CAMERA DI COMMERCIO
DEL SUD EST SICILIA

Allegato n. 6

# Camera di commercio, industria artigianato e agricoltura del Sud Est Sicilia

## DISCIPLINARE PER IL CORRETTO UTILIZZO DEGLI STRUMENTI INFORMATICI, DELLA RETE INFORMATICA E TELEMATICA (INTERNET E POSTA ELETTRONICA), DEL SISTEMA DI TELEFONIA FISSA E MOBILE E PER LA CORRETTA GESTIONE DEI DATI CARTACEI

ai sensi del Regolamento UE 2016/679 e dei Provvedimenti del Garante per la protezione dei dati personali

## INTRODUZIONE

### *PREMESSA*

L'ampia diffusione delle tecnologie dell'informazione avvenuta nel corso degli ultimi anni ha rappresentato sicuramente un traguardo importante per il mondo del lavoro. Tuttavia, accanto ai benefici generati da tali tecnologie, occorre contemperare le esigenze organizzative del datore di lavoro con quelle di tutelare la riservatezza dei dati

personali dei lavoratori.

In questo senso, viene fortemente sentita dai datori di lavoro la necessità di porre in essere adeguati sistemi di controllo sull'utilizzo di tali strumenti da parte dei dipendenti/collaboratori e di sanzionare conseguentemente quegli usi scorretti che, oltre ad esporre l'ente stesso a rischi tanto patrimoniali quanto penali, possono di per sé considerarsi contrari ai doveri di diligenza e fedeltà previsti dagli artt. 2104 e 2105 del Codice civile. I controlli sull'uso degli strumenti informatici/telefonici tuttavia, devono garantire tanto il diritto del datore di lavoro di proteggere la propria organizzazione, quanto il diritto del lavoratore a non vedere invasa la propria sfera personale, e quindi il diritto alla riservatezza ed alla dignità come sanciti dallo Statuto dei lavoratori e dalla disciplina sul trattamento e la tutela dei dati personali.

In considerazione di ciò, e sollecitato da diverse segnalazioni, il Garante per la protezione dei dati personali ha avvertito la necessità di predisporre delle linee guida per i datori di lavoro pubblici e privati, affinché prevedessero un'apposita disciplina interna per l'utilizzo dei dispositivi tecnologici da parte dei lavoratori.

Gli obiettivi che il Garante si è prefisso attraverso l'elaborazione di tali linee guida sono molteplici. Da un lato si auspica la predisposizione, da parte dei datori di lavoro, di regole interne volte alla definizione delle modalità di utilizzo delle tecnologie informatiche da parte dei lavoratori. Dall'altro lato, le linee guida si propongono di soddisfare esigenze di tutela dello stesso lavoratore o dei terzi, contro le condotte dei datori di lavoro che si traducano in una violazione della riservatezza. In considerazione dei peculiari riconoscimenti che il nostro ordinamento assegna al luogo di lavoro, il Garante ha ritenuto imprescindibile stabilire specifiche regole a presidio della integrità della *privacy* del lavoratore.

Tanto premesso è stato elaborato il presente Disciplinare per:

- indicare i criteri per il corretto utilizzo degli strumenti informatici/telematici, escludendo le piattaforme informatiche di uso centralizzato o di sistema, e telefonici da parte dei dipendenti e/o collaboratori nonché la corretta gestione dei dati cartacei;
- definire i limiti e le finalità entro i quali il datore di lavoro (Titolare del trattamento) può legittimamente porre in essere controlli sui predetti strumenti.

La regolamentazione di seguito proposta sotto forma di articolato, essendo rilevante ai fini delle eventuali azioni disciplinari attivabili dal datore di lavoro nei confronti del dipendente, è stata redatta tenendo conto, da una parte, delle disposizioni contenute nella Legge n. 300/1970 in tema di controllo dei lavoratori (art. 4) e di provvedimenti disciplinari (art. 7) e, dall'altra, delle indicazioni emerse nelle sentenze di merito e di legittimità rinvenibili in materia.

## *FINALITÀ DEL DOCUMENTO E MODALITÀ DI APPROVAZIONE*

In attuazione degli specifici obblighi formali e sostanziali proposti dal Regolamento UE 2016/679 (di seguito anche "GDPR"), dal D.Lgs. 196/2003, recante il Codice in materia di protezione dei dati personali, come modificato dal D.Lgs. 101/2018 (di seguito anche "Codice") e da specifici provvedimenti del Garante per la protezione dei dati personali (di seguito indicato anche "Garante"), si comunica a tutti i dipendenti e collaboratori della Camera di commercio del Sud Est Sicilia il presente "Disciplinare sull'utilizzo degli strumenti informatici, telematici, telefonici e di gestione dei dati in formato cartaceo".
Scopo del presente documento è definire i comportamenti da adottare al fine di:

- garantire nel tempo il livello di riservatezza, integrità e disponibilità dei dati personali richiesto dalla normativa vigente e, più in generale, delle informazioni raccolte e gestite dall'Ente in qualità di Titolare/Contitolare o Responsabile del trattamento (in relazione ad attività svolta con altri Enti);
- assicurare il corretto utilizzo degli strumenti messi a disposizione dei lavoratori;
- salvaguardare il patrimonio dell'Ente.

Il Disciplinare:

- deve essere conosciuto e condiviso quale **norma di comportamento durante lo svolgimento delle attività lavorative**, ognuno per la propria Area/Servizio/Ufficio e per le mansioni di competenza;
- devono intendersi quali **istruzioni impartite dal Titolare** obbligatorie con decorrenza dalla data della sua entrata in vigore e con valore di ordine di servizio, il cui mancato rispetto **costituisce inosservanza delle disposizioni al personale** e può essere, quindi, oggetto di provvedimenti disciplinari ai sensi della vigente normativa contrattuale e del Codice disciplinare della Camera di commercio;
- **integrano e completano, infine, l'informativa per il trattamento dei dati personali** ai fini di gestione del rapporto di lavoro/collaborazione, redatta e già fornita agli interessati ai sensi dell'art. 13 del GDPR e la nomina per i dipendenti a soggetti autorizzati al trattamento.

Il presente documento sarà comunicato alle Organizzazioni sindacali dell'Ente, regionali e aziendali, per le eventuali valutazioni sugli aspetti di competenza di cui al contratto di lavoro ed alla legge n. 300/1970.

