Camera di commercio, industria, artigianato e agricoltura di Cagliari

Disciplinare per il corretto utilizzo degli strumenti informatici, della rete informatica e telematica (internet e posta elettronica) e del sistema di telefonia fissa e mobile

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

Approvato con deliberazione della Giunta camerale n.56 del 30 luglio 2019

Camera di Commercio
Cagliari

INDICE

PREMESSA 3

Sezione I - DISPOSIZIONI GENERALI

Art. 1 – FINALITA 4

Art. 2 – PRINCIPI GENERALI 4

Art. 3 – DESTINATARI E CAMPO DI APPLICAZIONE 5

Sezione II

USO DEGLI STRUMENTI INFORMATICI, TELEMATICI E DI TELEFONIA

Art. 4 – CRITERI GENERALI DI UTILIZZO 7

Art. 5 – UTILIZZO DEGLI STRUMENTI INFORMATICI 7

Art. 6 – UTILIZZO DELLA RETE INFORMATICA INTERNA 8

Art. 7 – REGOLE COMPORTAMENTALI 9

Art. 8 – UTILIZZO DELLA RETE INTERNET 12

Art. 9 – UTILIZZO DELLA POSTA ELETTRONICA 12

Art. 10 – UTILIZZO DEGLI STRUMENTI DI TELEFONIA FISSA E MOBILE 14

Sezione III

CONTROLLI

Art. 11 – MODALITA' DI EFFETTUAZIONE DEI CONTROLLI 15

Art. 12 – EVENTUALI CONTROLLI SUI VEICOLI 16

Sezione IV

DISPOSIZIONI FINALI

Art. 13 – NORMA DI RINVIO 17

Art. 14 – DISPOSIZIONI FINALI 18

PREMESSA

Gli strumenti informatici, della rete informatica e telematica (internet e posta elettronica) e del sistema di telefonia fissa e mobile, che identificano nel loro complesso le Tecnologie della Informazione e Comunicazione (TIC), rappresentano, ormai da diverso tempo, lo strumento di lavoro principale a disposizione delle pubbliche amministrazioni per perseguire le proprie finalità istituzionali.

Al riguardo, l'art. 12 del Codice dell'Amministrazione Digitale (D.Lgs. 7 marzo 2005, n. 82, come modificato, da ultimo, dal D. Lgs. 13 dicembre 2017, n. 217) impartisce alle pubbliche amministrazioni precise linee di condotta, stabilendo quanto segue: "*Le pubbliche amministrazioni nell'organizzare autonomamente la propria attività utilizzano le tecnologie dell'informazione e della comunicazione per la realizzazione degli obiettivi di efficienza, efficacia, economicità, imparzialità, trasparenza, semplificazione e partecipazione nel rispetto dei principi di uguaglianza e di non discriminazione, nonché per l'effettivo riconoscimento dei diritti dei cittadini e delle imprese di cui al presente Codice in conformità agli obiettivi indicati nel Piano triennale per l'informatica nella pubblica amministrazione di cui all'articolo 14-bis, comma 2, lettera b). 1-bis. Gli organi di Governo nell'esercizio delle funzioni di indirizzo politico ed in particolare nell'emanazione delle direttive generali per l'attività amministrativa e per la gestione ai sensi del comma 1 dell'articolo 14 del decreto legislativo 30 marzo 2001, n. 165, e le amministrazioni pubbliche nella redazione del piano di performance di cui all'articolo 10 del decreto legislativo 27 ottobre 2009, n. 150, dettano disposizioni per l'attuazione delle disposizioni del presente Codice. 1-ter. I dirigenti rispondono dell'osservanza ed attuazione delle disposizioni di cui al presente Codice ai sensi e nei limiti degli articoli 21 e 55 del decreto legislativo 30 marzo 2001, n. 165, ferme restando le eventuali responsabilità penali, civili e contabili previste dalle norme vigenti. L'attuazione delle disposizioni del presente Codice è comunque rilevante ai fini della misurazione e valutazione della performance organizzativa ed individuale dei dirigenti. 2. Le pubbliche amministrazioni utilizzano, nei rapporti interni, in quelli con altre amministrazioni e con i privati, le tecnologie dell'informazione e della comunicazione, garantendo l'interoperabilità dei sistemi e l'integrazione dei processi di servizio fra le diverse amministrazioni nel rispetto delle Linee guida. 3. Le pubbliche amministrazioni operano per assicurare l'uniformità e la graduale integrazione delle modalità di interazione degli utenti con i servizi informatici, ivi comprese le reti di telefonia fissa e mobile in tutte le loro articolazioni, da esse erogati, qualunque sia il canale di erogazione, nel rispetto della autonomia e della specificità di ciascun erogatore di servizi. 3-bis. I soggetti di cui all'articolo 2, comma 2, favoriscono l'uso da parte dei lavoratori di dispositivi elettronici personali o, se di proprietà dei predetti soggetti, personalizzabili, al fine di ottimizzare la prestazione lavorativa, nel rispetto delle condizioni di sicurezza nell'utilizzo.*"

La Camera di Commercio Industria Artigianato e Agricoltura di Cagliari (di seguito anche CCIAA o Camera) promuove, dunque, l'utilizzo della rete informatica e telematica, di internet e della posta elettronica quali strumenti atti a migliorare la qualità delle prestazioni lavorative al fine di incrementare l'efficienza operativa e garantire un miglior servizio ai cittadini.

