# Regolamento Utilizzo Sistemi ICT AGEC

Approvato con deliberazione del Cda n° 99 in data 09 ottobre 2018

Sommario

## 1. Premessa

La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer e dagli strumenti mobili, espone AGEC (in seguito anche "Azienda") ai rischi di un coinvolgimento sia patrimoniale sia penale, creando problemi alla sicurezza e all'immagine dell'Azienda stessa.
Premesso quindi che l'utilizzo delle risorse informatiche e telematiche della nostra Azienda deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, AGEC ha adottato un Regolamento interno, come previsto dal GDPR, General Data Protection Regulation - Regolamento UE 2016/679, diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla sicurezza nel trattamento dei dati.
Il Regolamento svolge anche la funzione di informare compiutamente gli utenti sugli specifici trattamenti dei loro dati personali che vengono effettuati e delle modalità adottate.
Anche lo sviluppo delle reti sociali on-line incide, direttamente o indirettamente, sulle attività dell'Azienda, sulla sua immagine e sulle relazioni commerciali instaurate. Infatti, l'uso dei *social media*, quali Facebook™, Twitter™, Linkedin™, dei blog e dei forum, anche professionali, costituisce un efficace strumento di condivisione di contenuti (testi, immagini, video) da parte degli utenti e, allo stesso tempo, un'evidente opportunità per l'Azienda, in particolare in ambito commerciale e di marketing. Risulta però necessario che, al fine di evitare il sorgere di rischi derivanti dalla presenza della denominazione dell'Azienda e/o di altri riferimenti ad essa riconducibili, eventualmente solo indiretta, sui *social media*, si tenga pure conto di questo preciso aspetto nel presente Regolamento.
Con l'entrata in vigore del presente Regolamento tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.
Oltre a detto Regolamento Agec ha adottato e continuano a permanere vigenti le seguenti diposizioni attinenti alla materia: ove vi fosse contrasto il presente regolamento avrà prevalenza.

- Il Codice Etico
- Il sistema di procedura secondo il decreto 231/2001
- Il Regolamento sugli archivi di AGEC
- Il manuale di gestione del protocollo informatico
- Disposizioni e procedure aziendali per l'assegnazione e l'uso dei terminali radiomobili e delle relative utenze approvato con determina del dg n° 06 del 20 marzo 2017

Copia di questo Regolamento è presente e liberamente consultabile sia in formato elettronico sia in formato cartaceo affisso nelle bacheche aziendali, nonché presso la Sezione Risorse Umane.

## 2. Amministratori di sistema, di rete e custodi delle credenziali

Gli amministratori di sistema o di rete designati dall'Azienda saranno individuati e pubblicizzati nell'apposito documento pubblico "Prospetto Informativo Piattaforme Aziendali (Servizi Informatici)" che sarà consultabile in formato elettronico sulla Intranet Aziendale, sia in formato cartaceo affisso nelle bacheche aziendali.

## 3. Campo di applicazione del Regolamento – normativa UE e glossario

Il presente Regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'Azienda a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratore a progetto, in stage, ecc.).

Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente e collaboratore (collaboratore a progetto, in stage, agente, ecc.) in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata quale "incaricato del trattamento".
Il presente regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'azienda a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratore a progetto, in stage, ecc.).
Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente e collaboratore (collaboratore a progetto, in stage, agente ,ecc.) in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venir indicata quale "incaricato del trattamento".

---

*NORMATIVA DI RIFERIMENTO: REGOLAMENTO UE 679/2016*

***Articolo 29 - Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento.***
*Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.*

***Articolo 32 - Sicurezza del trattamento***
*1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento ed il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:*

*a)* • *la pseudonimizzazione e la cifratura dei dati personali;*

*b)* • *la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;*

*c)* • *la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;*

*d)* • *una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento.*

*2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.*
*3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.*
*4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.*

*DOCUMENTI DI RIFERIMENTO*
*1. Regolamento Generale sulla Protezione dei dati personali (UE) 2016/679.*
*2. Procedura per la gestione dei Data Breach – Violazione dei Dati.*

3. *Procedura sull'esercizio dei diritti dell'Interessato.*
4. *Registro dei Trattamenti ex art. 30 GDPR.*

## *GLOSSARIO E ACRONIMI*

***Aree Sensibili:*** *sono quei luoghi fisici o della Rete Aziendale in cui vengono Trattati Dati Particolari e/o Dati Giudiziari relativi a persone fisiche; e/o luoghi in cui vengono gestiti e consultati documenti riservati a cui è assolutamente vietato accedere se non per motivi di servizio;*
***Autorità di Controllo:*** *l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 GDPR; Consenso dell'Interessato o Consenso: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'Interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i Dati Personali che lo riguardano siano oggetto di Trattamento;*
***Dati Biometrici:*** *i Dati Personali ottenuti da un Trattamento tecnico specifico relativi alle caratteristiche fisiche,*
*fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;*
***Dati Comuni:*** *sono tutti i Dati Personali che non appartengono alle categorie dei Dati Particolari e Dati Giudiziari;*
***Dati Genetici:*** *i Dati Personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;*
***Dati Giudiziari:*** *Dati Personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza;*
***Dati Particolari:*** *Dati Personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona; Dati relativi alla Salute: i Dati Personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;*
***Dato Personale:*** *qualsiasi informazione riguardante una persona fisica identificata o identificabile ("Interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;*
***Destinatario/i:*** *la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di Dati Personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di Dati Personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate Destinatari; il Trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del Trattamento;*
***Apparati Fissi:*** *si intendono gli strumenti informatici non facilmente removibili dal perimetro dello Studio quali personal computer, server locali, stampanti affidati alle Persone Autorizzate per uso professionale;*
***Apparati Mobili:*** *in generale si intendono quegli strumenti informatici che per loro natura sono facilmente asportabili dal perimetro aziendale quali chiavette USB, SD cards, hard disk esterni, notebook, ultrabook, tablet e smartphone utilizzati dagli incaricati del trattamento per uso professionale;*
***DPO o Data Protection Officer:*** *è una persona fisica, nominata obbligatoriamente solo nei casi di cui all'art. 37.1 GDPR dal Titolare o dal Responsabile del Trattamento e deve possedere una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati per assisterli nel rispetto a livello interno del GDPR;*
***GDPR o Regolamento:*** *Regolamento Generale sulla Protezione dei dati personali (UE) 2016/679;*
***Incaricato/i o Persona/e Autorizzata/e:*** *si tratta dei Collaboratori autorizzati al Trattamento dei Dati Personali sotto la diretta autorità del Titolare e/o del Responsabile ex artt. 4(10) e 29 del GDPR. Stante la*

*definizione fornita dal Gruppo di Lavoro Articolo 29 dell'Opinione 2/2017 questa definizione ricomprende: dipendenti ed ex dipendenti, dirigenti, sindaci, collaboratori e lavoratori a partita IVA, lavoratori a chiamata, part-time, job-sharing, contratti a termine, stage, senza distinzione di ruolo, funzione e/o livello, e, più in generale, tutti coloro che utilizzino od abbiano utilizzato Strumenti Aziendali o Strumenti Personali, operino sulla Rete Aziendale ovvero siano a conoscenza di informazioni aziendali rilevanti quali, a titolo esemplificativo e non esaustivo: (a) i Dati Personali di clienti, dipendenti e fornitori, compresi gli indirizzi di posta elettronica; (b) tutte le informazioni aventi ad oggetto informazioni confidenziali di natura commerciale, finanziaria o di strategia di business; nonché (c) i dati e le informazioni relative ai processi aziendali, inclusa la realizzazione di marchi, brevetti e diritti di proprietà industriale, la cui tutela prescinde dagli effetti pregiudizievoli che potrebbe comportare la diffusione delle medesime.*