Il documento è diffuso a tutto il personale attraverso:

- collocazione su cartella condivisa in drive Icsuite;
- specifici interventi formativi e informativi generalizzati o specifici di ambito professionale;
- comunicazione mezzo mail istituzionale inviata a tutti i dipendenti;

## *RIFERIMENTI NORMATIVI*

Il presente documento risponde ai seguenti requisiti normativi:

- Regolamento UE 2016/679, Relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (GDPR);
- D.Lgs. 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali così come modificato dal D.Lgs. 101/2018;
- L. 20 maggio 1970, n. 300, Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento;
- L. 23 dicembre 1993 n. 547, Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica;
- D.L. 27 luglio 2005, n. 144, convertito con la L. 31 luglio 2005 n. 155, Misure urgenti per il contrasto del terrorismo internazionale; Decreto Interministeriale del 16 agosto 2005 (in G.U. n. 190 del 17 agosto 2005);
- Art. 24 della L. 20 novembre 2017, n. 167, Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea – Legge europea 2017;
- L. 22 aprile 1941 n. 633, Protezione del diritto d'autore e di altri diritti concessi al suo esercizio [*al cui interno è compresa la disciplina dei programmi per elaboratori e le banche dati*];
- D. Lgs. 10 febbraio 2005, n. 30, Codice della proprietà industriale;
- D. Lgs. 1° agosto 2003, n. 259, Codice delle comunicazioni elettroniche;
- D. Lgs.-7 marzo 2005, n. 82, Codice dell'amministrazione digitale;
- D.P.R. 16 aprile 2013, n. 62, Regolamento recante codice di comportamento dei dipendenti pubblici, a norma dell'articolo 54 del decreto legislativo 30 marzo 2001, n. 165 [Il Codice di comportamento dei dipendenti della Camera di commercio è pubblicato nel sito camerale alla voce Amministrazione trasparente → Disposizioni generali → Atti generali];
- Presidenza del Consiglio dei Ministri, Dipartimento della Funzione Pubblica, Direttiva 26 maggio 2009, n. 2, Utilizzo di Internet e della casella di posta elettronica istituzionale sul posto di lavoro;
- Garante per la protezione dei dati personali, Provvedimento del 13 ottobre 2008, Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali;
- Garante per la protezione dei dati personali, Provvedimento del 27 novembre 2008, Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema.
- UNI EN ISO 9001:2015 "Sistemi di gestione per la Qualità - Requisiti".

Ulteriori provvedimenti ed indicazioni del Garante che delineano il contesto di riferimento in materia sono:

- Deliberazione n. 13 del 1° marzo 2007, Linee guida del Garante per posta elettronica e *internet* (G.U. n. 58 del 10 marzo 2007);
- Deliberazione n. 23 del 14 giugno 2007, Linee guida del Garante in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico (G.U. n. 161 del 13 luglio 2007);
- Provvedimento del 17 gennaio 2008 in tema di sicurezza dei dati di traffico telefonico e telematico (G.U. n. 30 del 5 febbraio 2008);
- Provvedimento del 24 luglio 2008 in tema di sicurezza dei dati di traffico telefonico e telematico (G.U. n. 189 del 13 agosto 2008);
- Vademecum relativo alle regole per il corretto trattamento dei dati personali dei lavoratori da parte di soggetti pubblici e privati, pubblicato dal Garante il 24 aprile 2015 (https://www.lavoroediritti.com/wp-content/files/Privacy_e_lavoro_-_vademecum_2015.pdf);
- Provvedimento n. 456 del 30 luglio 2015, relativo al trattamento effettuato sulle e-mail di dipendenti ed ex

dipendenti;

- Provvedimento n. 547 del 22 dicembre 2016, relativo all'accesso da parte del datore di lavoro alla posta elettronica dei dipendenti;
- Newsletter n. 424 del 17 febbraio 2017, relativa relativo all'accesso da parte del datore di lavoro alla posta elettronica ed agli smartphones dei dipendenti (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5989944#1);
- Newsletter n. 430 del 24 luglio 2017, relativa all'accesso da parte del datore di lavoro *all'*uso privato dei social network e le comunicazioni dei lavoratori, spazi riservati sul cloud (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6633587#3);
- Newsletter n. 437 del 26 gennaio 2018, relativa alla legittimità da parte del datore di lavoro del controllo sui telefoni aziendali dei dipendenti (https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7570001#3).

## *ACRONIMI E DEFINIZIONI GENERALI UTILIZZATE*

| | |
|---|---|
| GDPR/Regolamento | Regolamento UE 2016/679 (General Data Protection Regulation) |
| Codice | D. Lgs. n. 196/2003 "Codice in materia di protezione dei dati personali" (come modificato dal D. Lgs. n. 101/2018) |
| Garante | Garante per la protezione dei dati personali |
| WP29 | Working Party article 29 – Gruppo di lavoro ex art. 29 (ora Comitato europeo della protezione dei dati) |
| RPD/DPO | Responsabile della Protezione dei Dati/ *Data Protection Officer* |
| Delegato del Titolare | Soggetto che, secondo le deleghe/procure formalizzate ed il sistema di gestione della privacy, garantisce specifiche funzioni ai fini della *compliance* al GDPR |
| SG | Segretario Generale della Camera di commercio del Sud Est Sicilia |

## *GLOSSARIO DEI TERMINI*

| | |
|---|---|
| Casi di urgenza<br><br>Situazioni di necessità | Con questa terminologia si intendono tutte quelle situazioni in cui è necessario intervenire senza frapporre tempi morti o di richiesta che potrebbero pregiudicare l'azione puntuale dell'Ente rispetto ad eventi o servizi non procrastinabili. |
| Delegato del dipendente | Trattasi di soggetto con il quale il Dipendente ha un rapporto fiduciario a cui vengono affidate dallo stesso le credenziali per accedere in via emergenziale a fronte dell'impossibilità dimostrata del Dipendente ad accedere direttamente ai servizi oggetto dell'intervento.<br><br>Il nominativo del delegato deve essere comunicato al responsabile dell'ufficio o alla Segreteria Generale. Gli ambiti in cui è necessario disporre di questa procedura sono: posta elettronica (lì dove il dipendente non utilizzi caselle e-mail di gruppo per ricevere comunicazioni dell'ente), casella PEC (lì dove il dipendente abbia un uso esclusivo della stessa e la password non fosse a conoscenza del suo Responsabile diretto), cartelle personali su server (lì dove il dipendente custodisca su cartelle personali documenti che servono per le attività dell'Ente e non le abbia riposte nelle apposite cartelle condivise), il computer assegnato (lì dove il dipendente abbia riposto su cartelle presenti sul computer assegnato, e non sulle apposite cartelle condivise su server) materiale indispensabile all'Ente. |
| Regole di data retention | Per tutti i dati personali oggetto di trattamento presso l'Ente sono stabilite delle regole di data retention (tempo di conservazione); queste regole valgono: per i documenti cartacei, per le basi dati ma anche per i file eventualmente frutto di estrazioni e/o elaborazioni effettuate per l'Ente o per soggetti esterni. Ogni singolo designato al trattamento (soggetto |

| | |
|---|---|
| | che può trattare specifici dati personali su mandato dell'Ente) ha la responsabilità di garantire il rispetto dei tempi di data retention per tutto quello che è al di fuori dei processi automatici di gestione delle banche dati: fascicoli cartacei, file oggetto di estrazioni, archivi derivati non cancellati automaticamente. |
| Ragioni di urgenza o di necessità | La ragioni di urgenza e di necessità richiamate più volte nel disciplinare sono di difficile definizione preventiva ma vogliono intendere che al Dipendente è lasciato uno spazio di operatività che può essere utilizzato, avvalendosi anche di strumentazioni dell'Ente, per affrontare e rispondere con efficacia a problematiche di ordine episodico NON risolvibili in modalità differita. Questo tipo di situazione deve essere valutato dell'interessato in sua completa responsabilità sapendo che ogni abuso, o utilizzo non lecito o non emergenziale, esce dagli ambiti di giustificabilità dell'azione. |

