Sommario

/

Premessa

L'ambito lavorativo porta la nostra organizzazione a gestire una serie di "informazioni", proprie e di terzi, per poter erogare i servizi che le vengono contrattualmente richiesti.

Tali informazioni possono essere considerate, ai sensi del Regolamento UE 2016/679 (GDPR), "dati personali" quando sono riferite a persone fisiche e per la loro gestione (Trattamento), sia cartacea che automatizzata, è necessario che la azienda adotti una serie di misure minime ed idonee previste dalle norme.

Altre informazioni, pur non essendo "dati personali" ai sensi di legge, sono in tutto e per tutto "informazioni riservate", ovvero informazioni tecniche, commerciali, contrattuali, di business o di altro genere per le quali l'organizzazione è chiamata a garantire la riservatezza, o per NDA, o per una più ampia tutela del patrimonio aziendale.

Ai fini di questo disciplinare si specifica, pertanto, che con il termine "dati" deve intendersi l'insieme più ampio di informazioni di cui un dipendente o un collaboratore può venire a conoscenza e di cui deve garantire la riservatezza e la segretezza e non solo i "dati personali" intesi a norma di legge (fare riferimento a: registro trattamento dei dati); Dettagli di trattamento si evidenziano nel Registro trattamenti con le analisi dei rischi per ogni banca dati.

Anche nei rapporti interni tra colleghi o collaboratori, la circolazione dei dati personali deve essere limitata ai soli casi strettamente necessari per l'espletamento dell'attività lavorativa (principio di minimizzazione).

Il presente regolamento costituisce parte integrante delle istruzioni impartite agli autorizzati e la sua osservanza è fondamentale per prevenire violazioni della privacy (Data Breach) e garantire i diritti degli interessati.

Il presente Regolamento Interno si applica agli autorizzati che si trovino ad operare con dati della azienda (cioè coloro che sottoscrivono le nomine ad autorizzato al trattamento dei dati personali).

Una gestione dei dati cartacei, un uso dei COMPUTER CELLULARI, TABLET e di altri dispositivi elettronici (di seguito anche dispositivi nonché dei servizi di internet e della posta elettronica difforme dalle regole contenute nel presente Disciplinare potrebbe esporre l'organizzazione ad aumentare la minaccia di accessi non autorizzati ai dati e/o al sistema informatico aziendale, furti o divulgazioni di informazioni riservate nonché furti o danneggiamenti del sistema informatico e/o malfunzionamenti in generale dell'intero sistema informatico.

Le informazioni contenute nel presente Disciplinare vengono rilasciate anche ai sensi dell'art. 13 del Regolamento UE 2016/679 (GDPR) e costituiscono, quindi, parte integrante dell'informativa rilasciata agli autorizzati.

Il presente regolamento integra le disposizioni di cui agli artt. 2104 e 2105 codice civile, quelle dei CCNL e delle procedure e regolamenti adottati in azienda e trova applicazione nei confronti dei dipendenti o di altro personale, anche esterno, (da qui in avanti anche detti "utenti") che, in ragione delle mansioni e/o delle attività assegnate e del lavoro e/o della collaborazione da svolgersi, abbiano in dotazione un personal computer, un cellulare o altro dispositivo con connessione a Internet, nonché una casella di posta elettronica aziendale e operano nell'ambito del trattamento di dati personali.

Considerato inoltre che **GRAFICHE ANTIGA S.P.A.**, nell'ottica di uno svolgimento proficuo e più agevole della propria attività, ha da tempo deciso di mettere a disposizione dei propri collaboratori, che ne necessitassero per il tipo di funzioni svolte, telefoni e mezzi di comunicazione adeguati (computer portatili, telefoni cellulari, tablet, etc.), sono state inserite nel regolamento alcune clausole relative alle modalità ed i doveri che ciascun dipendente deve osservare nell'utilizzo di tale strumentazione.

1. Utilizzo del Personal Computer

Il Personal Computer e, più in generale qualsiasi strumento e/o mezzo informatico, affidato al dipendente è da considerarsi a tutti gli effetti uno **strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa che prevede il coinvolgimento di dati personali può contribuire alla lesione dei diritti dell'interessato, ciò potrebbe comportare costi di manutenzione e, soprattutto, minacce alla sicurezza dei dati dell'interessato al trattamento.

L'accesso all'elaboratore è protetto da password che deve essere custodita dall'autorizzato con la massima diligenza e non divulgata. La stessa password deve essere attivata per l'accesso alla rete, per lo screen

/

saver e per il collegamento ad Internet. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte dell'Incaricato della gestione e manutenzione dei Sistemi Elettronici.