***Pseudonimizzazione:*** *il Trattamento dei Dati Personali in modo tale che i Dati Personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali Dati Personali non siano attribuiti a una persona fisica identificata o identificabile;*

***Responsabile del Trattamento o Responsabile:*** *la persona fisica o giuridica, l'autorità pubblica, il servizio o altro*

*organismo che tratta Dati Personali per conto del Titolare del Trattamento; deve presentare garanzie sufficienti di attuare misure tecniche e organizzative adeguate in modo tale che il Trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato;*

***Rete Aziendale:*** *rappresenta il perimetro digitale dello Studio, possibilmente contenente Dati Personali e/o informazioni riservate, comprensivo dei dispositivi hardware/software sia per la gestione dei servizi interni (es. switch, LAN, Wi-Fi) che dei collegamenti da o verso l'esterno (es. boundary router, SSH, VPN);*

***Strumenti Aziendali:*** *l'insieme di Device Fissi e Device Mobili concessi in comodato d'uso dall'Azienda agli incaricati del trattamento al fine di svolgere le proprie mansioni;*

***Titolare del Trattamento o Titolare:*** *la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del Trattamento di dati personali; quando le finalità e i mezzi di tale Trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il Titolare o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;*

***Trattamento o Trattato/Trattati:*** *qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a Dati Personali o insiemi di Dati Personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;*

***Violazione Dei Dati Personali ovvero Data Breach:*** *è la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai Dati Personali trasmessi, conservati o comunque Trattati.*

## *4. Informativa riguardante l'utilizzo degli strumenti elettronici Aziendali*

AGEC rende noto che il sistema informativo è gestito dalle seguenti figure:

a) Personale incaricato che opera presso l'Area Servizi Generali – Sezione Servizi Generali – Servizio Sistemi Informatici oppure consulenti esterni che operano sotto la diretta supervisione del Servizio Servizi Informatici;
b) AGEC ha affidato in outsourcing alcuni servizi;

Per il dettaglio delle modalità di erogazione di questi e di altri servizi, si rimanda all'apposito documento pubblico "Prospetto Informativo Piattaforme Aziendali (Servizi Informatici)" che

sarà consultabile sia in formato elettronico sia in formato cartaceo affisso nelle bacheche aziendali.
Ogni figura indicata è stata autorizzata a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi come ad esempio aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware etc..
Detti interventi, in considerazione dei divieti di cui ai successivi punti da 5 a 12, potranno anche comportare l'accesso, in qualunque momento, ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica, nonché alla verifica sui siti internet acceduti dagli utenti abilitati alla navigazione esterna. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Azienda, si applica anche in caso di assenza prolungata od impedimento dell'utente.
Il personale incaricato ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc.
L'intervento viene effettuato esclusivamente su chiamata dell'utente (nel momento di attivazione della connessione con il suo esplicito consenso) o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.
Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà della Direzione Aziendale, direttamente o tramite il personale de Servizio Servizi Informatici o addetti esterni alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.
Si rammenta che l'utilizzo degli strumenti mobili come smartphone e/o tablet deve seguire le stesse regole indicate successivamente per gli strumenti informatici aziendali.

## *5. Nuovi Dipendenti e/o Collaboratori*

All'arrivo di un nuovo dipendente e/o collaboratore, la Sezione Risorse Umane, in relazione alle mansioni affidate, si occuperà di coordinare la creazione e/o assegnazione degli strumenti aziendali (siano essi strumenti fisici e/o informatici), la consegna delle lettere di incarico al trattamento dei dati, il Regolamento Aziendale ed ogni altra documentazione legata al rapporto di lavoro.
In particolare, il Dirigente di settore relativo al nuovo dipendente o collaboratore si coordinerà con il Servizio Sistemi Informatici al fine di garantire la fornitura dei corretti strumenti aziendali e la relativa attivazione delle specifiche login informatiche in base ai servizi aziendali che dovrà utilizzare, nonché ad una formazione adeguata all'utilizzo degli stessi.

## *6. Creazione nuove banche dati, gestione programmi*

Senza preventiva autorizzazione dei Titolari del Trattamento dei Dati ad AGEC non è permesso realizzare nuove ed autonome banche dati, con finalità diverse da quelle già previste.

## *7. Trattamento dei dati personali*

Il trattamento dei dati personali deve essere effettuato esclusivamente in conformità alle finalità previste e dichiarate dall'Azienda e, pertanto, in conformità alle informazioni che AGEC

ha comunicato agli interessati. L'eventuale raccolta di dati dovrà avvenire nel rispetto delle procedure e dei modelli di informativa e/o consenso elaborati da AGEC.
L'incaricato deve prestare particolare attenzione all'esattezza dei dati trattati e provvedere, inoltre, all'aggiornamento degli stessi.

## *8. Comunicazione e diffusione dei dati*

In relazione alle banche dati di cui è autorizzato il trattamento nello svolgimento delle mansioni affidate, è autorizzata la comunicazione dei dati stessi esclusivamente ai soggetti esterni indicati da AGEC per ognuna di esse.
Ogni ipotesi diversa di comunicazione o, addirittura, di diffusione dei dati dovrà essere preventivamente autorizzata di volta in volta dall'Azienda.

## *9. Misure di sicurezza*

Ogni incaricato è tenuto ad osservare tutte le misure di protezione e sicurezza atte a evitare rischi di distruzione, perdita, accesso non autorizzato, trattamento non consentito, già predisposte da AGEC, nonché quelle che in futuro verranno comunicate.

## *10. Utilizzo del Personal Computer*

Il Personal Computer affidato al dipendente o collaboratore, che deve sempre ispirarsi ai principi di diligenza e correttezza, è uno strumento di lavoro: esso deve essere custodito con cura evitando manomissioni, danneggiamenti o utilizzi, anche da parte di altre persone. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza, pertanto esso va utilizzato esclusivamente per fini professionali (in relazione alle mansioni assegnate), evitando usi per fini personali al di fuori dei casi consentiti ed autorizzati in maniera scritta dalla Direzione.
L'accesso all'elaboratore (accesso alla rete e screen saver), al sistema gestionale e a tutti gli altri applicativi aziendali sono protetti da binomio nome utente/password; quest'ultima deve essere custodita dall'incaricato con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione (Bios) degli strumenti informatici che ne abbiano la funzione, senza preventiva autorizzazione da parte degli Amministratori di sistema.
Il custode delle parole chiave riservate, per l'espletamento delle sue funzioni, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno. Il custode delle parole chiave riservate potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere alla stessa Azienda, titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate dalla stessa Azienda, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività aziendale nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio in caso di prolungata assenza od impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato.
In caso di interventi da parte di personale tecnico, l'utente è invitato a digitare personalmente la password ed a presenziare durante le operazioni di assistenza e/o installazione.
Non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione esplicita degli Amministratori di sistema, in quanto sussiste il grave pericolo di portare virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.
Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dagli Amministratori si sistema di AGEC l'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'Azienda a gravi responsabilità civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (D.Lgs. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore ed altri diritti connessi al suo esercizio aggiornato, da ultimo, con le modifiche apportate dal D.L. 16 ottobre 2017, n. 148, convertito, con modificazioni, dalla L. 4 dicembre 2017, n. 172.) che impone la presenza, nel sistema, di