*MATRICE DELLA REDAZIONE E DELLE REVISIONI*

| Data | Stato | Descrizione | Approvazione |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

## DISCIPLINARE SULL'UTILIZZO DI SISTEMI INFORMATICI, TELEMATICI E TELEFONICI

Il Disciplinare proposto riguarda l'uso di internet, della posta elettronica (ed altri strumenti/risorse informatiche e/o telematiche), nonché la telefonia fissa o mobile oltre che la corretta gestione dei dati cartacei. Dopo una breve premessa introduttiva, il Disciplinare consta di 12 articoli distribuiti all'interno di quattro Sezioni.

La Sezione I, recante le "Disposizioni generali", chiarisce le finalità della disciplina che, per un verso, è una misura organizzativa di strumenti tecnici e tecnologici all'interno dell'Ente e, per un altro verso, costituisce le "istruzioni" del datore di lavoro (nonché Titolare del trattamento dei dati personali) finalizzate a:

- 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.

Nell'ambito dei principi generali si chiarisce che gli strumenti informatici, telematici, telefonici e, in genere, tutta la strumentazione posta a disposizione del lavoratore fa parte delle risorse di proprietà dell'Ente.

Tra i principi generali si esplicita che:

- le prescrizioni del Disciplinare integrano le specifiche istruzioni impartite agli autorizzati in materia di trattamento dei dati personali ai sensi del Regolamento UE 2016/679 e del D. Lgs. 196/2003 come modificato dal D. Lgs. 101/2018;
- il mancato rispetto delle regole e dei divieti 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 (con il risarcimento dei danni causati all'Ente dalla condotta del lavoratore). Per i collaboratori esterni il mancato rispetto delle regole e dei divieti costituisce violazione degli obblighi contrattuali.

Alle modalità di applicazione delle Sanzioni è dedicata la Sezione III.

La Sezione II, dedicata all'"Uso degli strumenti informatici, telematici e di telefonia e alla corretta gestione dei dati cartacei", dopo alcune indicazioni generali, è ripartita in 10 ambiti, ciascuno dei quali è oggetto di un articolo. Gli ambiti sono:

- l'utilizzo degli strumenti informatici;
- scelta, uso, modifica e custodia delle credenziali di autenticazione;
- la rete Internet e la navigazione;
- l'utilizzo della posta elettronica;
- la protezione antivirus;
- la gestione dei backup;
- l'utilizzo di strumenti di telefonia fissa e mobile, mobile device, fotocopiatrici e fax;
- uso, custodia e dismissione dei supporti rimovibili;
- istruzioni sull'utilizzo dei social network;
- trattamento dati senza ausilio di strumenti informatici.

Con specifico riferimento alla posta elettronica (anch'essa una risorsa dell'Ente) si sono tenute in debito conto le indicazioni del Garante sul rispetto di diritti costituzionali dei dipendenti (manifestazione del pensiero e tutela della corrispondenza) contrapposti all'esigenza del datore di lavoro di poter accedere alle comunicazioni di posta elettronica. L'accesso "circostanziato" prevede la collaborazione del dipendente, ovvero di altro dipendente da questi "legittimato", di modo da riservare solo a situazioni eccezionali un accesso diretto da parte dell'Ente.

La Sezione III, come si diceva, concerne i controlli.

Per le modalità di svolgimento dei controlli si rinvia al successivo paragrafo.

Infine, la Sezione IV, comprende alcune disposizioni sull'entrata in vigore e sulla pubblicazione del Disciplinare.

## CONTROLLI E SANZIONI

### *MODALITA' DEI CONTROLLI*

L'Ente si riserva la facoltà, nel rispetto della tutela del diritto alla riservatezza e del principio di proporzionalità e non eccedenza, di svolgere dei controlli sugli strumenti informatici e di telefonia assegnati al personale.

**I controlli non potranno mai svolgersi direttamente e in modo puntuale, ma dovranno preliminarmente essere compiuti su dati aggregati e opportunamente anonimizzati, riferiti all'intera struttura organizzativa o a sue unità operative anche attraverso specifiche verifiche informatiche**.

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 ed alle istruzioni impartite.

Se a detta comunicazione non dovessero seguire, nei quindici giorni successivi, ulteriori anomalie, l'Ente non procederà a ulteriori verifiche.

In caso contrario, verranno inoltrati preventivi avvisi, sempre su base anonima, riferiti all'unità organizzativa dalla quale provenga l'anomalia riscontrata.

Qualora continuino i comportamenti sono effettuati controlli nominativi o su singoli dispositivi e postazioni e, a seconda della gravità della violazione riscontrata, saranno applicate le sanzioni indicate di seguito.

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

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, in violazione dell'art. 4 della L. 300/1970 (Statuto dei lavoratori).

**Resta sempre salvo l'obbligo dell'Ente di trasmettere tutti i dati richiesti (es. file log, tracce informatiche e quant'altro) contenenti le prove informatiche relative ai comportamenti illeciti dei dipendenti alle Autorità Giudiziarie competenti che ne facciano richiesta nei termini e secondo la normativa vigente.**

## FORMAZIONE

L'Ente, nell'ambito del programma di formazione sulla sicurezza, nonché di quello permanente sulla tutela dei dati personali, svolge attività di informazione e formazione con riferimento ai contenuti del Disciplinare con l'obiettivo, fra le altre cose, di rendere edotti tutti i dipendenti dei possibili rischi connessi con comportamenti non in linea con i contenuti di questo disciplinare. Verrà effettuata anche formazione specifica con riferimento anche alle tematiche concernenti il *Data Breach*. Per la formazione il competente ufficio acquisisce le indicazioni e il parere in merito del RPD.