La Camera, inoltre, intende assicurare la funzionalità e il corretto impiego di tali risorse definendo un apposito Disciplinare interno, volto, da un lato, a sensibilizzare il personale camerale, i collaboratori, nonché gli organi politici, a un uso delle tecnologie dell'informazione e della comunicazione coerente con l'attività lavorativa, e dall'altro, ad assicurare il giusto contemperamento tra le esigenze organizzative della Camera, quale datore di lavoro, e quelle di tutela della riservatezza dei dati personali dei lavoratori, nel rispetto della vigente normativa in materia di privacy, di cui al Regolamento UE 679/2016, al Codice in materia di protezione dei dati personali (D.Lgs. del 30 giugno 2003, n.196 – Codice Privacy) e ai Provvedimenti del Garante per la protezione dei dati personali (Garante Privacy), con particolare riferimento alla deliberazione n.13 del 1 marzo 2007).

Sezione I
DISPOSIZIONI GENERALI

Art. 1
FINALITA'

1. Il presente Disciplinare è diretto a dotare la CCIAA di Cagliari di una disciplina interna in grado di garantire l'efficienza, l'efficacia e l'economicità dei processi lavorativi dell'Amministrazione nel rispetto della normativa vigente in materia di tutela della privacy, attraverso la regolamentazione dell'uso delle risorse tecnologiche e informatiche e la responsabilizzazione dei lavoratori/utilizzatori in merito all'eventuale uso delle stesse in modo non coerente con l'attività lavorativa, con gli interessi dell'ente e con le norme che disciplinano il lavoro nelle pubbliche amministrazioni.
2. Il Disciplinare, in particolare, è diretto a:

a) individuare 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/utilizzatori e del diritto alla loro riservatezza;

b) informare coloro che utilizzano 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 e 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 anche con riguardo ai danni all'immagine dell'Amministrazione, rendendoli consapevoli che ogni accesso alle tecnologiche informatiche può essere facilmente ricondotto alla persona che lo ha effettuato;
- definire in maniera trasparente le modalità di effettuazione dei controlli e le conseguenze, anche disciplinari, di un utilizzo indebito.

Ai fini del presente punto b), il contenuto del Disciplinare integra l'informativa già fornita ai dipendenti e ai collaboratori ai sensi dell'art. 13 del Regolamento UE n. 679/2016, con Disposizione Gestionale n. 9 del 27 maggio 2019 del Segretario Generale quale Delegato Privacy, ai sensi de Modello organizzativo Privacy adottato dalla Camera di commercio con la delibera della Giunta camerale n. 36 del 14 maggio 2019, e tutte le informative che si forniranno in futuro.

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 alla Camera. Tali strumenti sono messi a disposizione degli organi politici, del personale, degli addetti che operano in outsourcing e per coloro che per lo svolgimento dell'attività lavorativa in ambito camerale siano stati espressamente autorizzati. 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. I soggetti di cui al precedente comma, dopo aver ricevuto le relative istruzioni, e comunque anche a prescindere da queste, sulla base dei principi di diligenza, correttezza e buona fede, sono responsabili, sotto i profili amministrativi civili e penali, del corretto uso degli strumenti informatici, telematici e di telefonia e del contenuto delle comunicazioni effettuate, e rispondono 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 e 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.
6. La Camera cura l'adeguata formazione del personale sull'utilizzo degli strumenti informatici, telematici e di telefonia anche in relazione alla tutela dei dati personali.

Art. 3
DESTINATARI E CAMPO DI APPLICAZIONE

1. Il presente Regolamento definisce le regole e gli standard di comportamento che dovranno rispettare le seguenti categorie di soggetti utilizzatori/utenti degli strumenti TIC che operano all'interno della Camera:

- i dirigenti;
- il personale dipendente dell'Amministrazione (a tempo indeterminato e a tempo determinato);
- i collaboratori esterni;
- le unità lavorative in servizio presso l'Ente con altre forme di rapporto di lavoro;
- i soggetti che svolgono tirocini formativi e di orientamento;
- tutti i soggetti autorizzati ad accedere anche temporaneamente alla rete camerale e agli strumenti informatici, telematici e di telefonia per lo svolgimento della propria attività lavorativa, o in quanto si trovano, per motivi diversi, a operare all'interno dell'Amministrazione.

2. Il Disciplinare si applica anche ai componenti degli Organi Politici camerali, ma restano escluse dal suo campo applicativo, al fine di preservare il libero esercizio delle funzioni politiche e sindacali, le strumentazioni individuali messe a disposizione di tali Organi, nonché l'apposita strumentazione messa a disposizione della Rappresentanza Sindacale Aziendale (RSA).
3. Il Disciplinare regola l'utilizzo di tutti gli strumenti informatici, telematici e di telefonia a disposizione degli Uffici/Servizi, siano essi impiegati in modalità indipendente o collegati alla rete informatica camerale. Esso deve essere conosciuto e applicato da tutti i Servizi dell'Amministrazione.