software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore (art. 615-ter e 615–quater c.p. richiamati dall'articolo 24-bis del decreto 231/2001).
Nel caso fosse necessario sviluppare dei nuovi programmi o database personalizzati (ad esempio in Microsoft Access, HTML, ecc.) ad accesso condiviso da più utenti, è necessario discuterne preventivamente con il Servizio Sistemi Informatici per valutarne la fattibilità, le possibili alternative e la protezione dei dati.
Non è consentito all'utente modificare le caratteristiche impostate sul proprio personal computer, salvo previa autorizzazione esplicita degli Amministratori di sistema.
Il personal computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. L'attivazione dello screen saver protetto da password è gestita in modo automatico dal sistema (dopo un intervallo di inattività di 20 minuti). Si raccomanda comunque attivare manualmente il blocco del proprio PC quando ci si allontana dallo stesso. Lo si può fare premendo contemporaneamente la combinazione di tasti "CTRL + ALT + CANC" e, nella videata che appare, premere il pulsante "Blocca computer".
Non è consentita l'installazione sul proprio personal computer di nessun dispositivo di memorizzazione, comunicazione o altro (come, ad esempio, masterizzatori, modem, "chiavette" USB), se non con l'autorizzazione espressa degli Amministratori di sistema.
Non è consentito l'utilizzo di sistemi di archiviazione esterna basati su "cloud" (a titolo esemplificativo ma non esaustivo sistemi come Dropbox, Wetransfer, OneDrive, etc) né l'utilizzo di sistemi di posta elettronica non aziendali se non per casi di assoluta necessità, in ogni caso evitando di utilizzarli per qualsiasi documento e/o file che contenga dati personali in carico al Titolare del Trattamento AGEC.
L'utilizzo di tutte le reti WiFi presenti in Azienda è limitato agli utenti autorizzati. A tale scopo si precisa che l'utilizzo di qualsiasi rete WiFi disponibile in Azienda e dalla stessa configurata è possibile solo a seguito di digitazione di specifiche credenziali che vengono assegnate dal Servizio Sistemi Informatici.

## *11. Utilizzo della rete di AGEC*

Le unità di rete 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 queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup. Ciascun utente ha a disposizione un'unità di rete condivisa (K:\) sui server aziendali.
Per una più ampia divulgazione delle circolari affisse nelle bacheche aziendali, è disponibile anche una "bacheca informatica", consultabile nelle cartelle di rete e/o nella Intranet aziendale, dove si possono trovare tutte le comunicazioni ufficiali da parte della Direzione, con decorrenza dalla data odierna.
Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.
L'Amministratore di sistema può in qualunque momento procedere alla rimozione di ogni cartella, file o applicazione che riterrà non essere attinenti alle finalità lavorative e/o essere pericolosi per la sicurezza, sulle unità di rete. Per quanto riguarda eventuali files e/o cartelle presenti sui singoli personal computer degli incaricati si rimanda al paragrafo successivo.
Costituisce buona regola la periodica (almeno ogni tre mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È, infatti, assolutamente da evitare una doppia archiviazione di dati.
Qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, sulla Intranet aziendale.

E' fatto divieto assoluto di salvare qualsiasi tipologia di file contenente dati personali (con particolare attenzione a quelli contenenti dati personali particolari, che devono comunque essere sempre crittografati) sulle cartelle di rete accessibili indistintamente a tutti gli utenti, da utilizzarsi solo per appoggio temporaneo e il cui contenuto viene cancellato in automatico ogni 48 ore.
È cura dell'utente effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. È buona regola stampare documenti o file molto lunghi sui dispositivi multifunzione. Su tali dispositivi è inoltre possibile stampare documenti riservati e/o contenenti dati particolari, proteggendoli con una password, come pure effettuare scansioni di documenti, indirizzandole direttamente alla propria email aziendale. In caso di necessità le stampe o le scansioni in corso possono essere eliminate.
E' vietato stampare documenti contenenti dati particolari, se non per casi strettamente necessari e alle seguenti condizioni congiunte:

- Immediata asportazione del documento cartaceo dalla stampante;
- utilizzo solo di stampanti protette da codice di stampa, l'utente dovrà inserire un apposito codice personale per attivare la stampa del documento.

È vietato scansionare digitalmente documenti contenenti dati particolari, se non per casi strettamente necessari e alle seguenti condizioni congiunte:

- immediata asportazione del documento cartaceo dalla stampante;
- solo su file con destinazione cartelle di rete protette da password e/o ad accesso riservato esclusivamente all'utente che effettua la scansione o con invio via mail alla casella di posta di chi effettua la scansione.

## *12. Utilizzo della rete Intranet di AGEC*

È presente una Intranet aziendale basata su piattaforma web interna. Ad essa possono avere accesso tutti gli utenti abilitati e profilati in relazione al ruolo aziendale.
Essendo un portale con autenticazione integrata con Microsoft Active Directory, devono attenersi alle indicazioni sulle procedure di scelta e gestione delle password secondo quanto riportato al successivo capitolo 13.
Dal punto di vista tecnico essa equivale ad una cartella di rete. Le unità di rete 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, sulla Intranet aziendale.
È fatto divieto assoluto di salvare qualsiasi tipologia di file contenete dati personali senza la preventiva autorizzazione scritta del proprio Responsabile e/o del moderatore del servizio.

## *13. Gestione delle password*

Le credenziali di accesso ai sistemi sono qualcosa di riservato e personale che l'utente deve custodire con molta cura. Non devono ad esempio essere scritte su fogli lasciati sulle scrivanie o essere inserite su file di testo non protetti sul desktop del proprio PC.
Qualsiasi password deve essere immediatamente sostituita, dandone comunicazione al custode delle parole chiave, nel caso si sospetti che la stessa abbia perso la segretezza.
Qualora l'utente venga a conoscenza delle password di altro utente, è tenuto a darne immediata notizia al custode delle parole chiave.
La password di ingresso alla rete e del gestionale non devono essere comunicate ai custodi delle parole chiave (Servizio Sistemi Informatici). Le altre password devono essere comunicate, solo nei casi in cui la mancata comunicazione pregiudicherebbe lo svolgimento dell'attività lavorativa in caso di prolungata assenza dell'incaricato (ad es. Programma per la gestione delle paghe, Home Banking, fogli Word o Excel protetti da password, strumenti come smartphone aziendali, ecc.). Tale comunicazione deve avvenire tramite la consegna al Servizio Sistemi Informatici di un foglio in busta chiusa, o altro sistema equivalente, indicante:

- il proprio nome e cognome;

- l'eventuale nome di account dell'utente;
- la password;
- il nome dell'applicazione o del file o dell'apparato protetto.

## 14. Utilizzo dei supporti magnetici

Tutti i supporti magnetici riutilizzabili (dischetti, cassette, cartucce, cd-rom e/o cd-rw, DVD e/o DVD-RW, schede di memorizzazione SD o similari, "chiavette" USB, ecc.) contenenti dati particolari devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato e/o ve ne sia l'accesso da parte di persone non autorizzate, essi vanno quindi sempre crittografati completamente (oppure salvare su di essi documenti informatici in forma crittografata). Qualora i supporti magnetici contenenti dati particolari non debbano più essere utilizzati per gli scopi per i quali erano stati destinati, essi devono essere consegnati agli Amministratori di sistema, i quali provvederanno a cancellarne il contenuto, annullando e rendendo non intelligibili e tecnicamente in alcun modo non ricostruibili le informazioni in essi contenute. Una persona esperta potrebbe, infatti, recuperare i dati memorizzati anche dopo la loro cancellazione.