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, ivi compresi gli archivi di posta elettronica interna ed esterna, secondo quanto previsto al punto 6 del presente regolamento.

Il custode delle parole chiave o un suo incaricato potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere alla stessa Azienda, titolare del trattamento, di accedere ai dati trattati da ogni autorizzato con le modalità fissate dalla stessa Azienda, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività della Azienda 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.

Non è consentito installare autonomamente programmi provenienti dall'esterno senza la previa autorizzazione esplicita dell'Incaricato della gestione e manutenzione dei Sistemi Informatici, poiché esiste il serio rischio di introdurre virus informatici e di compromettere la stabilità delle applicazioni del sistema. Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente dal responsabile dei sistemi informativi della **GRAFICHE ANTIGA S.P.A.**.

Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo previa autorizzazione esplicita dell'Incaricato della gestione e manutenzione dei Sistemi Informatici.

Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici.

Non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, chiavette UMTS, etc.), se non con l'autorizzazione espressa dell'Incaricato della gestione e manutenzione dei Sistemi Informatici.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente l'Incaricato della gestione e manutenzione dei Sistemi Informatici nel caso in cui vengano rilevati virus.

Tutti i PC devono essere dotati di SOFTWARE ANTIVIRUS aggiornato costantemente.

2. Utilizzo della rete

Le unità di rete sono aree di condivisione d'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 copiato, nemmeno per brevi periodi, in queste unità. Su tali unità, vengono svolte regolari attività di controllo, amministrazione e backup.

Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite (vedi procedura gestione password psw_01). È assolutamente vietato entrare nella rete e nei programmi con altri nomi utente.

L'Incaricato della gestione e manutenzione dei Sistemi Informatici può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.

Costituisce buona regola la periodica (almeno ogni sei 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 un'archiviazione ridondante.

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 evitare di stampare documenti o file non adatti (molto lunghi o non supportati) su stampanti comuni. In caso di necessità la stampa in corso può essere cancellata.

3. Gestione delle Password

La gestione delle password avviene come indicato nella **"Policy password"**.

In ogni caso l'incaricato deve:

- Mantenere segreta la password.
- Comunicare la sua eventuale variazione. Utilizzare password che non contengano riferimenti alla sua persona e/o alla Azienda.
- Utilizzare minimo 8 (otto) caratteri.

/

- Rispettare le indicazioni della suddetta istruzione.

4. Login e Logout

Il "Login" è l'operazione con la quale l'autorizzato si connette al sistema informativo aziendale o ad una parte di esso, dichiarando il proprio Username e Password (ossia l'Account), aprendo una sessione di lavoro. In molti casi è necessario effettuare più login, tanti quanti sono gli ambienti di lavoro (ad es. applicativi web, Intranet), ognuno dei quali richiede un username e una password. Tali utenze e le persone che eventualmente ne condividono gli accessi devono essere riportate all'interno del registro "REG_UT-Registro Utenti e assegnazione").

In questi casi, sebbene sia preferibile che ogni utente abbia un suo specifico user name e password, l'organizzazione potrà assegnare un univoco user name e password per gruppi di incaricati per l'accesso alla macchina fisica, mentre rimarranno separati ed univoci per l'accesso agli applicativi che contengono dati.

Il "Logout" è l'operazione con cui viene chiusa la sessione di lavoro. Al termine della sessione lavorativa, tutte le applicazioni devono essere chiuse secondo le regole previste dall'applicazione stessa.

La non corretta chiusura può provocare una perdita di dati o l'accesso agli stessi da parte di persone non autorizzate.

Il "blocco del computer" è l'operazione con cui viene impedito l'accesso alla sessione di lavoro (tastiera e schermo disattivati) senza chiuderla. Tale operazione deve avvenire ogni volta che l'autorizzato abbandona il posto di lavoro e gli strumenti di accesso ai dati. -

IN OGNI CASO LA PERSONA AUTORIZZATA CHE DEVE LASCIARE IL POSTO DI LAVORO ATTIVA IL BLOCCO DEL COMPUTER (che in sistemi Microsoft avviene con l'uso contemporaneo dei tasti indicati a lato).

Assicurarsi di NON impostare automatismi che permettano di mantenere l'utente "connesso" anche dopo l'interruzione della sessione di lavoro.