4. A tal proposito, il Disciplinare:

- è parte integrante del contratto individuale di lavoro o dell'atto di incarico o di instaurazione della collaborazione e deve essere, pertanto, portato a personale conoscenza di tutti i dipendenti e di coloro che hanno in atto una collaborazione o un incarico, i quali sottoscriveranno apposita dichiarazione che ne attesti la presa visione e accettazione; con riferimento ai rapporti di lavoro o alle collaborazioni o incarichi di nuova costituzione, è consegnato in concomitanza con la sottoscrizione del contratto o dell'atto, quale allegato;
- è, altresì, parte integrante del Codice di comportamento della Camera ed è reso fruibile, tramite pubblicazione sul sito istituzionale dell'Amministrazione: a tutti i dipendenti con valenza, a tutti gli effetti, ai sensi dell'art. 55, comma 2, del D. Lgs. 165/2001, di affissione all'ingresso della sede di lavoro, atteso che tutti i lavoratori hanno accesso alla rete internet dalla propria stazione di lavoro; ai componenti degli Organi Politici; a tutti i collaboratori e incaricati esterni; la pubblicazione deve avvenire nella sezione Amministrazione Trasparente – Disposizioni Generale – Statuto e Regolamenti e Codice disciplinare e di condotta del sito istituzionale e nella Intranet dell'Amministrazione; il Responsabile del procedimento di trasmissione e informazione è il Responsabile del Servizio competente in materia di risorse umane;
- integra, infine, le specifiche istruzioni impartite, in materia di trattamento dei dati personali, ai sensi del Regolamento UE n. 679/2016, dal Segretario Generale quale Delegato Privacy, con Disposizione Gestionale n. 10 del 4 giugno 2019, ai soggetti di cui al menzionato Modello organizzativo Privacy adottato dalla Camera di commercio con la delibera della Giunta camerale n. 36 del 14 maggio 2019.

5. La rete informatica, telematica e telefonica comprende:

- il complesso delle risorse infrastrutturali, nell'ambito delle quali rientra ogni personal computer (pc), stampante, scanner e strumentazione informatica in uso presso la Camera nelle componenti hardware (tutte le componenti "fisiche" del computer, quali: periferiche, parti elettriche, meccaniche, elettroniche ed ottiche) e software (i programmi e le procedure) e gli apparati elettronici collegati alla rete informatica camerale;
- i collegamenti fissi o mobili a internet e alla posta elettronica e gli apparati elettronici necessari;
- il patrimonio informativo digitale, che include le banche dati digitali e, in generale, il materiale e la documentazione prodotta tramite i suddetti strumenti;
- ogni apparecchiatura telefonica in uso presso l'Amministrazione, quali telefoni fissi, mobili, cellulari.

6. La vigilanza sul rispetto del Disciplinare da parte dei destinatari è esercitata, anche attraverso il ricorso a operazioni di backup (copia e conservazione dei dati archiviati nella memoria di massa del computer), nel rispetto della normativa vigente, dal Segretario Generale sulle aree dirigenziali e dai Dirigenti d'area sui Servizi assegnati e, nell'ambito del singolo Servizio, il controllo sugli utenti è affidato al relativo responsabile.

7. 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 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.

Sezione II

USO DEGLI STRUMENTI INFORMATICI, TELEMATICI E DI TELEFONIA

Art. 4
CRITERI GENERALI DI UTILIZZO

1. Premesso che, nell'ambito dei comportamenti da porre in essere con riferimento ai rapporti di lavoro, vigono i principi di diligenza e di fedeltà – artt. 2104 e 2105 del Codice Civile – e che gli stessi si applicano anche all'utilizzo delle risorse informatiche e telematiche, attraverso il presente Disciplinare si intende evitare che comportamenti consapevoli o inconsapevoli possano arrecare danni o creare minacce per l'Amministrazione.
2. È escluso qualsivoglia uso delle risorse informatiche e telematiche per scopi privati e/o personali, a eccezione dei casi d'urgenza e comunque a condizione che tale uso avvenga in modo non ripetuto o per periodi prolungati.
3. Come precisato, infatti, nella Direttiva della Presidenza del Consiglio dei Ministri 26 maggio 2009, n. 2, si può consentire l'utilizzo della rete per attività concernenti l'assolvimento di incombenze personali amministrative e/o burocratiche senza allontanarsi dal luogo di lavoro, (ad esempio, per effettuare adempimenti on line nei confronti di pubbliche amministrazioni e di concessionari di servizi pubblici, ovvero per tenere rapporti con istituti bancari e assicurativi). Tale modalità, purché contenuta nei tempi strettamente necessari allo svolgimento delle transazioni, ha, infatti, il vantaggio di contribuire a ridurre gli spostamenti delle persone e gli oneri logistici e di personale per l'amministrazione che eroga il servizio, favorendo, altresì, la dematerializzazione dei processi produttivi.
4. I soggetti che utilizzano le TIC camerali, destinatari del Disciplinare, devono rispettare la riservatezza dei dati e delle misure di accesso ai servizi e sono invitati a segnalare all'Amministrazione, nella figura del Segretario Generale, quale Delegato Privacy, o del Responsabile per la Protezione dei Dati (RPD) o del Responsabile del Servizio di appartenenza, eventuali violazioni della riservatezza delle quali venissero a conoscenza, nel rispetto del "Regolamento sulla procedura di gestione degli incidenti di sicurezza riguardanti i trattamenti di dati personali (data breach) svolti dalla Camera di commercio di Cagliari" adottato con delibera della Giunta camerale n. 51 del 25 giugno 2019 ed eventuali successivi aggiornamenti e modifiche.
5. La Camera si riserva la possibilità di configurare dei filtri o dei sistemi per prevenire operazioni che non rientrano nell'attività lavorativa. A titolo esemplificativo, può prevedere sistemi che impediscono l'upload (caricamento), ovvero l'accesso a specifici siti, inseriti in una cosiddetta blacklist, e/o il download (scaricamento) di file o software che hanno determinate caratteristiche legate alla tipologia dei dati o alla loro dimensione. Queste e altre misure preventive volte a ridurre il rischio di utilizzo improprio e potenzialmente dannoso, sono espressamente raccomandate dal Garante della Privacy nella Deliberazione 1 marzo 2007, n. 13 (G.U. n. 58 del 10 marzo 2007). Ogni provvedimento verrà attuato e debitamente pubblicizzato nel pieno rispetto del Regolamento UE 679/2016 e del Codice Privacy.