## 15. Utilizzo di dispositivi portatili

In aggiunta a quanto indicato al capitolo 10 "Utilizzo del personal computer" si definiscono ulteriori regole per gli utilizzatori di personal computer portatili e/o tablet e/o smartphone aziendali. L'utente è responsabile del o degli apparati portatili assegnati dall'Azienda e deve custodirli con diligenza, sia durante gli spostamenti, sia durante l'utilizzo nel luogo di lavoro.
Ai dispositivi portatili si applicano le regole di utilizzo previste per i personal computer connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sugli stessi prima della riconsegna e/o in caso di riparazione, in quanto potrebbero essere accessibili informazioni personali come, a titolo esemplificativo, foto, documenti, cronologia navigazione, email.
I dispositivi portatili utilizzati all'esterno (convegni, visite in aziende, ecc.), in caso di allontanamento, devono essere custoditi in un luogo protetto.
Al termine della giornata lavorativa, i dispositivi portatili devono essere lasciati negli uffici oppure si possono portare nella propria abitazione sotto diretta custodia.
Altri obblighi:

1. Tenere il dispositivo portatile con sé quando è possibile. Non condividere il proprio dispositivo portatile con altri per scopo privato.
2. Se si viaggia in aereo e/o treno, non mettere il dispositivo portatile nel bagaglio che viene imbarcato e/o riposto nelle cappelliere, e prestare attenzione a possibili furti nell'area di check-in degli aeroporti.
3. Il dispositivo portatile non dovrebbe essere lasciato in un veicolo incustodito.
4. Se è necessario lasciare il dispositivo portatile nell'albergo, chiuderlo in cassaforte, se disponibile.
5. Assicurarsi di collegare il personal computer portatile alla rete aziendale almeno una volta al mese, per scaricare gli aggiornamenti di sistema e dell'antivirus.

## 16. Uso della posta elettronica

La casella di posta, assegnata dall'Azienda all'utente, è uno strumento di lavoro, i criteri che dovranno governare lo sfruttamento di questa risorsa sono la correttezza ed il buon senso. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse, tutti i messaggi inviati tramite l'indirizzo aziendale saranno considerati nella disponibilità dell'Azienda.
Il sistema aziendale per la posta elettronica è fornito dal programma Thunderbird o similare oppure tramite accesso all'interfaccia web del sistema. All'interno della rete aziendale è vietato utilizzare qualsiasi altro sistema di messaggistica non autorizzato dagli Amministratori di

sistema (ad esempio, il comando Net Send di Windows, il programma Outlook/Windows MAIL, etc.). Sono comunque consentiti solamente gli strumenti resi disponibili all'interno della intranet.
È fatto divieto di utilizzare le caselle di posta elettronica aziendale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list, salvo diversa ed esplicita autorizzazione e salvo casi di effettiva necessità e/o urgenza.
È buona norma evitare messaggi completamente estranei al rapporto di lavoro o alle relazioni tra colleghi. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti. Ogni incaricato è tenuto a rispettare le dimensioni massime, stabilite dagli Amministratori di sistema, per la propria casella di posta elettronica aziendale e per i singoli messaggi.
In caso di accertata necessità lavorativa è possibile ottenere una estensione dello spazio della casella di posta; la richiesta va inviata tramite mail sia a sezioneinformatica@agec.it che al proprio dirigente e/o responsabile di ufficio.
Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per AGEC deve essere visionata od autorizzata dalla Direzione, o in ogni modo è opportuno fare riferimento alle procedure in essere per la corrispondenza ordinaria.
La documentazione elettronica che costituisce per l'azienda "know how" aziendale tecnico o commerciale protetto (tutelato in base all'art. 6 bis del r.d. 29.6.1939 n.1127), e che, quindi, viene contraddistinta da diciture od avvertenze dirette ad evidenziarne il carattere riservato o segreto a tutela del patrimonio dell'impresa, non può essere comunicata all'esterno senza preventiva autorizzazione della Direzione.
È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario, ma di norma, per la documentazione ufficiale, è necessario rispettare le procedure previste dal manuale di gestione del protocollo informatico.
Per la trasmissione di file, che non contengano dati particolari, all'interno di AGEC è possibile utilizzare la posta elettronica, prestando attenzione alla dimensione degli allegati. È obbligatorio controllare i file allegati di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti). E' assolutamente necessario verificare la correttezza e provenienza delle mail contenenti link nei corpi delle email; prima di procedere a cliccare sul link è necessario verificarne la provenienza nei casi particolari anche con l'ausilio del Servizio Sistemi Informatici.
Tutti i messaggi contenenti dati particolari nel corpo del testo e/o negli allegati vanno creati solo se strettamente necessario, in base alle mansioni svolte e quindi in base all'incarico ricevuto, vanno inviati solo a destinatari autorizzati e comunque sempre crittografati prima dell'invio. Rivolgersi agli Amministratori di Sistema per l'attivazione del servizio di crittografia, in base alle autorizzazioni all'utilizzo da parte dell'Azienda.
È vietato inviare catene telematiche (o "di Sant'Antonio"). Se si dovessero ricevere messaggi di tale tipo, si deve comunicarlo immediatamente agli Amministratori di sistema. Non si devono in alcun caso attivare gli allegati di tali messaggi. Ciò vale anche per i messaggi di provenienza non identificabile.
Non è consentito utilizzare la posta elettronica per pubblicizzare o divulgare messaggi personali non riguardanti l'attività lavorativa all'interno della rete aziendale.
Non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
Per evitare perdite di dati, è possibile eseguire periodicamente l'archiviazione della posta elettronica. Tale archiviazione deve essere eseguita sull'unità di rete: per le relative istruzioni, si invita a contattare gli Amministratori di sistema.
Al fine di garantire la funzionalità del servizio di posta elettronica aziendale e di ridurre al minimo l'accesso ai dati, nel caso di assenza programmata, nel rispetto del principio di necessità e di proporzionalità, l'utente deve attivare la risposta automatica ai messaggi di posta

elettronica ricevuti, che informi i mittenti della durata della sua assenza e delle coordinate aziendali che dovranno utilizzare in tale periodo.
Per garantire la continuità dell'attività, nei soli casi di assenza improvvisa o prolungata, l'azienda incarica gli amministratori di rete di accedere alla casetta postale dell'utente, per inoltrare al titolare del trattamento le comunicazioni ritenute rilevanti per lo svolgimento dell'attività lavorativa. In tal caso sarà premura del responsabile del trattamento redigere di tale attività un apposito verbale che informi il lavoratore interessato alla prima occasione utile.
Al fine di ribadire agli interlocutori la natura esclusivamente aziendale della casella di posta elettronica, si invita tutto il personale ad inserire nei messaggi un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi precisando che, pertanto, il personale debitamente incaricato potrà accedere al contenuto del messaggio inviato alla stessa casella secondo le regole fissate nel proprio regolamento aziendale.