5. Utilizzo dei supporti magnetici

Nel caso in cui siano utilizzati supporti informatici quali chiavette usb, schede SSD, cd-rom o nastri per la memorizzazione di dati personali particolari, gli Incaricati devono osservare alcune misure di sicurezza al fine di salvaguardare la riservatezza dei dati:

- i supporti informatici già contenenti dati personali particolari possono essere riutilizzati solo dopo aver provveduto a cancellare i dati e le informazioni in essi contenuti, in modo che non siano tecnicamente ed in alcun modo recuperabili;
- qualora si riscontrassero delle difficoltà nello svolgimento di tali operazioni, si può richiedere l'intervento dell'Incaricato della gestione e manutenzione dei Sistemi Informatici;
- qualora la procedura di cancellazione dei dati risulti inapplicabile, al termine delle operazioni di trattamento i supporti di memoria utilizzati devono essere distrutti;
- fra i supporti di memorizzazione sono ricompresi a pieno titolo i dischi equipaggiati nei computer dimessi e/o sostituiti dai dipendenti.
- **GRAFICHE ANTIGA S.p.A.** non risponderà della perdita dei dati strettamente personali, eventualmente archiviati nella propria postazione di lavoro, il cui trattamento in ogni caso non deve interferire con la normale attività lavorativa. In particolare, tali dati non potranno essere salvati nei server aziendali

L'autorizzato al trattamento dei dati personali ha la responsabilità di:

- segnalare la necessità di un'eventuale riparazione degli hard disk;
- segnalare la necessità di un'eventuale dismissione dei CD-ROM, dei nastri magnetici, delle chiavette USB e delle schede SSD, o altro supporto;
- segnalare la necessità di un'eventuale dismissione degli hard disk, dei nastri magnetici, delle chiavette USB e delle schede SSD, o altro supporto;
- eseguire la re-inizializzazione delle chiavette USB e delle schede SSD o altro supporto per poterli successivamente riutilizzare;

/

- effettuare il test sulla re-inizializzazione, delle chiavette USB e delle schede SSD o altro supporto eseguita precedentemente.

Le attività d'uso e riuso sono possibili solo se disposte ed autorizzate specificatamente dal proprio Responsabile e/o Titolare ed ogni caso non devono in alcun modo pregiudicare I livelli di sicurezza richiesti dall'attività specifica della nostra organizzazione.

I supporti magnetici contenenti dati particolari (ex dati sensibili) e giudiziari devono essere custoditi in archivi chiusi a chiave.

6. Utilizzo di PC portatili

L'utente è responsabile del PC portatile assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

I PC portatili utilizzati all'esterno (convegni, visite in Azienda, etc...), in caso di allontanamento, devono essere custoditi in un luogo protetto.

Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

7. Utilizzo delle stampanti e dei materiali di consumo

L'utilizzo delle stampanti e dei materiali di consumo in genere (carta, inchiostro, toner, cd-rom, dvd, ecc) è riservato esclusivamente ai compiti di natura strettamente istituzionale. Devono essere evitati in ogni modo sprechi dei suddetti materiali o utilizzi eccessivi e/o copie ridondanti. Non è consentito lasciare incustoditi presso le stampanti documenti cartacei contenenti dati sensibili o riservati.

8. Gestione delle firme elettroniche/PEC

Nel caso fossero presenti firme elettroniche del Titolare del Trattamento, queste devono essere utilizzate solo dal proprietario e/o il delegato, che detiene i codici per l'utilizzo. Qualora si renda necessario l'utilizzo di una firma elettronica e non sia presente il proprietario della medesima, l'uso è consentito solo a persona debitamente delegata per iscritto a tale attività dal proprietario. La delega deve specificare quali siano gli utilizzi consentiti.

9. Antivirus

La Azienda è dotata di un antivirus centralizzato installato su tutte le postazioni client collegate in rete, pur tuttavia ciascun utente deve tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.

Nel caso in cui il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente:

- sospendere ogni elaborazione in corso senza spegnere il computer;
- eseguire la scansione del PC e/o del dispositivo su cui è stato rilevato il virus;
- qualora l'antivirus non sia riuscito a rimuovere l'infezione, segnalare l'accaduto al personale del Sistema Informativo.

Non è consentito l'utilizzo di dispositivi esterni e/o supporti di memorizzazione di provenienza ignota. Ogni dispositivo di memorizzazione dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus non curato dall'antivirus, dovrà essere consegnato al personale del Sistema Informativo.

10. Web-conference ed utilizzo di strumenti di comunicazione vocale e video su internet

È consentita la partecipazione a web-conference e a sessioni di comunicazione multimediale esclusivamente per usufruire di corsi per l'approfondimento di tematiche specifiche legate alla formazione personale o per condurre attività comunque previste dall'Azienda (compreso lo smart-working).