ALLEGATO

Camera di commercio, industria, artigianato e agricoltura del Sud Est Sicilia

**DISCIPLINARE PER IL CORRETTO UTILIZZO DEGLI STRUMENTI INFORMATICI, DELLA RETE INFORMATICA E TELEMATICA (INTERNET E POSTA ELETTRONICA), DEL SISTEMA DI TELEFONIA FISSA E MOBILE E CORRETTA GESTIONE DEI DATI CARTACEI**

## PREMESSA

- La Camera di commercio, industria, artigianato e agricoltura del Sud Est Sicilia (di seguito "CCIAA", o "Ente") promuove ed incentiva l'utilizzo sempre più diffuso delle moderne tecnologie nell'ambito dello svolgimento dell'attività lavorativa, in quanto consente di perseguire con maggior efficacia, efficienza ed economicità le proprie finalità istituzionali, in un'ottica di semplificazione dell'attività amministrativa.
- A tal fine la CCIAA 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.

## Sezione I - DISPOSIZIONI GENERALI

### *Art. 1 - FINALITA'*

- Il presente Disciplinare è diretto a:
- porre in essere 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;
- informare coloro che utilizzano per lavoro gli strumenti informatici, la Rete Informatica e Telematica e il Sistema di telefonia messi a disposizione dalla CCIAA 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*

- La CCIAA 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.
- La titolarità dei beni e degli strumenti informatici, telematici e di telefonia è in capo alla CCIAA. 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.

- 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.
- La CCIAA 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.
- Nello svolgimento dell'attività di monitoraggio e controllo la CCIAA 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*

- Il presente Disciplinare si applica a tutti i dipendenti ed a tutti coloro i quali, a vario titolo, sono 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 nei confronti dell'Ente.
- Le prescrizioni del presente Disciplinare integrano le specifiche istruzioni impartite agli incaricati in materia di trattamento dei dati personali ai sensi del Regolamento UE 2016/679 e del D. Lgs. 196/2003, così come modificato dal D. Lgs. 101/2018.
- 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 CCIAA 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.
- Al presente Disciplinare verrà data la massima pubblicità, anche mediante affissione in ogni posto di lavoro, in luogo accessibile a tutti i dipendenti e collaboratori esterni, nonché con l'adeguata formazione anche in relazione alla tutela dei dati personali.

## Sezione II - USO DEGLI STRUMENTI INFORMATICI, TELEMATICI E DI TELEFONIA. GESTIONE DEI DATI SENZA L'AUSILIO DI STRUMENTI INFORMATICI

### *Art. 4- CRITERI GENERALI DI UTILIZZO*

- Gli strumenti informatici (a titolo esemplificativo personal computer, stampanti, ecc.), telematici (a titolo esemplificativo accesso ad Internet, tramite collegamento fisso o mobile, la posta elettronica), telefonici (a titolo esemplificativo telefono fisso, mobile, cellulare), messi a disposizione, costituiscono strumento di lavoro.
- Pertanto, l'utilizzo di essi è consentito, di regola, 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.
- Nella definizione di attività lavorativa sono comprese anche le attività strumentali e collegate allo svolgimento del rapporto di lavoro. È escluso qualsivoglia uso per scopi privati e/o personali, ad eccezione dei casi d'urgenza e comunque a condizione che tale uso avvenga solo per brevissimi periodi e in maniera estremamente episodica.
- 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 CCIAA ed ai quali l'Ente si riserva, pertanto, il diritto di accedere nei limiti consentiti dalle norme di legge e contrattuali.
- 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 di chi ne abbia la competenza. Il personale è altresì tenuto ad informare direttamente il proprio dirigente/funzionario o il responsabile da questi delegato nell'ipotesi di furto, danneggiamento o malfunzionamento anche parziale degli strumenti e/o del sistema.

## *Art. 5 - UTILIZZO DEGLI STRUMENTI INFORMATICI*

- L'accesso alla postazione di lavoro è condizionato al corretto inserimento delle credenziali di autenticazione (nome utente e password). Per l'uso, la scelta, la modifica e la custodia delle credenziali si rinvia a quanto previsto dall'Art. 6 del presente Disciplinare.
- È vietato:
  - installare sulla postazione di lavoro software, anche se gratuiti (freeware o shareware) non distribuiti e/o comunque non espressamente autorizzati dalla CCIAA e collegare alla stazione di lavoro periferiche hardware o dispositivi non messi a disposizione dall'Ente;
  - 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'autorizzato/l'utente 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'Amministratore di Sistema e/o al dirigente di settore/responsabile delegato ogni anomalia o disfunzione al fine di ripristinare il corretto funzionamento degli stessi;
  - accedere al *Bios* delle stazioni di lavoro e impostare protezioni o password ulteriori rispetto a quelle contemplate all'Art. 6 del presente Disciplinare che limitino l'accesso alle stazioni di lavoro stesse;
  - caricare o detenere nelle postazioni di lavoro e/o stampare materiale di contenuto non attinente allo svolgimento dell'attività lavorativa, in particolare quando questi comportamenti interferiscano con le mansioni attribuite, ovvero aggravino i rischi connessi all'utilizzo dei relativi strumenti;
  - in ogni caso, caricare, detenere e/o stampare materiale informatico:
    - il cui contenuto (a mero titolo esemplificativo: testo, audio, video, software) sia chiaramente tutelato da diritto d'autore. Nel caso in cui ciò sia necessario per la propria attività lavorativa, l'utente è tenuto ad attivare il processo di richiesta verso il proprio Responsabile;
    - il cui contenuto sia contrario a norme di legge.
- Tutte le modifiche alla configurazione delle stazioni di lavoro possono essere effettuate unicamente da soggetti espressamente e formalmente autorizzati dalla CCIAA. Il personale non è autorizzato a modificare per nessun motivo qualsiasi stazione di lavoro presente presso l'ente e tanto meno la postazione di lavoro assegnata.
- A titolo esemplificativo, ma non esaustivo, sono considerate modifiche del sistema:
  - modificare i collegamenti di rete esistenti;
  - 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 CCIAA;
  - aprire la struttura esterna (case) dell'elaboratore e procedere alla modifica (eliminazione o aggiunta) di componenti dello stesso;
  - 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.
- Le cartelle presenti sui server (anche virtuali e in cloud) utilizzati dalla CCIAA 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 salvato, nemmeno per brevi periodi, in queste unità. Su tali unità vengono svolte attività di backup.
- 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.
- Con regolare periodicità ciascun utente deve provvedere alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili o su cui siano attive regole di data retention.
- Ciascun dipendente deve delegare per iscritto un altro lavoratore ad accedere ai dati del proprio personal computer nel caso in cui, durante la propria assenza, ciò si renda indispensabile ed indifferibile per esclusiva

necessità di operatività o sicurezza o per improrogabili necessità legate all'attività lavorativa. A tale scopo ogni utente deve consegnare al lavoratore da lui delegato una busta chiusa contenente le proprie credenziali di accesso avendo cura di sostituirla ogni volta che esse vengono cambiate. (rif).