## *17. Uso della rete Internet e dei relativi servizi*

Il personal computer abilitato alla navigazione in Internet costituisce uno strumento aziendale necessario allo svolgimento della propria attività lavorativa. Pertanto, è consentita la navigazione solamente nei siti legati all'attività lavorativa stessa.
È fatto divieto all'utente lo scarico di software gratuito (freeware) e a pagamento (shareware) prelevato da siti Internet, se non espressamente autorizzato dagli Amministratori di sistema.
È in ogni caso attivo un sistema di protezione che impedisce lo scarico di tali software, anche in funzione della prevenzione dei reati di cui agli artt. 615-quinquies, 635-bis, 635-ter, 635-quater e 635-quinquies del Codice Penale.
È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla Direzione e con il rispetto delle normali procedure di acquisto.
È vietata la navigazione su siti a pagamento, se non si è espressamente autorizzati dalla Direzione.
È da evitare ogni forma di registrazione a siti i cui contenuti non sono legati all'attività lavorativa.
È vietata la partecipazione a forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche, le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) e l'iscrizione a social forum.
È vietato ascoltare musica tramite Internet, scaricare file musicali e altri file di natura multimediale non riconducibili all'attività lavorativa.
Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, AGEC rende peraltro nota l'adozione di uno specifico sistema di blocco o filtro automatico che prevengano determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una black list.
Si rende noto che i moderni sistemi di controllo e sicurezza della navigazione (web proxy), come quello adottato in AGEC, per soddisfare i requisiti di protezione, devono effettuare, con opportune tecniche, il controllo della navigazione effettuata tramite protocollo HTTPS (ormai diffuso nella maggior parte dei siti web), questa modalità permette al sistema di tracciare anche eventuali immissione di informazioni all'interno di pagine crittografate, come ad esempio login e password.
I controlli, compiuti dal personale incaricato ai sensi del precedente capitolo 2, avverranno mediante il sistema di controllo dei contenuti Sophos Web Protection e su base statistica.
Il controllo sui file di log non è continuativo ed i file stessi vengono conservati per un tempo congruo e bilanciato e comunque mai superiore ai 6 mesi, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'azienda.

## *18. Uso degli impianti telefonici*

Per "impianti telefonici aziendali" si intendono tutte le infrastrutture tecniche e le apparecchiature, sia fisse sia mobili, atte alla comunicazione vocale ed in uso all'interno e all'esterno (ad es. i cellulari assegnati) dell'Azienda.
Gli impianti telefonici aziendali rientrano nella categoria dei "beni aziendali" e per questo il loro uso deve essere improntato alla tutela del patrimonio aziendale. Questo significa che chi è autorizzato all'utilizzo degli stessi lo dovrà fare nel rispetto del principio indicato.
Chiunque usi gli impianti telefonici per scopi estranei all'attività professionale a cui è addetto lo dovrà fare limitando al minimo i costi derivanti dalla telefonata. Da questo discende che l'uso degli impianti in questione per scopi privati è consentito in caso di necessità ma limitato secondo le regole della correttezza e del buon senso.
Nessun tipo di controllo personale verrà effettuato sulla natura e sulla durata delle telefonate eventualmente compiute. Il contenuto di esse ed il numero chiamato sono obbligatoriamente segreti ed ogni controllo in merito violerebbe diritti costituzionalmente garantiti. Verranno effettuate esclusivamente rilevazioni di carattere impersonale ed anonimo sull'eventuale aumento del traffico generale telefonico e sull'eventuale aumento dell'importo delle bollette. In caso di riscontro positivo qualunque ulteriore indagine in merito sarà autorizzata con provvedimento dell'Autorità Giudiziaria. Solo successivamente a questa verifica potranno essere presi provvedimenti disciplinari.
L'Azienda assume l'impegno di non accedere ai dati inerenti al traffico telefonico per finalità diverse da quella della tutela del patrimonio aziendale. E' altresì esclusa la riferibilità del numero telefonico composto alla persona del chiamante. Per qualunque indagine di questo tipo verrà preventivamente richiesta l'autorizzazione all'Autorità giudiziaria competente.
Per tutto quanto non espressamente riportatosi farà riferimento alle Disposizioni e procedure aziendali per l'assegnazione e l'uso dei terminali radiomobili e delle relative utenze approvato con determina del dg n° 06 del 20 marzo 2017 e smi.

## *19. Controlli*

Il datore di lavoro può riservarsi di controllare (direttamente o attraverso la propria struttura) l'effettivo adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro (cfr. artt. 2086, 2087 e 2104 cod. civ.). Nell'esercizio di tale prerogativa il datore di lavoro deve rispettare la libertà e la dignità dei lavoratori nonché, con specifico riferimento alla disciplina in materia di protezione dei dati personali, i principi di correttezza (secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori), di pertinenza e non eccedenza; ciò tenuto anche conto che tali controlli, indipendentemente dalla loro liceità, possono determinare il trattamento di informazioni personali, anche non pertinenti o idonee a rivelare convinzioni religiose, filosofiche o di altro genere, opinioni politiche, lo stato di salute o la vita sessuale (cfr. § 5.2 e 6.1 del provv. Del Garante del 1° marzo 2007 "Lavoro: le linee guida del Garante per posta elettronica e internet" pubblicate in G. U. n. 58 del 10 marzo 2007).
AGEC si riserva di effettuare controlli, in conformità alle leggi vigenti e nel pieno rispetto dello statuto dei lavoratori, saltuari o occasionali, sull'uso dei servizi indicati in questo Regolamento, con particolare attenzione all'uso del Pc (fisso o portatile), della Posta elettronica e di Internet.
In caso di anomalie, il personale incaricato deL Servizio Sistemi Informatici effettuerà controlli anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base più ristretta o anche individuale potranno essere computi solo in caso di successive ulteriori anomalie.
Tali controlli saranno effettuati per verificare la funzionalità e la sicurezza del sistema. Nel caso di individuazione di abusi singoli o reiterati, si procederà come segue:

- 1° avviso collettivo tramite e-mail a tutti gli utenti aziendali ("all users")
- 2° avviso collettivo tramite e-mail agli utenti facenti parte di uno specifico ufficio

- 3° avviso individuale tramite e-mail ad un utente specifico.

In alcun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

## *20. Trattamenti cartacei*

In base al principio di stretta pertinenza dei trattamenti rispetto alle mansioni svolte, ogni incaricato potrà accedere agli archivi relativi alle banche dati di tipo cartaceo ubicate negli uffici di appartenenza. Gli archivi contenenti dati sensibili e/o giudiziari sono ad accesso selezionato e riservato alle sole persone autorizzate.
L'incaricato, nel trattare documenti contenenti dati particolari, è tenuto a custodirli fino alla restituzione in modo da evitare l'accesso agli stessi da parte di persone prive di autorizzazione. L'accesso fuori dell'orario di lavoro impone la registrazione e identificazione delle persone ammesse ai locali.
I documenti (o copia degli stessi) non possono, senza specifica autorizzazione, essere portati fuori dai luoghi di lavoro, salvo i casi di comunicazione dei dati a terzi preventivamente autorizzati in via generale da AGEC L'incaricato del trattamento deve inoltre controllare che i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici, composti da numerose pagine o più raccoglitori, siano sempre completi e integri; al termine dell'orario di lavoro l'incaricato del trattamento deve riportare tutti i documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici, nei locali individuati per la loro conservazione. I documenti contenenti dati personali trattati senza l'ausilio di strumenti elettronici non devono essere mai lasciati incustoditi sul tavolo durante l'orario di lavoro. Quando i documenti devono essere portati al di fuori dei locali individuati per la loro conservazione o addirittura all'esterno del luogo di lavoro, l'incaricato del trattamento deve tenere sempre con sé la cartella o la borsa, nella quale i documenti sono contenuti. E' proibito discutere, comunicare o comunque trattare dati personali per telefono, se non si è certi che il destinatario sia un incaricato autorizzato a potere trattare i dati in questione. Si raccomanda vivamente di non parlare mai ad alta voce, trattando dati personali per telefono, soprattutto utilizzando apparati cellulari, in presenza di terzi non autorizzati, per evitare che i dati personali possano essere conosciuti da terzi non autorizzati, anche accidentalmente. Queste precauzioni diventano particolarmente importanti quando il telefono è utilizzato in luogo pubblico od aperto al pubblico.
Per tuto quanto non espressamente riportatosi farà riferimento al Regolamento degli Archivi di AGEC ed al Manuale di Gestione del Protocollo informatico.

