutte le regole già descritte per le postazioni fisse.

2. Si evidenzia che le stazioni di lavoro portatili, utilizzate al di fuori della sede, sono maggiormente esposte

a rischi di sicurezza, quali danneggiamenti conseguenti agli spostamenti, furti, violazione della riservatezza delle informazioni contenute. Tutti gli Utenti, pertanto, devono custodire con cura e diligenza la postazione di lavoro portatile assegnata.

3. Le postazioni di lavoro portatili devono essere verificate dall'Ufficio Servizi Informatici e Strumentali per l'installazione di eventuali aggiornamenti e/o patch di sicurezza. La verifica avviene mediante appuntamento concordato con l'Ufficio stesso. In caso di significativo rischio di compromissione o/e sicurezza, l'Ufficio può richiedere all'utente lo spegnimento della PdL portatile fino a tale verifica.

Art. 7
UTILIZZO DELLA RETE INTERNET

1. L'accesso alla Rete Internet costituisce strumento di lavoro ed è consentito, di regola, per finalità direttamente attinenti o comunque connesse all'esercizio dell'attività lavorativa. È escluso qualsivoglia uso per scopi privati e/o personali.

2. È vietato entrare nella rete e nei programmi con un codice di identificazione diverso da quello assegnato. Le credenziali di accesso alla rete ed ai programmi sono segrete e vanno gestite secondo le istruzioni e le procedure impartite.

3. E', altresì, vietato:

a) scaricare e/o installare software non espressamente autorizzati dall'Ente;
b) scaricare e/o usare materiale informatico non direttamente attinente all'esercizio dell'attività lavorativa;
c) scaricare e/o usare materiale informatico il cui contenuto (a mero titolo esemplificativo: software, testo, audio e video) sia chiaramente tutelato dal diritto di autore;
d) partecipare a forum di discussione online, a chat, utilizzare sistemi di chiamata o di video chiamata, ecc. per ragioni non direttamente attinenti o connesse all'attività lavorativa;
e) navigare in internet su siti contrari a norme di legge;
f) effettuare ogni genere di transazione finanziaria per fini personali;
g) installare e utilizzare strumenti per lo scambio di dati attraverso internet con metodologia *Peer to Peer* (es. eMule, kazaa, bittorrent etc.) indipendentemente dal contenuto dei file scambiati;
h) cedere, anche temporaneamente, il kit di firma digitale.

4. In un'ottica preventiva l'amministratore di sistema Infocamere s.c.r.l. ha già provveduto a predisporre un sistema informatico di filtraggio teso ad impedire la navigazione su siti web contrari a norme di legge, o considerati non sicuri. Tuttavia, l'Ente si riserva di disporre ed effettuare controlli, anche tramite l'esame puntuale delle registrazioni degli accessi (file di log) relativi al traffico web, finalizzati al rispetto del presente Disciplinare.

Art. 8
UTILIZZO DELLA POSTA ELETTRONICA

1. La Camera mette a disposizione di ogni lavoratore il servizio di posta elettronica, assegnando a ciascuno di essi caselle di posta istituzionali (cognome@bg.camcom.it), per fini esclusivamente lavorativi.

2. Al fine di agevolare lo svolgimento dell'attività lavorativa, l'Ente rende disponibili indirizzi di posta elettronica condivisi tra più utenti (caselle di posta istituite per singole unità organizzative) affiancandoli a quelli individuali.

3. L'indirizzo di posta elettronica messo a disposizione costituisce uno strumento di lavoro ed il suo utilizzo è consentito unicamente per finalità attinenti o comunque connesse allo svolgimento dell'attività lavorativa. Conseguentemente, stante la sua natura di strumento di comunicazione aziendale, il dipendente è consapevole che sullo stesso non potrà essere garantita la riservatezza dei documenti inviati e ricevuti; pertanto, sarà impegno del dipendente evitare l'utilizzo delle caselle di posta elettronica per comunicazioni di carattere personale o che esulino dal contesto lavorativo cui sono preposte.

4. La sicurezza e la riservatezza della posta elettronica sono garantite dalla necessità di disporre di idonee credenziali di autenticazione per accedere alla stessa. La password dell'account di posta elettronica è scelta e registrata dal dipendente nel rispetto dei criteri e delle regole indicati dal Piano Generale in materia di misure

di sicurezza dell'Ente.