- Il lavoratore delegato, appurato che non è possibile l'intervento diretto da parte del Dipendente, accede ai dati e alle procedure su richiesta e alla presenza del dirigente o del proprio Responsabile di ufficio. Dell'attività compiuta è redatto apposito verbale a cura del dirigente/responsabile che ne informa il dipendente alla prima occasione utile. Nel caso in cui anche il lavoratore delegato non sia presente, il dirigente di settore/responsabile procede con le modalità indicate di seguito. Di tale attività è redatto apposito verbale a cura del dirigente/responsabile ed è informato l'utente alla prima occasione utile.

## *Art. 6 - SCELTA, USO, MODIFICA E CUSTODIA DELLE CREDENZIALI DI AUTENTICAZIONE*

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user-id), associato ad una parola chiave (password) riservata che dovrà essere custodita con la massima attenzione e mai divulgata.

La parola chiave che l'utente deve impostare al primo accesso alla rete, deve rispettare le seguenti condizioni:

- Composta da almeno 8 caratteri
- Contenere caratteri di almeno tre delle seguenti categorie:
  - Lettere MAIUSCOLE
  - Lettere minuscole
  - Numeri
  - Caratteri speciali (!, $, £, &, %, ecc.)
- Non contenere alcun riferimento o essere banale e facilmente riconducibile all'utilizzatore (data di nascita, cognome o nome, nome del cane, del paese di origine, di un congiunto, squadra di calcio, ecc)
- Prevedere che la password assegnata o forzata debba necessariamente essere sostituita al primo accesso. Ciò per costringere l'utilizzatore a definire immediatamente una nuova password di cui solo lui è a conoscenza

Non deve essere inviato alcun messaggio (di posta elettronica o cartaceo o sms) che contenga la password o riferimenti alla stessa, per evitare che altri soggetti non autorizzati ne vengano accidentalmente a conoscenza.

A titolo meramente esemplificativo, potrebbero essere password soddisfacentemente sicure:

- parole che non contengono nomi propri o di familiari, date di nascita, anagrammi e cose simili;
- parole facilmente digitabili sulla tastiera (ma di complessa formulazione) per ridurre al minimo il tempo di digitazione ed evitare che la stessa possa essere spiata da terzi nelle vicinanze;
- parole che compongono una frase, debitamente sintetizzata

Altro accorgimento è quello di evitare di utilizzare la stessa password per autenticarsi su sistemi interni ed esterni alla rete informatica del Titolare, come ad esempio l'accesso al proprio conto corrente bancario e ad altre attività legate o non legate all'ambito lavorativo.

Non conservare la/le password sul proprio cellulare, o su tablet, o su bigliettini nei cassetti, ecc.

Se qualcuno insiste per conoscere la parola chiave, dapprima fare riferimento a questo Disciplinare e poi informare immediatamente l'Amministratore di Sistema o il proprio superiore gerarchico.

Se si ha il minimo sospetto che la propria password possa essere stata compromessa o trafugata, bisogna provvedere immediatamente alla sostituzione della stessa riferendo l'accaduto al proprio Responsabile. Qualora si abbia il sospetto di una violazione dei dati e quindi di *Data Breach*, informare tempestivamente il privacy manager o il DPO o il Segretario Generale.

Gli stessi criteri nella scelta e nell'uso delle credenziali di accesso devono essere rispettati dal personale autorizzato all'inserimento di contenuti all'interno delle pagine web del sito istituzionale dell'Ente.

## *Art. 7 - UTILIZZO DELLA RETE INTERNET E LA NAVIGAZIONE*

- 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, salvo che tale uso sia motivato da ragioni di urgenza o di necessità. È in ogni caso vietato l'uso reiterato e prolungato per fini personali.

- È vietato accedere alla rete e ai 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.
- È altresì vietato:
  - scaricare e/o installare software non espressamente autorizzati dalla CCIAA;
  - scaricare e/o usare materiale informatico non direttamente attinenti all'esercizio dell'attività lavorativa;
  - scaricare e/o usare materiale informatico il cui contenuto (a mero titolo esemplificativo: software, testo, audio e video) sia tutelato dal diritto di autore;
  - partecipare a forum di discussione on line, a chat, utilizzare sistemi di chiamata o di video chiamata, ecc. per ragioni non direttamente attinenti o connesse all'attività lavorativa;
  - navigare in internet su siti contrari a norme di legge; a tal fine si raccomanda di attivare le funzioni di blocco dei pop-up presenti su ogni browser aggiornato e che impediscono l'attivazione automatica di eventuali link a siti malevoli;
  - effettuare ogni genere di transazione finanziaria per fini personali;
  - installare e utilizzare strumenti per lo scambio di dati attraverso internet con metodologia *Peer to Peer* (ad es., eMule, kazaa, bittorrent etc.) indipendentemente dal contenuto dei file scambiati o strumenti di *instant messaging*, come What's App On Line non idonei ad attività di condivisione professionale sicura di dati.
- In un'ottica preventiva la CCIAA utilizza, nell'ambito dei servizi per la gestione della rete messi a disposizione da InfoCamere, dei sistemi di filtraggio automatico posti sugli apparati che governano la rete che provvedono a bloccare l'accesso a un insieme di siti web identificati come pericolosi o appartenenti a categorie specifiche non legate alle necessità di tipo operativo della Camera. Tale attività viene svolta automaticamente e il rigetto della navigazione richiesta non dà seguito a segnalazioni. I dati della navigazione internet vengono, comunque, salvati come previsto dalla legge da parte di InfoCamere che li conserva in un apposito bunker a disposizione delle eventuali richieste che dovessero giungere dall'Autorità Giudiziaria a fronte di eventi che giustifichino l'intervento di quest'ultima.
- L'utilizzo della rete da parte di soggetti esterni all'Ente deve avvenire solo tramite l'assegnazione di apposita user e password temporanea e non deve prevedere assolutamente la concessione da parte del Dipendete delle sue credenziali di accesso.