Art. 5
UTILIZZO DEGLI STRUMENTI INFORMATICI

1. Gli strumenti informatici, telematici, telefonici, di cui al precedente art. 3, comma 5, messi a disposizione dalla Camera, costituiscono strumento di lavoro.

2. 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 e interne e delle esigenze di funzionalità e di sicurezza dei sistemi informativi.
3. Nella definizione di attività lavorativa sono comprese anche le attività strumentali e collegate alla stessa, quali a esempio quelle che attengono allo svolgimento del rapporto di lavoro, e le attività compiute dai componenti degli Organi Politici.
4. 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 e ai quali l'Ente si riserva, pertanto, il diritto di accedere nei limiti consentiti dalle norme di legge e contrattuali.
5. Gli strumenti affidati devono essere custoditi e utilizzati 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 o di chi ne abbia la competenza. Il personale è altresì tenuto a informare direttamente il proprio Dirigente o il Responsabile del Servizio, nell'ipotesi di furto, danneggiamento o malfunzionamento anche parziale degli strumenti e/o del sistema.
6. La Camera si affida, di regola, alla società in house InfoCamere, per assicurare un costante aggiornamento e individuare le soluzioni tecnologiche appropriate al fine di ottimizzare le funzioni istituzionali e gestionali degli strumenti TIC e, conseguentemente, di migliorare l'attività lavorativa dei destinatari, ma può affidarsi anche ad altre società esterne.

Art. 6
UTILIZZO DELLA RETE INFORMATICA INTERNA

1. Lo sviluppo e la gestione della rete informatica interna della Camera di Cagliari, che collega l'insieme dei servizi dell'Amministrazione e garantisce l'accesso e l'utilizzo della rete internet a tutte le stazioni di lavoro attestate sulla rete stessa, è affidata alla società InfoCamere.
2. Alla rete informatica interna possono essere collegate le stazioni di lavoro di tutti i Servizi della Camera. La CCIAA si riserva la possibilità di concedere, attraverso contratti o convenzioni, il collegamento alla propria rete a soggetti/Enti pubblici o privati, a seguito di autorizzazione e approvazione da parte dell'Amministrazione che attesti la necessità della connessione ai fini della collaborazione. In tale ipotesi, sarà richiesto, alla predetta società InfoCamere, di creare un account per l'accesso alla rete con i privilegi minimi e necessari per effettuare l'attività prevista.
3. Tutti coloro che si collegano e utilizzano la rete camerale accettano senza alcuna riserva il presente Disciplinare.
4. Per accedere alla rete della Camera ogni utente deve essere in possesso delle credenziali di autenticazione costituite da un codice di identificazione (user-ID) e da una parola chiave (password), che vengono attribuite al momento dell'entrata in servizio e a seguito di richiesta a InfoCamere da parte del Servizio individuato dal Segretario Generale con propria disposizione organizzativa e in subordine dal Servizio competente in materia di risorse umane o del Servizio di provveditorato o del Servizio nell'ambito del quale si trova la stazione di lavoro.
5. Il codice per l'identificazione o codice utente è alfanumerico, formato da lettere e numeri. Per i dipendenti camerali esso è formato dalle lettere "cca" seguite dal numero di matricola dell'utente, il tutto in minuscolo (es. cca0101). I criteri di formazione del codice alfanumerico da assegnare agli utilizzatori esterni sono stabiliti dalla società InfoCamere in base alle distinte

categorie degli utilizzatori. I codici identificativi assegnati agli utilizzatori esterni da InfoCamere sono tempestivamente comunicati alla Camera.

6. Con riferimento alla password, il sistema assegna automaticamente una password generica (es. infocam1) e, in occasione del primo accesso, sarà l'utilizzatore a inserire la sua password personale che dovrà essere modificata alle scadenze predefinite e visualizzate a schermo.
7. In caso di smarrimento o perdita di riservatezza, l'utilizzatore può richiedere la modifica della password anche prima dell'eventuale termine previsto.
8. A tutela della riservatezza, ogni utilizzatore deve dotare il proprio pc di una password nello screen saver, prevedendo il tempo di inattività pari ad almeno 5/10 minuti, se non di meno, e "vistando" la casella "ripristino con password", al fine di evitare che, qualora ci si dovesse spostare dalla propria postazione, altri soggetti possano utilizzare il pc assegnato.
9. Non è consentito l'accesso alla rete e ai vari programmi con le credenziali di identificazione di un altro utente, fatto salvo quanto previsto, in caso di assenza, nei successivi artt. 7, commi 15, 16 e 17, e 9, commi 15 e 16, del presente Disciplinare.
10. Ogni singolo utente, infatti, è responsabile della custodia e della vigilanza dei beni e degli strumenti che gli vengono affidati e non può invocare a propria discolpa la motivazione che altri soggetti in sua assenza abbiano utilizzato tali strumentazioni.
11. Nelle unità di rete, trattandosi di aree di condivisione di dati e informazioni prettamente concernenti l'attività lavorativa, non devono sostare, neanche per brevi periodi, documenti non inerenti la suddetta attività.
12. La Camera può svolgere attività di controllo regolari e/o straordinarie e backup, nel rispetto della normativa vigente in materia di tutela della privacy.