## *21. Obbligo di fedeltà*

AGEC ricorda in via formale che i dipendenti e collaboratori tutti sono tenuti alla rigorosa osservanza dell'obbligo di fedeltà secondo quanto espressamente previsto, in via generale, dall'art. 2105 Cod. Civ. che, fra l'altro, fa espresso divieto a ciascun prestatore di lavoro di "divulgare notizie attinenti all'organizzazione" e "ai metodi di produzione dell'impresa", o fame uso in modo da poter "recare ad essa pregiudizio".
Ciascun dipendente e collaboratore deve quindi astenersi non solo dai comportamenti espressamente vietati dall'art. 2105 Cod. Civ. ma anche da tutti quei comportamenti che, per la loro natura e le loro conseguenze, possano creare situazioni di conflitto ovvero di pregiudizio per le finalità e gli interessi dell'Azienda stessa o siano idonei, comunque, a ledere il presupposto fiduciario del rapporto di lavoro.
A mero titolo esemplificativo si ricorda che a ciascun dipendente e collaboratore è fatto espresso divieto di sottrarre documenti aziendali, di utilizzarne il contenuto, a vantaggio proprio ovvero di terzi, di rivelare dati e notizie riservate della Azienda, non solo tecniche, acquisite in occasione del rapporto di lavoro, potendo derivare da simili condotte una responsabilità anche di rilievo penale, integrando esse i reati sanzionati dall'art. 624 Cod. Pen. in tema di "Furto" dall'art. 623 Cod. Pen. in tema di "Rivelazione di segreti scientifici o industriali".

Ciascun dipendente e collaboratore è tenuto al rispetto delle norme in materia di protezione del diritto d'autore di cui alla Legge 22 aprile 1941, n. 633, la cui violazione potrebbe integrare, ad esempio, le fattispecie penali di cui all'art. 171 (Divulgazione di opere dell'ingegno attraverso rete telematica) e all'art. 171-bis (Reati in materia di software e banche dati) della medesima Legge n. 633/1941. È espressamente vietato l'impiego per finalità aziendali di beni tutelati da diritti d'autore acquisiti in elusione dei relativi obblighi o comunque con modalità difformi da quelle previste dal titolare. È inoltre espressamente vietato l'impiego di beni aziendali (come fotocopiatrici, sito web o altro) al fine di porre in essere condotte che violino la tutela dei diritti d'autore, quale che sia il vantaggio perseguito.
Si ricorda che chi fosse o venisse a conoscenza di comportamenti equivoci e/o potenzialmente dannosi per l'Azienda da parte di collaboratori, di ex-collaboratori, fornitori, concorrenti ovvero di terzi in generale (ad esempio: richieste di specifiche o di disegni tecnici, di nominativi di Clienti o fornitori, ecc.) è tenuto ad informare prontamente la Direzione Generale e tanto sia per evitare qualsiasi danno a carico della Società, sia per evitare di essere incautamente coinvolto in atti di favoreggiamento a favore ed in concorso con quanti cerchino di danneggiare la AGEC in violazione dei diritti delle Aziende stesse.
AGEC espressamente si riserva e fa salva ogni iniziativa ed azione a tutela delle proprie ragioni e posizioni ove vengano accertati comportamenti da parte dei propri dipendenti e collaboratori contrari agli obblighi di fedeltà, di lealtà, di - correttezza e di riservatezza sopra richiamati, potendo tra l'altro detti comportamenti integrare gli estremi della giusta causa ovvero del giustificato motivo di licenziamento nei confronti dei dipendenti responsabili e comunque giustificare la irrogazione di sanzioni disciplinari.

## *22. Norme basilari di uso degli strumenti informatici*

Al fine di evitare problemi correlati ad infezioni informatiche, dovranno essere rispettate almeno le seguenti prescrizioni:

1. i supporti removibili (a titolo esemplificativo ma non esaustivo per supporto removibile si intende: CD, DVD, Schede di memoria SD, dispositivi esterni USB) non possono essere utilizzati sugli strumenti informatici se non previo controllo da parte del Servizio Sistemi Informatici.
2. è obbligatorio sottoporre a controllo tutti i supporti removibili di provenienza incerta prima di eseguire o caricare uno qualsiasi dei file in esso contenuti;
3. limitare la trasmissione di file eseguibili (.COM, .EXE, .OVL, .OVR) e di sistema (.SYS) tra computer in rete;
4. il personale del Servizio Sistemi Informatici non deve utilizzare il server di rete come stazione di lavoro;
5. non aggiungere mai dati o file ai supporti removibili contenenti programmi originali.

<u>Regole operative</u>

1. Tutti i computer dell'Azienda devono essere dotati di programmi antivirus;
2. Il Responsabile deve assicurarsi che i computer delle società esterne, qualora interagiscano con proprio sistema informatico, siano dotati di adeguate misure di protezione antivirus;
3. Il personale delle ditte addette alla manutenzione dei supporti informatici devono usare solo dischetti preventivamente controllati e certificati singolarmente ogni volta;
4. Ogni P.C. deve essere costantemente sottoposto a controllo anti-virus;
5. I supporti di memorizzazione quali, a titolo di esempio non esaustivo CD, DVD, Floppy, USB Drive, Smartphone, provenienti dall'esterno devono essere sottoposti a verifica da attuare con un dispositivo non connesso alla rete (macchina da quarantena), ed inoltre devono essere individuate le aree dell'Amministrazione che, in relazione alla loro particolare attività, sono da considerare a più alto rischio nei riguardi dell'infezione da virus;

6. All'atto della individuazione di un'infezione il virus deve essere immediatamente rimosso;
7. Tutti gli utenti del sistema informatico devono sapere a chi rivolgersi per la disinfezione e l'informazione dell'infezione deve essere mantenuta riservata;
8. Il personale deve essere a conoscenza che la diffusione dei virus è punita dagli artt. 615-quinquies, 635-bis, 635-ter, 635-quater e 635-quinquies del Codice Penale.
9. Il software acquisito deve essere sempre controllato contro i virus e verificato perché sia di uso sicuro prima che sia installato.