Non sono consentite le comunicazioni interpersonali audio e video su Internet, quando non espressamente autorizzate in seno di attività o progetti. Per le attività di web conference/web collaboration è consentito esclusivamente l'utilizzo degli strumenti espressamente attivati e messi a disposizione dall'Azienda.

Non è consentito l'utilizzo di alcuno strumento o servizio sul sistema ICT che non sia fornito direttamente o non sia stato espressamente o implicitamente autorizzato; analoga regolamentazione subiscono i servizi usufruibili su Internet.

/

11. Teleassistenza

Relativamente alle attività di manutenzione remota su personal computer connessi alla rete aziendale e/o Sistema Informativo, il personale delle aziende che assicurano la manutenzione dei software in uso potrà utilizzare specifici software. Tali programmi vengono utilizzati per assistere l'utente durante la normale attività informatica ovvero per svolgere manutenzione su applicativi e su hardware. L'attività di assistenza e manutenzione avviene previo avviso all'utente interessato che può rifiutare tale tipo di assistenza allungando però in questa maniera i tempi d'intervento. La configurazione del software prevede un indicatore visivo sul monitor dell'utente che segnala quando un tecnico è connesso al personal computer.

12. Utilizzo Logo aziendale

L'uso del marchio è di competenza esclusiva e riservata dell'Azienda.

Il personale, nella produzione di documenti e strumenti di comunicazione istituzionale, deve sempre garantire l'identità visiva dell'Azienda utilizzando i formati (carta intestata, moduli, locandine, slide, ecc.) disponibili nella intranet aziendale.

L'uso del marchio dell'Azienda da parte di soggetti esterni deve essere sempre espressamente e preventivamente autorizzato dalla Direzione.

13. Uso della posta elettronica

Il dipendente può accedere alla sua casella di posta elettronica da tutti gli strumenti che utilizza (*Desktop*, *Laptop*, *Tablet*, Telefono Mobile). Gli strumenti dovranno essere dotati dei minimi requisiti di sicurezza definiti dal presente documento; l'Area IT può richiedere l'eventuale installazione di appositi applicativi di sicurezza.

Nell'utilizzo del servizio ciascun utente è tenuto a attivare, in caso di assenza prolungata, la funzione di risposta automatica che inviti il mittente a prendere contatto con altre risorse della azienda (in caso di cessazione/dimissione del dipendente il Responsabile IT dovrà procedere alla chiusura ed eliminazione dell'account di posta e si dovrà procedere ad informare i mittenti del dipendente cessato a prendere contatto con altre risorse della azienda).

La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e allegati ingombranti che potrebbero saturare lo spazio disponibile. Il tempo di conservazione dei messaggi di posta è illimitato.

I messaggi inviati o ricevuti dall'Utente sono raccolti sui server di posta elettronica aziendale, in cui rimangono conservati in base allo spazio di memoria disponibile per la casella assegnata a ciascun utente, secondo le prassi aziendali.

I contenuti delle singole caselle di posta elettronica sono soggetti a periodico backup.

Le informazioni contenute nei messaggi di posta elettronica sono da considerarsi riservate e confidenziali.

Il loro utilizzo è consentito esclusivamente al destinatario in indirizzo e ne è vietata la diffusione in qualunque modo eseguita, salvo che ne sia data espressa autorizzazione da parte del mittente.

È fatto divieto di utilizzare le caselle di posta elettronica elencate nel registro ei trattamenti e assegnazione per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica aziendale per:

- la ricezione e l'invio di messaggi di posta che contengono allegati con le caratteristiche di tipo eseguibile o di applicazione. Si precisa che il sistema di sicurezza e antivirus installato a protezione del server di posta elettronica della Azienda non consente comunque tale operazione. Eventuali esigenze particolari possono essere segnalate per individuare la soluzione tecnica più appropriata;
- trasmettere a soggetti esterni alla nostra organizzazione informazioni riservate o comunque documenti aziendali, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte, per l'adempimento di un obbligo di legge o di contratto di cui sia parte della nostra organizzazione o al fine di difendere un diritto della nostra organizzazione;
- l'invio di messaggi aventi contenuto lesivo per la reputazione della azienda a e che gettino discredito sulla medesima o il compimento di qualsiasi atto o fatto illecito attraverso l'utilizzo della casella aziendale che possano far attribuire alla nostra organizzazione ed a chi la rappresenta una responsabilità penale, civile od amministrativa;