Art. 7
REGOLE COMPORTAMENTALI

1. In capo a ogni utilizzatore vige l'obbligo di espletare le prestazioni lavorative con comportamenti idonei a non causare danni o pericoli agli strumenti e beni mobili a esso affidati (D.M. 28 novembre 2000 "Codice di comportamento dei dipendenti delle pubbliche amministrazioni" e CCNL), comprese tutte le risorse TIC messe a disposizione dall'Amministrazione.
2. Qualora l'utilizzatore dovesse riscontrare anomalie o furti con riferimento alla strumentazione a lui assegnata ha l'obbligo di comunicare immediatamente quanto appreso al proprio responsabile, in modo da poter avviare le procedure di denuncia all'Autorità competente.
3. Gli utilizzatori che, per la posizione ricoperta e le funzioni svolte, si trovino a gestire documenti che contengono dati sensibili o informazioni riservate dell'Amministrazione devono adottare particolari cautele, oltre che nella custodia, anche nell'utilizzo di strumenti tecnologici come supporti magnetici rimovibili (DVD, CD, supporti USB, ecc.), al fine di evitare che il contenuto possa essere trafugato e/o manomesso.
4. Il soggetto abilitato alla predisposizione e manutenzione della stazione di lavoro - che può essere rappresentato da una società esterna a cui venga affidato l'incarico - effettua le operazioni necessarie e dota la postazione stessa di tutti gli strumenti utili allo svolgimento dell'attività lavorativa. Esso procede, dunque, alla consegna della stazione di lavoro una volta effettuata l'installazione del sistema operativo, la configurazione per l'accesso alla rete camerale, l'installazione di tutti i software consoni all'attività da svolgere (es. office/openoffice, antivirus, software per l'utilizzo di internet e per l'utilizzo delle periferiche e così via), l'installazione e la configurazione delle periferiche (es. stampante, scanner, ecc.) e ogni altro intervento utile. Il

procedimento suesposto dovrà essere specificato in apposita scheda, rilasciata dalla medesima società al Servizio di provveditorato.

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 e 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. I principi di diligenza, correttezza e buona fede prevedono anche i seguenti comportamenti:

- l'obbligo di non manomettere le funzionalità del collegamento alla rete camerale e di non eseguire programmi che possano danneggiare il sistema;
- l'obbligo di porre in essere tutte le misure di sicurezza legate alle procedure di accensione e spegnimento delle apparecchiature;
- l'obbligo di utilizzo dei software e dello spazio disponibile sul server per la memorizzazione dei dati concernenti l'attività lavorativa: a tal fine, si raccomanda il salvataggio dei dati per il tempo utile, ripulendo la memoria periodicamente ed evitando ridondanze e la conservazione di file obsoleti;
- l'obbligo di segnalare tempestivamente all'amministratore di sistema e/o al dirigente di settore/responsabile delegato ogni anomalia o disfunzione degli hardware e dei software al fine di ripristinare il corretto funzionamento degli stessi;
- l'obbligo di non effettuare modifiche hardware agli apparecchi in dotazione;
- il divieto di installare sulla stazione di lavoro software non connessi alle prestazioni lavorative e/o non dotati di licenze d'uso legali e, comunque, software anche gratuiti (freeware o shareware) non distribuiti e/o comunque non espressamente autorizzati dalla Camera;
- il divieto di collegare alla stazione di lavoro periferiche hardware o dispositivi non messi a disposizione dall'Ente;
- il divieto di porre in essere azioni contrarie alle norme di legge vigenti e in generale l'obbligo di non adottare comportamenti che possano avere effetti negativi per l'Amministrazione e per l'operatività della rete camerale e degli strumenti di sua proprietà.

8. InfoCamere, nell'ambito dell'ordinaria attività di manutenzione e di gestione della sicurezza, può monitorare e controllare il corretto utilizzo della rete camerale. L'Amministrazione si riserva di assumere le decisioni che ritiene più opportune su dati e informazioni contenuti nella memoria delle apparecchiature di sua proprietà. Il tutto nel rispetto della normativa vigente.
9. Per quanto concerne le periferiche (es. stampanti) e il materiale di consumo (es. carta, toner, supporti come CD e DVD), si precisa che il loro utilizzo deve essere riservato ad attività nell'ambito di funzioni istituzionali e devono essere evitati sprechi.
10. Qualora un utilizzatore ricevesse l'attribuzione di un pc portatile, quest'ultimo dovrà essere custodito con diligenza, non solo in relazione alla stazione di lavoro ma anche in occasione di spostamenti all'esterno delle sedi dell'Amministrazione, adottando tutte le misure necessarie per

evitare pericoli, danni o sottrazioni. L'utilizzatore è il responsabile del pc portatile che gli è stato assegnato.

11. E' vietato il collegamento alla rete camerale, anche attraverso WI-FI, con apparecchiature non di proprietà dell'Amministrazione (notebook, palmari, smartphone, ecc), se non a seguito di autorizzazione da parte della Camera e, comunque, nel rispetto del presente Disciplinare.
12. È vietato altresì:

a) 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.
b) accedere al *Bios* delle stazioni di lavoro e impostare protezioni o password ulteriori che limitino l'accesso alle stazioni di lavoro stesse;
c) 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;
d) 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, l'utente è tenuto ad attivare preventivamente gli adempimenti previsti dalla legge;
- il cui contenuto sia contrario a norme di legge.

13. 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.
14. 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.
15. Ciascun dipendente deve delegare per iscritto un altro lavoratore ad accedere a dati e procedure del proprio personal computer 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. A tale scopo ogni utente deve consegnare al lavoratore da lui delegato e al Dirigente o al Responsabile di Servizio, una busta chiusa contenente le proprie credenziali di accesso avendo cura di sostituirla ogni volta che esse vengono cambiate.
16. Il lavoratore delegato accede ai dati e alle procedure su richiesta del Dirigente o del Responsabile di Servizio. Dell'attività compiuta è informato per iscritto, a cura del Dirigente/Responsabile, il dipendente alla prima occasione utile.
17. In caso di assenza del delegato è consentito l'uso delle credenziali di accesso direttamente al Dirigente/Responsabile che effettuerà l'accesso informando, per iscritto, il dipendente assente, alla prima occasione utile, delle operazioni effettuate.