## *Art. 8 - UTILIZZO DELLA POSTA ELETTRONICA*

- La CCIAA mette a disposizione di ogni lavoratore il servizio di posta elettronica, assegnando a ciascuno di essi caselle di posta istituzionali per fini esclusivamente lavorativi. Al fine di agevolare lo svolgimento dell'attività lavorativa, la CCIAA rende disponibili indirizzi di posta elettronica condivisi tra più utenti (caselle di posta istituite per singole unità organizzative o di gruppi di lavoro) affiancandoli a quelli individuali. Quest'ultima modalità di lavoro è quella da privilegiare al fine di inviare comunicazioni che impegnino, sia verso l'interno che all'esterno, l'Ente rispetto ad azioni e/o procedure.
- L'indirizzo di posta elettronica messo a disposizione dalla CCIAA, contraddistinto dalla presenza del nome di dominio " ctrgsr.camcom.it", costituisce uno strumento di lavoro ed il suo utilizzo è consentito unicamente per finalità attinenti o comunque connesse allo svolgimento dell'attività lavorativa.
- È escluso, di regola, l'uso per scopi privati e/o personali, ad eccezione dei casi d'urgenza e di necessità e comunque non in modo continuativo e con alta frequenza.
- L'accesso e la riservatezza della posta elettronica sono garantiti dalla necessità di disporre di idonee credenziali di autenticazione per accedere alla stessa. La password dell'account di posta elettronica è scelta e registrata dall'utente nel rispetto dei criteri e delle regole indicati nel presente Disciplinare.
- Al fine di un corretto utilizzo della posta elettronica è vietato:
  - Inviare materiale riservato di mero utilizzo della Camera o documenti pubblici che non rispondano ad una richiesta formale e tracciata effettuata da un soggetto avente diritto;
  - 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 CCIAA o a terzi nonché messaggi a catena e/o spam;
  - scambiare messaggi impersonando un mittente diverso da quello reale;
  - 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;
- aprire messaggi di posta o allegati di tipo eseguibile o con macro presenti, salvo il caso di certezza assoluta dell'identità del mittente e della sicurezza del messaggio.

- 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 essere personalizzato dal personale e potrà indicare l'indirizzo di posta elettronica di un altro lavoratore al quale il mittente può fare riferimento in caso di comunicazioni urgenti. Nel messaggio è opportuno evitare di dare indicazioni ai soggetti che scrivono del periodo di assenza del Dipendente onde evitare che questa informazione possa essere utilizzata per compiere atti illeciti o dannosi nei confronti del Dipendente o dell'Ente.

- In caso di assenze prolungate dal lavoro non preventivamente programmate, l'utente attiva da remoto, se possibile, il sistema di risposta automatica della propria casella di posta elettronica.

- Il lavoratore delega per iscritto un altro lavoratore a verificare il contenuto dei messaggi a lui indirizzati e a inoltrare al dirigente/funzionario di settore o al responsabile da quest'ultimo indicato quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa nel caso in cui, durante la propria assenza, ciò si renda indispensabile e indifferibile per esclusiva necessità di operatività o sicurezza o per improrogabili necessità legate all'attività lavorativa. Il lavoratore delegato provvede su richiesta e alla presenza del dirigente/funzionario. Di tale attività è redatto apposito verbale a cura del dirigente/responsabile dell'area ed è informato il lavoratore alla prima occasione utile. (rif)

- Nel caso in cui anche il lavoratore delegato non sia presente, il dirigente di settore o il soggetto da lui incaricato richiede all'Ufficio Affari del Personale di contattare, in sua presenza, il lavoratore per le vie brevi. Il lavoratore effettuerà senza indugio l'accesso al suo servizio di posta elettronica per provvedere alla richiesta del dirigente/responsabile del servizio. Di tale attività è contestualmente redatto apposito verbale a cura del dirigente/responsabile.

- Nell'ipotesi in cui anche l'attività di cui al precedente punto 9 non dovesse avere esito positivo, il dirigente/funzionario responsabile del servizio potrà – con relazione motivata e solo ed esclusivamente in caso di assoluta urgenza e ad esigenze di natura indifferibile – chiedere che il Segretario Generale disponga la forzatura della password da parte dell'amministratore di sistema. Di tale attività è contestualmente redatto apposito verbale a cura del dirigente/responsabile. L'autorizzazione a tale attività dovrà essere contenuta nella delega di cui al punto 9.

### *Art. 9 - Disposizioni relative alle ipotesi di cessazione del rapporto di lavoro*

Alla data di conclusione del rapporto di lavoro, l'Ufficio Personale comunica l'interruzione del rapporto di lavoro al Coordinamento Informatico, indicandone la causa di cessazione (conclusione del rapporto di lavoro o collocamento in quiescenza). Entro 8 giorni dal ricevimento di detta comunicazione, il Coordinamento Informatico procede all'estinzione dei permessi attribuiti al dipendente. Tale termine può essere prorogato su richiesta del responsabile del servizio o su esplicita comunicazione del Segretario Generale, al fine di effettuare l'accesso ai file contenuti per l'esecuzione di eventuali backup. Trascorsi ulteriori 30 giorni, il Coordinamento Informatico procederà, previa comunicazione al Segretario Generale e al responsabile del servizio nel quale era assegnato il dipendente, alla cancellazione definitiva della cartella di rete assegnata in modalità esclusiva e non sarà possibile recuperare i dati in essa contenuti, alla revoca delle user-id ed alla disabilitazione delle relative abilitazioni.

Con gli stessi termini sopra indicati viene disposta la dismissione dell'account di posta elettronica, che comporta l'irrimediabile cancellazione di qualsiasi dato ivi contenuto, con contestuale adozione di un messaggio automatico volto ad informarne i terzi e a indicare un account alternativo per contattare l' Ente.

In ragione della natura irreversibile della procedura, nei 15 giorni precedenti la data di pensionamento, il dipendente viene invitato al salvataggio/consegna al Responsabile d'ufficio di tutti i file inerenti i processi e le attività di sua competenza.

Infine, le relative apparecchiature informatiche in uso ai medesimi, ove utilizzabili, possono essere formattate e rese disponibili in caso di necessità oppure, se non diversamente collocabili, discaricate dall'inventario e disposte per lo smaltimento.

### *Art. 9 - PROTEZIONE ANTIVIRUS*

- Il sistema informatico dell'Ente è protetto, in modo centralizzato, da sistemi antivirus gestiti dalla Società InfoCamere S.c.p.A. In ogni caso, l'utente deve tenere comportamenti tali da ridurre il rischio di attacco da virus/ malware ecc.

- Qualora l'utente dovesse rilevare situazioni anomale o presenza di virus, lo stesso dovrà, senza ulteriore ritardo,

informare prontamente il coordinatore informatico o il referente tecnico, oltre che il proprio Responsabile di Area, e sospendere ogni ulteriore elaborazione, al fine di ridurre al minimo gli effetti di un attacco ai sistemi.