## *23. Caratteristiche di base del software antivirus*

Il software antivirus deve essere sottoposto a costante e frequente aggiornamento (almeno 1 volta a settimana) ed in particolare:

a. gli aggiornamenti devono essere resi disponibili non solo per posta ma anche tramite Internet;
b. deve essere particolarmente efficace contro i virus della nostra area geografica
c. deve poter effettuare automaticamente una scansione ogni volta che viene avviato un programma
d. deve poter effettuare una scansione automatica del floppy disk e comunque dei supporti di memorizzazione esterni come gli USB drives.
e. deve accorgersi del tentativo di modificare le aree di sistema
f. deve essere in grado di effettuare scansioni a intervalli regolari e programmati
g. deve essere in grado di effettuare la scansione all'interno dei file compressi
h. deve mantenere il livello di protezione in tempo-reale
i. deve eseguire la scansione in tempo reale
j. deve poter eseguire la rimozione del codice virale in automatico
k. in caso di impossibilità di rimozione i file non pulibili devono essere spostati una sub directory predefinita
l. deve essere attivo nella protezione per Applet di ActiveX e Java contenenti codice malizioso
m. deve essere in grado di effettuare la rilevazione la pulizia dei virus da Macro sconosciute
n. deve essere in condizione di rilevare e rimuovere i virus da macro senza file pattern con un grado di riconoscimento superiore al 97%
o. deve essere in grado di riconoscere i codici virali anche in file compattati utilizzando qualsiasi programma di compressione e in qualsiasi ambiente operativo

Considerato che in sistemi basati su reti locali o su reti geografiche, aumenta il pericolo di diffusione dei virus, ove possibile il sistema antivirus deve essere centralizzato e predisposto a svolgere almeno le funzioni di:

1. distribuzione degli aggiornamenti sia dei motori di scansione che degli eventuali file "pattern"
2. controllo e monitoraggio degli eventi virali
3. automatico spostamento in directory di "quarantena" di virus informatici risultati non pulibili
4. avviso all'amministratore di sistema di rilevazione di virus e indicazione del file "infetto".

## *24. Osservanza delle disposizioni in materia di Privacy*

È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicate nella lettera di designazione di Incaricato del trattamento dei dati.
Gli strumenti tecnologici considerati nel presente Regolamento costituiscono tutti strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa, anche ai sensi e per gli effetti dell'art. 4, comma secondo, della Legge n.300/1970; conseguentemente, le informazioni raccolte sulla base di quanto indicato nel Regolamento, possono essere utilizzate a tutti i fini connessi al rapporto di lavoro, essendone stata data informazione ai lavoratori sulle modalità di uso degli strumenti stessi, sugli interventi che potranno venir compiuti nel sistema informatico aziendale ovvero nel singolo strumento e sui conseguenti sistemi di controllo che potessero

venir eventualmente compiuti (conformemente al precedente capitolo 19), fermo restando il rispetto della normativa in materia di protezione dei dati personali (GDPR 679/2016).
Viene, infine, precisato che non sono installati o configurati sui sistemi informatici in uso agli utenti apparati hardware o strumenti software aventi come scopo il loro utilizzo come strumenti per il controllo a distanza dell'attività dei lavoratori; peraltro, lì dove l'adozione di tali apparati risultasse necessaria per finalità altre, es. esigenze organizzative e produttive, di sicurezza del lavoro e/o di tutela del patrimonio aziendale, AGEC provvederà conformemente a quanto disposto dall'art.4, comma primo, della Legge n.300/1970, dandone anche opportuna informazione agli utenti stessi.

## *25. Violazione dei Dati – Data Breach*

Con il termine data breach si intende un incidente di sicurezza in cui dati personali, protetti o riservati vengono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato. Solitamente il data breach si realizza con una divulgazione di dati riservati o confidenziali all'interno di un ambiente privo di misure di sicurezza (ad esempio, su web) in maniera involontaria o volontaria. Tale divulgazione può avvenire in seguito a:

- **perdita accidentale**: ad esempio, data breach causato da smarrimento di una chiavetta USB contenente dati riservati o confidenziali;
- **furto**: ad esempio, data breach causato da furto di un notebook contenente dati riservati o confidenziali;
- **infedeltà aziendale**: ad esempio, data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico;
- **accesso abusivo**: ad esempio, data breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite.

Ogni collaboratore e/o dipendente e/o Amministratore è tenuto a comunicare immediatamente al Direttore Generale qualsiasi evento, anche solo sospetto, di una violazione di dati. L'Azienda adotta delle apposite procedure di gestione e di risposta in ottemperanza al Regolamento UE 679/2016.

## *26. Non osservanza della normativa aziendale*

Il mancato rispetto o la violazione delle regole contenute nel presente Regolamento comporta l'assunzione diretta da parte dell'utente delle responsabilità nascenti da tali condotte e determina, nei casi ed entro i limiti previsti dalla vigente normativa, la contestabilità a suo carico di tali comportamenti con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

## *27. Social Media*

L'utilizzo a fini promozionali e commerciali dei social media – quali, a titolo esemplificativo ma non esaustivo, Facebook™, Twitter™, Linkedin™, Google™, dei blog e dei forum, anche professionali – verrà gestito ed organizzato esclusivamente dall'Azienda attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli utenti.
Fermo restando il pieno ed inderogabile diritto della persona alla libertà di espressione ed al libero scambio di idee ed opinioni, l'Azienda ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine ed il patrimonio aziendale, anche immateriale, quanto i propri collaboratori, i propri clienti e fornitori, gli altri partners, oltre che gli stessi utenti utilizzatori dei social media, fermo restando che viene vietata la partecipazione agli stessi social media durante l'orario di lavoro, con l'esclusione dei

dipendenti e collaboratori che hanno tra le mansioni aziendali la gestione e/o monitoraggio dei portali dei social network di AGEC. La policy qui dettata deve venir seguita dagli utenti sia che utilizzino dispositivi messi a disposizione dall'Azienda, sia che utilizzino propri dispositivi, sia che partecipino ai social media a titolo personale, sia che lo facciano per finalità professionali, come dipendenti o collaboratori della stessa Azienda.
La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni aziendali considerate dall'Azienda riservate ed in genere, a titolo esemplificativo e non esaustivo, sulle informazioni finanziarie ed economiche, commerciali, sui piani industriali, sui clienti, sui fornitori ed altri partners dell'Azienda stessa. Inoltre, ogni comunicazione e divulgazione di contenuti dovrà essere effettuata nel pieno rispetto dei diritti di proprietà industriale e dei diritti d'autore, sia di terzi che dell'Azienda; l'utente, nelle proprie comunicazioni, non potrà quindi inserire marchi od altri segni distintivi dell'Azienda, né potrà pubblicare disegni, modelli od altro connesso ai citati diritti. Ogni deroga a quanto sopra disposto potrà peraltro avvenire solo previa specifica autorizzazione della Direzione Aziendale.
L'utente deve garantire la tutela della privacy delle persone; di conseguenza, non potrà comunicare o diffondere dati personali (quali dati anagrafici, immagini, video, suoni e voci) di colleghi e in genere di collaboratori aziendali, se non con il preventivo personale consenso di questi, e comunque non potrà postare nel social media immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro aziendali, se non con il preventivo consenso del Responsabile del proprio d'ufficio, oppure solo per quanto riguarda la piattaforma Facebook sulle pagine di Agec, nel rispetto di quanto definitivo nelle specifiche direttive aziendali di utilizzo di tale strumento.
L'utente risponde personalmente dei propri comportamenti e deve astenersi dal porre in essere, nei confronti in genere di terzi e specificatamente verso l'Azienda, i colleghi, i clienti ed i fornitori, attività che possano essere penalmente o civilmente rilevanti; a titolo esemplificativo ma non esaustivo, sono quindi vietati comportamenti ingiuriosi, diffamatori e denigratori, discriminatori o che configurano molestie. In tal senso, è vivamente auspicato da parte di tutti un comportamento civile e sobrio, in particolar modo in qualunque occasione in cui l'espressione o il contesto in cui essa avviene possa essere collegata all'ambito aziendale.
Infine, in via generale ed ove non autorizzato in senso diverso dal proprio Responsabile d'ufficio, oppure se non diversamente definito nelle specifiche direttive aziendali di utilizzo della piattaforma Facebook, l'utente, nell'uso dei social network, esprimerà unicamente le proprie opinioni personali; pertanto, ove necessario od opportuno per la possibile connessione con l'Azienda, in particolare in forum professionali, l'utente dovrà precisare che le opinioni espresse sono esclusivamente personali e non riconducibili all'Azienda.