Art. 8
UTILIZZO DELLA RETE INTERNET

1. L'accesso alla Rete Internet costituisce strumento di lavoro ed è consentito per finalità direttamente attinenti o comunque connesse all'esercizio dell'attività lavorativa, fatto salvo quanto previsto dal precedente art. 4, comma 3.
2. Non sono ammesse le seguenti attività:

a) l'accesso con credenziali di autenticazione differenti a quelle assegnate; anche le credenziali di accesso alla rete e ai programmi sono segrete e vanno gestite secondo le istruzioni e le procedure impartite;

b) scaricare e/o installare software non necessari allo svolgimento delle prestazioni professionali e comunque non espressamente autorizzati dalla Camera;

c) scaricare e/o usare materiale informatico non direttamente attinenti all'esercizio dell'attività lavorativa;

d) 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;

e) partecipare, anche tramite pseudonimi o nicknames, a forum di discussione on line, a chat non professionali, e utilizzare sistemi di chiamata o di video chiamata, ecc. per ragioni non direttamente attinenti o connesse all'attività lavorativa;

f) l'utilizzo di programmi e siti internet per ascoltare radio, canzoni, per effettuare download di film, ecc.;

g) navigare in internet su siti contrari a norme di legge;

h) 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;

i) l'utilizzo improprio che possa in qualsiasi modo arrecare un danno patrimoniale e/o d'immagine alla CCIAA.

3. In un'ottica preventiva Camera 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, la Camera 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.
4. La Camera, al fine di favorire lo sviluppo di nuovi modelli comunicativi, diffondere sistemi di scambio di informazioni, come le bacheche virtuali, di discussione virtuale, quale il forum, e ogni altro strumento innovativo ritenga opportuno.
5. In tal caso, gli utenti che partecipano alla comunità virtuale sono responsabili del contenuto dei propri messaggi e rispondono personalmente delle violazioni delle norme di comportamento che andranno ad integrare il presente Regolamento e che verranno emanate e pubblicizzate nel rispetto della normativa vigente.

Art. 9
UTILIZZO DELLA POSTA ELETTRONICA

1. Il dominio ca.camcom.it/ca.camcom.gov.it identifica in modo incontrovertibile la CCIAA di Cagliari, e, pertanto, qualunque informazione e messaggio che viene inviato tramite l'indirizzo di posta istituzionale ha la medesima valenza di una lettera su foglio (analogico o digitale), intestato in quanto a esso assimilabile.
2. Il predetto dominio può essere associato, quindi, esclusivamente alle caselle di posta elettronica attivate per gli Organi Politici, il personale, e gli altri soggetti specificamente autorizzati dal

Segretario Generale sulla base di apposito atto giustificativo.

3. Inoltre, al fine di agevolare lo svolgimento dell'attività lavorativa, la Camera rende disponibili indirizzi di posta elettronica condivisi tra più utilizzatori, come le caselle di posta istituite per singole unità organizzative, affiancandoli a quelli individuali.
4. Ogni comunicazione, con contenuti ufficiali, inviata o ricevuta a mezzo delle caselle di posta elettronica come sopra identificate dovrà essere protocollata secondo le modalità adottate dall'Amministrazione.
6. L'assegnatario di una casella di posta elettronica personale, rappresentata da nome.cognome@ca.camcom.it., è responsabile del relativo uso.
7. La responsabilità della casella di posta elettronica assegnata a un Servizio è posta in capo al Dirigente e al Responsabile.
8. L'attribuzione e attivazione delle caselle di posta elettronica deve essere richiesta secondo le modalità previste nell'art. 6, comma 4, del presente Disciplinare.
9. L'indirizzo di posta elettronica messa a disposizione dalla Camera, costituisce uno strumento di lavoro e il suo utilizzo è consentito per finalità attinenti o comunque connesse allo svolgimento dell'attività lavorativa, fatto salvo quanto previsto dal precedente art. 4, comma 3.
10. Non è, dunque, consentito l'utilizzo della posta elettronica con modalità che possano causare danni e ricadute di carattere patrimoniale e/o d'immagine nei confronti della Camera.
11. Al fine di un corretto utilizzo della posta elettronica è vietato:

- l'invio o la memorizzazione di messaggi non correlati all'attività lavorativa, o non veritieri, di natura oltraggiosa, volgare, diffamatoria e/o discriminatoria, e, in ogni caso, contrari a norme di legge o idonei a creare danno alla Camera o a terzi, e, dunque, fonte di responsabilità, nonché di messaggi a catena e/o spam, e di ogni altro tipo di messaggi che possa causare problemi alla sicurezza del sistema;
- lo scambio di messaggi impersonando un mittente diverso da quello reale;
- lo scambio di 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;
- l'apertura di allegati di dubbia provenienza;
- l'apertura di messaggi di posta o allegati di tipo eseguibile, salvo il caso di certezza assoluta dell'identità del mittente e della sicurezza del messaggio;
- l'invio di dati sensibili e personali, a esclusione di quanto previsto dalla normativa in materia di protezione dei dati personali;
- l'invio di comunicazioni che comportino l'impegno contrattuale dell'Amministrazione, senza il previo consenso del proprio responsabile;
- l'invio di documenti strettamente riservati senza l'autorizzazione da parte del proprio responsabile;
- la diffusione di configurazioni della rete camerale, di user-ID, password, ecc.;

12. In caso di ripetuta ricezione di messaggi di dubbia provenienza o dai contenuti anomali come indicati nel comma precedente, sarà necessario informare il Responsabile del Servizio di appartenenza che adotterà le opportune misure.
13. La sicurezza e la riservatezza della posta elettronica sono garantite dalla necessità di disporre di idonee credenziali di autenticazione (user-ID e password) per accedere alla stessa.