5. Al fine di un corretto utilizzo della posta elettronica è vietato:

   a) inviare o memorizzare messaggi di natura oltraggiosa, volgare, diffamatoria e/o discriminatoria, ed in ogni caso contrari a norme di legge o idonei a creare danno alla Camera o a terzi nonché messaggi a catena e/o spam;
   b) scambiare messaggi impersonando un mittente diverso da quello reale;
   c) scambiare messaggi di posta contenenti file o link a siti con contenuti illegali, violenti, o pornografici, file o materiale informatico soggetto al diritto d'autore, password e/o codici d'accesso a programmi soggetti a diritto d'autore e/o a siti internet;
   d) aprire messaggi di posta o allegati di tipo eseguibile, salvo il caso di certezza assoluta dell'identità del mittente e della sicurezza del messaggio;
   e) utilizzare l'indirizzo e-mail per l'iscrizione e/o la partecipazione a social network, mailing list, servizi di instant messaging, forum o altri servizi pubblici su internet di interesse personale e non lavorativo;
   f) diffondere, all'esterno della Camera di Commercio, indirizzi di posta elettronica di altri colleghi, per motivi non legati all'attività lavorativa.

6. Nell'ambito dei rapporti di tirocinio di formazione verrà assegnata una casella di posta al tirocinante.

7. Tutti i messaggi di posta elettronica inviati dalle caselle istituzionali dell'Ente conterranno il seguente messaggio automatico: *"I dati comunicati in risposta a questa mail saranno oggetto di trattamento nel rispetto del Regolamento UE 2016/679 e della vigente normativa nazionale in materia di protezione dei dati personali. Titolare è la Camera di Commercio di Bergamo. Il contenuto del presente messaggio è riservato e diretto esclusivamente ai destinatari. Se avete ricevuto questo messaggio per errore Vi preghiamo di cancellarlo e di contattarci via mail. Grazie".*

8. In caso di assenze programmate dal lavoro, per ferie o per qualsiasi altro motivo di assenza prolungata, deve essere attivato preventivamente il sistema di risposta automatica. Il messaggio di risposta predefinito deve indicare il periodo di assenza e l'indirizzo di posta elettronica di un altro lavoratore in caso di comunicazioni urgenti.

Art. 9
TRATTAMENTO DEI DATI RELATIVI ALLA POSTA ELETTRONICA PER ASSENZE PROLUNGATE E IMPROVVISE DEI DIPENDENTI, EX DIPENDENTI ED EX COLLABORATORI DELL'ENTE

1. In caso di assenza prolungata e improvvisa del dipendente, l'Ufficio del personale in accordo con il dirigente responsabile, chiede all'Ufficio Servizi Informatici e Strumentali di far predisporre a Infocamere s.c.r.l. un messaggio automatico di risposta che segnali al mittente l'assenza e indichi il contatto alternativo.

2. Per coloro che a qualsiasi titolo cessino il proprio rapporto di lavoro o di collaborazione, l'Ufficio del Personale chiede all'Ufficio Servizi Informatici e Strumentali l'immediata disattivazione dell'indirizzo di posta elettronica. Su richiesta del Dirigente/Responsabile, l'Ufficio Servizi Informatici e Strumentali si attiva per far predisporre a Infocamere s.c.r.l. un sistema automatico di risposta che segnala al mittente che l'indirizzo di posta non è più attivo e indica il contatto alternativo a cui rivolgersi.

Art. 10
DISPOSITIVI DI MEMORIZZAZIONE RIMOVIBILI (HARD DISK, PEN DRIVE USB, ETC.)

1. L'utilizzo di supporti di memorizzazione rimovibili deve essere effettuato con molta cautela ed esclusivamente per le attività lavorative. Al momento della connessione di un dispositivo esterno viene avviata la scansione automatica antivirus, per permettere al sistema di completare la verifica di sicurezza che non può essere interrotta dall'utente. È inoltre fondamentale che il dispositivo non venga disconnesso durante la scansione, per non danneggiare e rendere illeggibili i dati.

2. L'utilizzo di dispositivi rimovibili, utile per esempio per effettuare copie di sicurezza o per trasportare file di grandi dimensioni, rimane in ogni caso sotto la responsabilità dell'utilizzatore, che è tenuto a rivolgersi all'Ufficio Servizi Informatici e Strumentali per le opportune configurazioni di sicurezza e/o crittografia del dispositivo.

3. È vietato consegnare a terzi supporti già utilizzati per la memorizzazione di informazioni o di dati personali, anche se cancellati, in quanto è tecnicamente possibile il loro recupero anche dopo l'intervenuta cancellazione.

4. L'Utente è tenuto a informare immediatamente il proprio responsabile/dirigente della struttura organizzativa di appartenenza, il Servizio Risorse Strumentali e il Responsabile della Protezione dei Dati (DPO), anche ai sensi della procedura di gestione delle violazioni di dati personali, di qualsiasi danno, furto o perdita di apparati, software e/o dati in proprio possesso, fatti salvi gli obblighi di denuncia alle autorità competenti.

5. I supporti rimovibili (CD, DVD, pen drive, schede di memoria, hard disk rimovibili, etc.) devono essere custoditi con la massima diligenza e riservatezza e non devono essere lasciati incustoditi o facilmente accessibili.