- Ove previsto l'utilizzo di dispositivi di memorizzazione esterna (a titolo esemplificativo, chiavette USB, hard disk esterni, ecc.), l'utente dovrà verificare, prima del suo utilizzo e mediante il programma antivirus, l'integrità dello strumento stesso. Qualora, invece, il sistema di protezione da virus evidenziasse una possibile infezione (corruzione), l'utente dovrà sospendere immediatamente l'utilizzo ed informare il Coordinatore informatico, il Referente Tecnico e il Responsabile dell'Area.
- Tutti i device presenti presso l'Ente, che si collegano alla rete, devono essere dotati di antivirus costantemente aggiornato e allineato all'ultima versione d'uso; questo criterio deve essere applicato anche per i device utilizzati episodicamente (sale conferenza, demo, ecc) in quanto il loro collegamento alla rete e, magari, anche l'uso da parte di soggetti esterni che partecipano ad incontri e/o eventi può mettere a rischio la sicurezza complessiva del sistema.

## *Art. 10 -GESTIONE BACK UP*

- La CCIAA favorisce, in un'ottica di riservatezza, integrità e disponibilità dei dati, meccanismi di back up utili a garantire la continuità operativa delle attività istituzionali. Per tale ragione, si evidenzia che le uniche Aree autorizzate al salvataggio sono le cartelle condivise presenti sui Server o l'utilizzo in maniera sistemica di macchine virtuali (VDI).
- Ogni utente può richiedere al Coordinatore Informatico o al Referente Tecnico la creazione di una propria cartella personale con lo scopo di garantire la conservazione sicura dei propri documenti (documenti in fase di lavorazione) in relazione alla specifica attività espletata all'interno dell'Ente.
- Esiste, altresì, un'area dedicata allo scambio di dati, accessibile agli utenti autenticati. Tali spazi sono configurati al fine di garantire la sicurezza e la custodia di dati, impedendo quindi accessi non consentiti, assicurandone la disponibilità in casi di emergenza e sottoposti a back up.
- Si ricorda che le attività di salvataggio sono garantite mediante sistemi messi a disposizione dalla Società InfoCamere S.c.p.A.
- Per tale ragione, ogni salvataggio in locale è vietato e, comunque, configura situazione di responsabilità in capo al dipendente.
- In caso di involontaria cancellazione di un documento contenente dati personali all'interno di cartelle su Server o di involontaria corruzione del file, l'utente dovrà, senza ritardo, rivolgersi al Referente tecnico che, in caso di non recupero del file, dovrà valutare, di concerto con il Responsabile per la protezione dati personali (DPO), l'effettiva perdita di dati personali e, quindi, attivare la prevista procedura *Data Breach*.
- Qualora un dipendente disponga di un notebook in dotazione e di proprietà dell'Ente, sul medesimo verranno attivate procedure di sincronizzazione automatica dei file e di aggiornamenti (anche di antivirus), previa consultazione e specifica autorizzazione del Segretario generale che ne dà indicazione al Referente Tecnico, anche in armonia alle disposizioni del presente disciplinare. Se ne desume che, l'affidamento del device comporta, per il dipendente, assunzione di responsabilità in caso di perdita, furto o incuria con relativa, possibile, compromissione dei dati personali in esso contenuti.

## *Art. 11 - UTILIZZO DEGLI STRUMENTI DI TELEFONIA FISSA E MOBILE, MOBILE DEVICES, FOTOCOPIATRICI E FAX*

- Gli strumenti di telefonia (sia fissa che mobile) messi a disposizione dalla CCIAA del Sud Est Sicilia costituiscono strumento di lavoro e ne è consentito l'utilizzo unicamente per finalità attinenti o comunque connesse all'esercizio dell'attività lavorativa.
- È escluso, di regola, l'uso per scopi privati e/o personali, salvo che tale uso sia motivato da ragioni di urgenza e di necessità. È in ogni caso vietato l'uso reiterato e prolungato per fini personali. (rif)
- Il dipendente assegnatario di uno smartphone, mobile device, ecc. è responsabile del suo utilizzo e della sua corretta custodia. Anche per questi strumenti è vietato l'utilizzo per natura personale e/o pertinente all'attività lavorativa, come, ad esempio, l'installazione di app non autorizzate, il salvataggio di foto/video/messaggi, ecc. Agli stessi, inoltre, devono essere applicate le stesse regole previste per l'uso degli altri device quali ad esempio: blocco dello schermo, antivirus attivo, effettuazione degli aggiornamenti, ecc.
- L'utilizzo di strumenti multifunzione, come fotocopiatrici, scanner, fax, è vietato per finalità di carattere

personale, salvo diversa esplicita autorizzazione da parte del proprio Responsabile di Area.

### *Art. 12 - USO, CUSTODIA E DISMISSIONE DI SUPPORTI RIMOVIBILI*

- Al fine di ridurre la minimo di perdita o distruzione di dati personali, è vietata la copia su supporti rimovibili, quali chiavette USB, hard disk, DVD, ecc. Allo stesso modo, non è consentito l'utilizzo di supporti di proprietà del dipendente, salvo autorizzazioni specifiche del proprio Responsabile di Area, non prima di aver analizzato l'integrità degli strumenti.
- Ove nello svolgimento della propria attività lavorativa risultasse necessario effettuare copia di dati, sarà obbligatorio utilizzare solo supporti rimovibili forniti dall'Ente e autorizzati dall'Amministratore di Sistema e/o dal proprio Responsabile di Area. Sarebbe opportuno che i supporti fossero formattati e privi di altri file che possano risultare infetti da virus.
- Ove possibile, i dati memorizzati dovranno essere protetti da cifratura o da altra misura equivalente.
- In ogni caso, i supporti rimovibili contenenti dati personali non devono essere lasciati incustoditi, mettendo in atto idonee procedure di conservazione, soprattutto qualora si tratti di dati meritevoli di ulteriore protezione in virtù della tipologia di dati personali (ad es., dati particolari o giudiziari ex artt. 9 e 10 del GDPR).
- Nel caso in cui il supporto rimovibile dovesse essere trafugato, smarrito, rubato, il dipendente responsabile, in adesione alla procedura adottata internamente all'Ente relativa alla violazione dei dati personali (c.d. *data breach*), dovrà informare immediatamente l'Amministratore di Sistema, il Responsabile per la protezione dei dati (RPD/DPO), i quali provvederanno, nel caso, a coinvolgere il Segretario Generale.
- Con riferimento alla dismissione dei supporti sopra richiamati, si rimanda a quanto stabilito in normative, linee guida e circolari vigenti al momento della dismissione ed eventualmente contenute in procedure in uso presso l'Ente.