14. In caso di assenza programmata, soprattutto se prolungata, deve essere attivato preventivamente il sistema di risposta automatica. Il messaggio di risposta predefinito potrà essere personalizzato indicando la data in cui la mail ricevuta potrà essere letta e processata, e potrà indicare un altro indirizzo di posta elettronica istituzionale al quale il mittente può fare riferimento in caso di comunicazioni urgenti, sempre che l'utente non abbia scelto di affidare le sue credenziali a un collega, attraverso delega scritta consegnata al delegato e al Dirigente o al Responsabile del Servizio di appartenenza, come descritto nel comma successivo.
15. L'assegnatario di una casella di posta elettronica può delegare per iscritto un altro assegnatario a verificare, in caso di sua assenza anche non prolungata e non programmata, il contenuto dei messaggi a lui indirizzati e a inoltrare al Dirigente o al Responsabile di Servizio 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 delegato provvede su richiesta e del Dirigente o del Responsabile di Servizio. Delle attività effettuate è informato l'assegnatario assente alla prima occasione utile.
16. In caso di assenza del delegato è consentito l'uso delle credenziali di accesso direttamente al Dirigente/Responsabile che effettuerà l'accesso informando, per iscritto, il dipendente assente, alla prima occasione utile, delle operazioni effettuate.
17. L'inoltro dei messaggi a un'altra casella di posta avviene, altresì, in occasione di cessazione del rapporto di lavoro. Si procederà, in tal caso, anche all'eliminazione della casella dell'utente cessato, a seguito di richiesta del responsabile del Servizio di riferimento.
18. In caso di assenze dal lavoro non programmate, l'utente attiva da remoto, se possibile, il sistema di risposta automatica della propria casella di posta elettronica che informa della data in cui la mail ricevuta potrà essere letta e processata.
19. Nei messaggi inviati tramite posta elettronica camerale, sia personale sia del Servizio, deve essere annesso il seguente testo: "*Prima di stampare pensiamo all'ambiente, grazie. Questa è una comunicazione elettronica, soggetta alla normativa privacy. Il contenuto del presente messaggio è riservato solo al destinatario e può contenere materiale confidenziale. Se ha ricevuto questo messaggio per errore, le saremmo grati se, via e-mail, ce ne comunicasse la ricezione e provvedesse alla distruzione del messaggio stesso.*"
20. E' possibile accedere alla casella di posta elettronica istituzionale al di fuori dei locali della Camera, nel rispetto, comunque, del presente Disciplinare.
21. In linea di principio, le caselle di posta personali non camerali non possono essere utilizzate per lo svolgimento delle attività istituzionali, salvo eventuali deroghe concesse dal Responsabile.

Art. 10
UTILIZZO DEGLI STRUMENTI DI TELEFONIA FISSA E MOBILE

1. Gli strumenti di telefonia (sia fissa che mobile) messi a disposizione dalla Camera costituiscono strumento di lavoro e ne è consentito l'utilizzo unicamente per finalità attinenti o comunque connesse all'esercizio dell'attività lavorativa, fatto salvo quanto previsto dal precedente art. 4, comma 3.
2. 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.

Sezione III

CONTROLLI

Art. 11
MODALITA' DI EFFETTUAZIONE DEI CONTROLLI

1. Le attività di controllo sull'utilizzo di tutti gli strumenti informatici, telematici e di telefonia in uso presso la Camera, sono poste in essere con modalità tali da garantire il diritto dell'Amministrazione di proteggere la propria organizzazione (adottando idonee misure di sicurezza per assicurare la disponibilità e l'integrità dei sistemi informativi) e tali da difendere il diritto del soggetto controllato a non vedere illecitamente invasa la propria sfera personale, nel rispetto del diritto alla riservatezza e alla dignità come sanciti, per il personale, dallo Statuto dei lavoratori e, comunque, dalla vigente normativa sulla privacy. Tutti i trattamenti dei dati degli utilizzatori delle TIC camerali verranno effettuati, quindi, anche in sede di controllo, nel rispetto del Regolamento UE 679/2016 e del Codice Privacy.
2. I controlli, dunque, sono effettuati con modalità conformi alle disposizioni di legge, sia per verificare la funzionalità e la sicurezza del sistema che per appurare un corretto utilizzo delle TIC da parte degli utenti, rispettando tutte le procedure di informazione e consultazione delle rappresentanze dei lavoratori come previsto dai CCNL di riferimento.
3. I controlli possono essere effettuati in relazione alla navigazione (con file log che tracciano le varie attività in rete degli utenti navigatori) o sui contenuti (tramite un sistema di controllo - Proxy server).
4. La Camera si riserva, in primo luogo, quindi, la facoltà, nel rispetto della tutela del diritto alla riservatezza e del principio di proporzionalità e non eccedenza, 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.
5. I controlli sono effettuati dall'Amministratore di sistema su richiesta del Segretario Generale.
6. I controlli non potranno mai svolgersi direttamente e in modo puntuale, ma dovranno preliminarmente essere compiuti, secondo il principio di gradualità nell'attività di controllo, su dati aggregati, riferiti all'intera struttura organizzativa o a sue unità operative anche attraverso specifici audit informatici, e comunque in forma anonima.
7. A seguito di detto controllo anonimo, qualora si rilevasse qualche effettiva e grave anomalia nell'utilizzo di internet, della posta elettronica o delle apparecchiature si provvederà con un avviso generalizzato a invitare tutti gli utenti dell'Area o del Servizio interessato a rispettare scrupolosamente le direttive impartite.
8. 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 almeno altri due preventivi avvisi, sempre su base anonima, riferiti all'unità organizzativa dalla quale provenga l'anomalia riscontrata.
9. Qualora continuino i comportamenti non conformi, sono effettuati controlli nominativi o su singoli dispositivi e postazioni specificando le motivazioni del controllo, e, a seconda della gravità della violazione riscontrata, saranno applicate le conseguenti sanzioni nel rispetto della procedura prevista dal Codice disciplinare del CCNL di riferimento, laddove applicabile, e dalla normativa vigente che prevedono sanzioni qualora venga riscontrata negligenza sia nell'esecuzione dei compiti assegnati che nella cura dei locali, dei beni mobili, nonché degli strumenti affidati e sui quali il lavoratore ha l'obbligo di custodia e vigilanza.
10. In particolare, il Codice di comportamento dei dipendenti delle pubbliche amministrazioni - D.M.