6. Nel momento in cui l'utente non ha più bisogno del supporto, sia esso riscrivibile o non riscrivibile (ad esempio: CD-R, DVD-R, DVD+R, CD-RW, DVD-RW, DVD+RW, pen drive, schede di memoria, hard disk rimovibili, etc.), è tenuto a restituirlo all'Ufficio Servizi Informatici e Strumentali.

Sezione III
CONTROLLI

Art. 11
MODALITA' DI EFFETTUAZIONE DEI CONTROLLI

1. La Camera si riserva la facoltà, nel rispetto della tutela del diritto alla riservatezza e del principio di proporzionalità e non eccedenza, nonché sul presupposto di un utilizzo responsabile dell'attrezzatura da parte degli utenti, di svolgere dei controlli saltuari e a campione che consentano di verificare l'effettiva conformità dell'uso degli strumenti informatici e di telefonia alle presenti prescrizioni.

2. I controlli sono effettuati da Infocamere s.c.r.l. su richiesta del Segretario Generale.

3. I controlli non potranno mai svolgersi direttamente e in modo puntuale, ma dovranno preliminarmente essere compiuti su dati aggregati, riferiti all'intera struttura organizzativa o a sue unità operative anche attraverso specifici audit informatici.

4. A seguito di detto controllo anonimo, laddove fosse rilevata una effettiva e grave anomalia dell'attività, potrà essere emesso un avviso generalizzato, con l'invito ad attenersi esclusivamente e scrupolosamente ai compiti assegnati e alle istruzioni impartite. Se a detta comunicazione non dovessero seguire, nei quindici giorni successivi, ulteriori anomalie, l'Ente non procederà a ulteriori controlli. In caso contrario, verranno inoltrati preventivi avvisi, sempre su base anonima, riferiti all'unità organizzativa dalla quale provenga l'anomalia riscontrata.

5. Qualora continuino i comportamenti non conformi, l'Ente si riserva la facoltà di svolgere successive azioni mirate alla verifica del corretto utilizzo e, a seconda della gravità della violazione riscontrata, potranno essere applicate sanzioni di tipo civile, penale e/o disciplinare.

6. In ogni caso non sono ammessi, su base individuale, controlli casuali, prolungati, costanti o indiscriminati.

7. L'Ente inoltre non effettuerà, in nessun caso, né farà effettuare da eventuali Responsabili esterni, trattamenti di dati personali mediante sistemi *hardware* e/o *software* che mirino al controllo a distanza dei lavoratori, ovvero a ricostruire l'attività del lavoratore, quali a titolo esemplificativo e non esaustivo:

a) lettura e/o registrazione sistematica dei messaggi di posta elettronica, ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio di posta elettronica stesso;
b) riproduzione ed eventuale memorizzazione sistematica delle pagine *web* visualizzate dal lavoratore, dei contenuti delle medesime, nonché del tempo di permanenza sulle stesse;
c) lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
d) analisi occulta di computer o altri dispositivi portatili affidati in uso, ovvero delle rispettive connessioni ad Internet;

e) le attività descritte, ed altre per i medesimi scopi, effettuate sulle utenze telefoniche fisse o relative a telefonia cellulare.

8. Resta sempre salvo l'obbligo dell'Ente di comunicare i *log file* o altre evidenze contenenti le prove informatiche relative ai comportamenti illeciti dei dipendenti alle Autorità Giudiziarie competenti che ne facciano richiesta secondo la normativa vigente.

Sezione IV
DISPOSIZIONI FINALI

Art. 12
INFORMATIVA

Il contenuto del presente disciplinare integra l'informativa già fornita ai dipendenti e ai collaboratori ai sensi dell'art. 13 [e 14] del Regolamento UE n. 679/2016 e del D.Lgs. n. 196/2003, nonché il "Piano Generale per la Sicurezza dei Documenti" approvato ed allegato alla delibera n.99 del 18.12.2023 e suoi eventuali successivi aggiornamenti.

Art. 13
DISCIPLINA RELATIVA A DEROGHE E MODIFICHE

1. Eventuali comportamenti non in linea con il presente documento, che venissero comunque tollerati dall'Ente, non costituiscono una rinuncia della stessa ad esercitare successivamente i suoi diritti per far valere il presente disciplinare. I componenti delle RSU e i dipendenti possono utilizzare gli indirizzi di posta elettronica aziendale nell'esercizio dei diritti sindacali. I contenuti di queste comunicazioni sono coperti da assoluta riservatezza.

Art. 14
ENTRATA IN VIGORE

1. Il presente Disciplinare entra in vigore dalla data di adozione del provvedimento di approvazione e sostituisce ed abroga eventuali procedure o disposizioni con esso incompatibili.

2. Del presente atto sarà fornita massima pubblicità e diffusione mediante la sua pubblicazione nella rete Intranet.

3. Per quanto non espressamente richiamato nel presente atto si rinvia alle disposizioni civili e penali vigenti in materia.