## *28. Ulteriori disposizioni per l'utilizzo delle carte di pagamento*

Ai dipendenti possono essere assegnate una o più carte di pagamento:

a) Carta aziendale di credito/debito: la Direzione si riserva il diritto di valutare le figure professionali eleggibili di tale strumento. In caso di furto o smarrimento, oltre a quanto previsto dal regolamento del gestore della carta consegnato contestualmente alla carta stessa, il dipendente è tenuto a darne tempestiva comunicazione all'Ufficio Tesoreria.

AGEC utilizzerà le informazioni sulla data, luogo, importo e modalità di pagamento esclusivamente ai fini di sicurezza, controllo di gestione e corrispondenza ai limiti previsti nonché per la prevenzione frodi.

## *29. Cessazione del rapporto di lavoro*

In caso di cessazione del rapporto di lavoro, per il corretto trattamento dei dati personali effettuato con gli strumenti elettronici aziendali e, come indicato nel presente Regolamento, premettendo che:

a) la posta elettronica, sia interna che esterna, è un mezzo di comunicazione messo a disposizione del dipendente o collaboratore esclusivamente per consentirgli lo svolgimento della propria attività lavorativa, avendo raccomandato di evitare l'utilizzo di tali strumenti per motivi non attinenti allo svolgimento delle mansioni assegnate, salvo casi eccezionali di comprovata urgenza;
b) salvo casi eccezionali di comprovata necessità, le unità di rete sono aree destinate alla condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Avendo raccomandato di non collocare, anche temporaneamente, in queste aree qualsiasi file che non sia attinente allo svolgimento dell'attività lavorativa;

L'utente, con anticipo di almeno sette giorni rispetto alla data di cessazione del rapporto di lavoro, è tenuto a:

a) eliminare, dalla propria casella di posta elettronica, solo gli eventuali messaggi personali;
b) eliminare dal disco di rete K:\ solo gli eventuali file personali;
chiedere l'intervento di un amministratore di sistema per:
c) copiare i dati aziendali accessibili nel disco locale del proprio pc in una posizione accessibile al proprio responsabile per successive consultazioni.
d) Eliminare i dati personali da eventuali dispositivi portatili aziendali dati in uso esclusivo.

L'amministratore di sistema, al termine dell'ultimo giorno di lavoro del dipendente o collaboratore, o al massimo entro il giorno lavorativo successivo, provvederà a:

a) disattivare l'utenza di rete (login di Windows) assegnata precedentemente al dipendente/collaboratore, provvedendo ad eliminarla definitivamente entro 30 giorni;
b) solo nel caso fosse assegnato un indirizzo email aziendale di tipo nome.cognome@agec.it, inserire nel sistema di posta elettronica un autorisponditore che segnalerà al mittente la disattivazione della casella di posta elettronica ed i dettagli sulle future comunicazioni verso l'Azienda. La casella di posta elettronica, comunque non più accessibile da nessuno, verrà definitivamente eliminata dal sistema entro 30 giorni (salvo diversi accordi).
c) Cancellare tutti i dati personali, se presenti, dai dispositivi aziendali, fermo restando che è onere del responsabile del dipendente/collaboratore verificare che lo stesso abbia correttamente consegnato i dati aziendali oppure richiedere per tempo all'amministratore di sistema di effettuare tale operazione per conto del dipendente/collaboratore.
d) Solo in casi eccezionali e documentati Agec potrà inoltrare le mail indirizzate al dipendente dimissionario ad altra casella di servizio. L'inoltro ad altra casella verrà attivato esclusivamente nei casi in cui l'indirizzo email sia associato a particolari servizi esterni (a titolo esemplificativo e non esaustivo le credenziali di accesso ad un servizio di newsletter) e verrà lasciato attivo per il tempo necessario alla comunicazione del cambio di associazione che dovrà essere comunicato da AGEC ai fornitori dei servizi esterni.
e) E' sempre prevista l'attivazione della risposta automatica al mittente con indicazione specifica riguardo alla nuova casella email a cui ci si deve rivolgere;

L'utente dovrà consegnare tutti i beni aziendali ricevuti in dotazione.
Si ricorda inoltre che l'utente, entro una settimana dalla data di cessazione, è tenuto ad aggiornare coerentemente i propri profili social.

## *30. Dismissione degli strumenti aziendali.*

Gli Strumenti Aziendali devono essere considerati in tutto il loro ciclo di vita e, dunque, regole di comportamento devono essere seguite anche quando diventano inservibili o, per qualsiasi causa, devono essere dismessi.
Nel seguito, come prescritto nel Provvedimento del Garante per la Protezione dei Dati Personali "Rifiuti di apparecchiature elettriche ed elettroniche (RAAE) e misure di sicurezza dei dati personali" del 13 ottobre 2008, si elencano le regole da rispettare per rottamare Strumenti Aziendali, quando non sono più utilizzabili poiché non funzionanti o, per qualsiasi motivo, non si intende più utilizzarli, nonché quando gli Strumenti Aziendali vengono smarriti o illecitamente sottratti.
Una volta effettuata la ricognizione dei dati contenuti nello Strumento Aziendale (che per definizione possono essere utilizzati solo per scopi lavorativi) da parte dell'assegnatario, l'Amministratore di Sistema e/o il personale dei Sistemi Informativi autorizzato e/o l'Azienda Esterna e/o il Consulente esterno incaricati delle attività di gestione sistemistica, provvedono ad applicare misure tecniche per la cancellazione sicura dei dati tramite programmi (es. wiping program) che provvedono a distruggere i dati ivi contenuti in modo crittograficamente sicuro o comunque a renderli totalmente irrecuperabili. L'effettiva cancellazione dei Dati Personali dai supporti contenuti negli strumenti elettronici può anche risultare dai seguenti metodi, anche secondo il tipo di Strumento Aziendale da dismettere:

- sistemi di punzonatura o deformazione meccanica;
- distruzione fisica;
- demagnetizzazione ad alta intensità.

Le tecniche usate dovranno essere in ogni caso adeguate agli standard internazionali. La stessa procedura si applica ai supporti cartacei - contenenti Dati Personali e/o informazioni aziendali - per i quali viene utilizzato, se del caso, un distruggi-documenti. Qualora i dati non siano stati cancellati prima della consegna dello Strumento Aziendale a un rottamatore, l'Azienda richiederà al rottamatore una dichiarazione scritta di garanzia di avere distrutto lo Strumento Aziendale consegnato e di non avere acceduto ai dati in esso contenuti o ceduti a terzi, né di averne tratto copie, né cartacee né informatiche, né totali né parziali

## *31. Aggiornamento e revisione*

Tutti gli utenti possono proporre, quando ritenute necessarie, integrazioni al presente Regolamento. Le proposte verranno esaminate dalla Direzione aziendale.
Il presente Regolamento è soggetto a revisione.