28 novembre del 2000, G.U. n. 84 del 10 aprile 2001 - che contiene principi e norme etico-comportamentali, che costituiscono una specificazione degli obblighi di diligenza, lealtà e imparzialità e che qualificano il corretto adempimento della prestazione lavorativa, la cui inosservanza è passibile di sanzione, prevede, all'art. 10, il divieto di utilizzare gli strumenti d'ufficio a fini privati.

11. In ogni caso il mancato rispetto del presente Disciplinare potrà avere, a seconda della gravità dell'infrazione, ricadute e conseguenze anche a livello civile e/o penale, e, in generale, è passibile di sanzione qualsiasi comportamento e/o attività che procuri un danno patrimoniale e/o d'immagine all'Amministrazione.
12. Qualora l'infrazione sia posta in essere da utenti esterni autorizzati all'utilizzo delle risorse camerali, si procederà alla revoca delle autorizzazioni, nonché ad ogni altra eventuale sanzione in base alla gravità dell'atto, come previsto dalle norme vigenti.
13. Non sono ammessi, su base individuale, controlli casuali, prolungati, costanti o indiscriminati.
14. 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:

- 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;
- riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore, dei contenuti delle medesime, nonché del tempo di permanenza sulle stesse;
- lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- analisi occulta di computer o altri dispositivi portatili affidati in uso, ovvero delle rispettive connessioni ad Internet;
- le attività descritte, ed altre per i medesimi scopi, effettuate sulle utenze telefoniche fisse o relative a telefonia cellulare.

15. 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.

Art. 12
EVENTUALI CONTROLLI SUI VEICOLI

1. Per i veicoli forniti ai dipendenti quando funzionali allo svolgimento delle attività, la Camera esclude l'utilizzo di sistemi di rilevazione della posizione dei veicoli stessi attraverso dispositivi basati su tecnologie GPS o altre con le medesime finalità.
2. L'eventuale collocazione e utilizzazione dei dispositivi di cui al comma precedente è ammessa, previa specificazione delle esigenze che le giustificano, con la procedura di cui all'art. 4, comma 1, della legge n. 300/1970. Il trattamento dei dati personali è effettuato nel pieno rispetto di quanto previsto dal Regolamento UE, con particolare riferimento ai principi di necessità, pertinenza, non eccedenza e minimizzazione.

Sezione IV
DISPOSIZIONI FINALI

Art. 13
NORMA DI RINVIO

1. Per quanto non previsto nel presente Disciplinare si fa espresso rinvio a ogni disposizione ordinamentale vigente in materia, con particolare riferimento ai seguenti testi normativi, regolamenti, circolari e provvedimenti del Garante Privacy:

- Regolamento UE 679/2016, 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;
- 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;
- 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".

2. Ulteriori provvedimenti e indicazioni del Garante Privacy che delineano il contesto di riferimento in materia al quale il Disciplinare espressamente rinvia sono:

- Deliberazione n. 13 dell'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**).**

Art. 14
DISPOSIZIONI FINALI

1. Il presente Disciplinare, sostituisce il precedente Regolamento approvato con deliberazione del Consiglio camerale n. 8 del 7 luglio 2011, ed entra in vigore il giorno dopo la pubblicazione disposta dal precedente art. 3, comma 4, previa pubblicazione sull'albo camerale.
2. La Camera può apportare in qualunque momento eventuali modificazioni e/o integrazioni al presente Disciplinare finalizzate al perseguimento di una sempre maggiore efficienza, efficacia ed economicità nell'organizzazione dell'attività lavorativa e tali da garantire la sicurezza, la disponibilità e l'integrità dei sistemi informativi.
3. Al fine di stimolare la partecipazione attiva, i dipendenti possono proporre, attraverso il proprio responsabile di servizio, integrazioni motivate al presente Disciplinare
4. Il Disciplinare, inoltre, potrà essere modificato e/o integrato a seguito di cambiamenti nella normativa di riferimento o in ragione dell'evolversi delle tecnologie dell'informazione e della comunicazione tali da richiedere adeguamenti delle disposizioni.
5. Tali modifiche dovranno essere tempestivamente comunicate a tutti i destinatari nelle forme previste dal precedente art. 3, comma 4.