### *Art. 13 - ISTRUZIONI SULL'UTILIZZO DEI SOCIAL NETWORK*

- I canali social della CCIAA vengono utilizzati per la divulgazione delle attività dell'Ente attraverso la pubblicazione di notizie relative a progetti/iniziative/convegni, comunicati e rassegne stampa, condivisione di iniziative locali, ecc.
- Il dipendente o professionista esterno preposto all'attività di gestione dell'account istituzionale su piattaforme social e all'implementazione delle relative pagine, deve operare ispirato dai principi di diligenza e correttezza, utilizzando altresì un linguaggio rispettoso durante le comunicazioni avviate con l'utenza.
- I canali social dell'Ente non possono essere utilizzati per affrontare argomenti personali. Per tale ragione non è ammessa la pubblicazione di contenuti e/o opinioni di carattere strettamente personale, né qualunque forma di pubblicità o di promozione di interessi privati. Sono parimenti vietati la pubblicazione di contenuti che violino il diritto d'autore o altrimenti illegali, offensivi o violenti, nonché l'utilizzo non autorizzato di marchi registrati, ecc.
- Nel rispetto delle regole sopra elencate nonché dei principi di pertinenza e non eccedenza, il soggetto preposto alla gestione delle pagine social potrà fornire informazioni e dare risposta alle richieste degli utenti.
- Si rammenta che l'utilizzo dei canali social in violazione delle prescrizioni dettate dall'Ente, può danneggiare anche gravemente l'immagine e la reputazione dell'Ente e, di conseguenza, delle figure professionali che vi lavorano; può esporre a sospensioni o cancellazioni del profilo, nel caso non si rispettino i termini del servizio contratti con il social media stesso; può esporre anche a danni diretti come richieste di risarcimento.

### *Art. 14 - TRATTAMENTO DATI SENZA L'AUSILIO DI STRUMENTI INFORMATICI*

- Gestione e conservazione fascicoli:
  - È buona regola evitare di detenere, oltre il periodo necessario alla fase istruttoria, documenti, stampe, fotocopie, fascicoli contenenti dati personali sulle scrivanie degli Uffici camerali, soprattutto quando questi fossero aperti al pubblico.
  - I fascicoli contenenti dati personali devono essere conservati in archivi/armadi chiusi a chiave e devono essere prelevati per il solo tempo necessario allo svolgimento dei propri compiti.
  - Al fine di ridurre il rischio di perdite e/o manomissioni dei fascicoli di archiviazione, evitare di asportare singoli documenti da un fascicolo, prelevando per il tempo necessario alla consultazione l'intero fascicolo/unità

archivistica all'interno del quale il documento è inserito.

- Ciascun dipendente deve preoccuparsi di non mantenere incustodita la documentazione, soprattutto laddove i luoghi siano accessibili a soggetti non autorizzati.
- Lo smarrimento o il furto di informazioni potrebbero configurare violazione dei dati personali (c.d. data breach) e per tale motivo l'evento deve essere comunicato ai referenti della procedura.
- I fascicoli contenenti categorie di dati particolari (ex art. 9 del GDPR) o dati relativi a condanne penali o reati (ex art. 10 del GDPR) devono essere conservati adottando tutte le idonee misure di sicurezza ed accessibili unicamente al personale espressamente autorizzato.
- In caso di temporaneo allontanamento dall'Ufficio e comunque alla fine della giornata lavorativa, è onere di ciascun dipendente assicurarsi che i documenti contenenti dati personali e informazioni riservate siano correttamente custoditi ed archiviati affinché gli stessi non risultino direttamente o indirettamente accessibili a terzi non autorizzati.
- Si invita ad evitare la stampa di documenti digitali qualora non sia essenziale ai fini del trattamento. Ove possibile, si invita ad effettuare la scansione dei documenti cartacei ed archiviarli digitalmente.
- È necessario rimuovere immediatamente ogni foglio stampato da una stampante o da un'apparecchiatura fax, per evitare che siano prelevati o visionati da soggetti non autorizzati.

- Gestione e conservazione chiavi archivi/armadi/cassetti:
  - Ogni dipendente a cui sono state affidate chiavi di archivi o possessore di chiavi di uffici contenenti dati dovrà prestare attenzione a che le stesse non siano lasciate incustodite nelle serrature, non siano messe a disposizione di estranei. In caso di perdita o furto sarà obbligatorio dare immediato allarme ai referenti della procedura Data Breach prevista presso l'Ente richiedendo la sostituzione di serrature e chiavi.

- Le procedure di scarto degli archivi cartacei devono avvenire, nel rispetto della relativa normativa vigente, mediante distruzione fisica in modo da evitare che soggetti non autorizzati possano accedere ad informazioni riservate o, comunque, non di loro competenza. Al di fuori di tale procedura, è fatto obbligo al personale dipendente di assicurare la completa e definitiva distruzione dei documenti contenenti dati personali utilizzando gli strumenti a tal fine messi a disposizione della Camera. In particolare, è fatto assoluto divieto di cestinare documenti integri.

## Sezione III - CONTROLLI

### *Art. 15 - MODALITA' DI EFFETTUAZIONE DEI CONTROLLI*

- La CCIAA si riserva la facoltà, nel rispetto della tutela del diritto alla riservatezza e del principio di proporzionalità e non eccedenza, di svolgere dei controlli sugli strumenti informatici e di telefonia assegnati al personale.
- I controlli non potranno mai svolgersi direttamente e in modo puntuale, ma dovranno preliminarmente essere compiuti su dati anonimi aggregati, riferiti all'intera struttura organizzativa o a sue unità operative anche attraverso specifiche verifiche informatiche.
- 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 ed 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.
- Qualora continuino i comportamenti non conformi, sono effettuati controlli nominativi o su singoli dispositivi e postazioni e, a seconda della gravità della violazione riscontrata, saranno applicate le sanzioni indicate in precedenza.
- In ogni caso non sono ammessi, su base individuale, controlli casuali, prolungati, costanti o indiscriminati.
- 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 in violazione dell'art. 4 L. 300/1970.-

- Resta sempre salvo l'obbligo dell'Ente di comunicare e di trasmettere tutti i dati richiesti (es. file log, tracce informatiche e quant'altro) contenenti le prove informatiche relative ai comportamenti illeciti dei dipendenti alle Autorità Giudiziarie competenti che ne facciano richiesta nei termini e secondo la normativa vigente.
-

## Sezione IV - DISPOSIZIONI FINALI

### *Art. 16 - INFORMATIVA E NOMINA SOGGETTI AUTORIZZATI*

- 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 2016/679 e del D. Lgs. 196/03 come modificato dal D. Lgs. 101/18 nonché la nomina a soggetto autorizzato al trattamento dei dati personali.

### *Art. 17 - DISPOSIZIONI FINALI*

- Il presente Disciplinare entra in vigore dalla data di pubblicazione della determinazione del Segretario Generale che ne approva il contenuto e sostituisce ed abroga eventuali procedure o disposizioni con esso incompatibili.
- Copia del Disciplinare è trasmesso al personale camerale e ai collaboratori presenti alla Camera per effettuazione di determinati progetti e/o servizi a tempo determinato.
-

SOMMARIO