/

- effettuare l'invio e l'archiviazione di messaggi di posta elettronica aventi natura oltraggiosa e/o discriminatoria;
- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es.mp3) non legati all'attività lavorativa; l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
- la partecipazione a catene telematiche (comunemente dette "di Sant'Antonio"). Se si dovessero peraltro ricevere messaggi di tale tipo, si dovrebbe comunicarlo immediatamente al Responsabile IT. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi;
- Eseguire o favorire pratiche di spamming;
- Utilizzare la login/password di un altro utente per accedere in sua assenza alla sua posta elettronica

I Responsabili incaricati, qualora ravveda situazioni particolarmente gravi e/o abusi del servizio, è tenuto ad informare la Direzione che provvederà alla contestazione delle mancanze rilevate.

Il Titolare può definire sistemi di controllo del traffico dati ed imposta dei limiti su tali attività per poter generare degli "alert" che permettano di rilevare usi scorretti e pericoli delle reti.

Qualora si debba conoscere il contenuto dei messaggi di posta elettronica delle caselle elencate nel registro dei trattaemnti, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa e/o alla sicurezza dei dati e per garantire i requisiti del S.G.P. si potranno attivare da parte del Responsabile IT procedure di accesso ai dati di tali "caselle", mantenendo comunque la riservatezza riguardo ad informazioni di cui potrebbe venire a conoscenza e provvedendo poi a comunicare all'interessato (proprietario della casella) la procedura attivata, segnalando la necessità di modificare la password di accesso. **Il personale è informato delle caselle di posta elettronica che sono condivise con altri utenti.**

14. Uso della rete Internet e dei relativi servizi

Il PC abilitato alla navigazione in Internet costituisce uno strumento della Grafiche Antiga S.p.A. necessario allo svolgimento della propria attività lavorativa

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.

Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, **Grafiche Antiga S.p.A.** si riserva di adottare uno specifico sistema di blocco o filtro automatico che prevenga determinate operazioni quali *l'upload*, il *download* o l'accesso a determinati siti inseriti in una *black list*. Gli eventuali controlli, compiuti dal personale incaricato, potranno avvenire mediante un sistema di controllo dei contenuti (*Proxy server*, *Web Filtering*) o mediante "file di log" della navigazione. La consultazione, ai soli fini lavorativi, di specifici siti bloccati dai sistemi di web filtering, se presenti, sarà possibile attraverso l'abilitazione su richiesta all'accesso che deve essere fatta al Responsabile IT; si ricorda che è necessario indicare l'esatto indirizzo del sito internet da abilitare ed il motivo della richiesta.

L'utente è direttamente responsabile, civilmente e penalmente, a norma delle vigenti leggi, per l'uso fatto del servizio internet. La responsabilità si estende anche alla violazione degli accessi protetti, del copyright e delle licenze d'uso. I log potranno essere oggetto di verifica e di provvedimenti dell'Autorità giudiziaria e amministrativa e in generale dei soggetti aventi funzioni ispettive e di controllo.

La Direzione potrà autorizzare:

- la registrazione a siti i cui contenuti non siano legati direttamente all'attività lavorativa;
- lo scarico di *software*;
- gli acquisti on-line;
- la partecipazione a Forum non specificatamente professionali;
- l'utilizzo di *chat line*, *social network*, di bacheche elettroniche e le registrazioni in *guest books*, a fronte di specifica richiesta presentata dal Responsabile;

È espressamente vietato:

- accedere ai servizi informatici aziendali e/o alle banche dati aziendali non possedendo le credenziali di accesso o mediante l'utilizzo delle credenziali di colleghi autorizzati;
- la navigazione su Social Network di qualsiasi tipo (ad es. Facebook, Twitter, Youtube, etc.), esclusi quelli

espressamente approvati dalla Direzione e per soli motivi professionali;
- l'installazione, la configurazione e l'utilizzo di software "Peer-To-Peer" (P2P tipo eMule e similari) il quale, oltre a saturare le risorse di banda internet disponibili è veicolo di potenziali e gravissimi rischi per la sicurezza del sistema informatico aziendale nonché può verificarsi il concreto rischio di scarico di materiale illegale (v. Legge sul Diritto d'Autore) e/o pedo-pornografico;
- l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa;
- il download di file del tipo MP3, AVI, MPG, Quicktime e/o altri tipi di file o programmi per la fruizione di contenuto audio/video non legati all'attività lavorativa;
- ricerche e/o consultazioni di siti unicamente per scopi personali;
- l'accesso, tramite internet, a caselle webmail di posta elettronica personale;
- la navigazione su siti appartenenti alle categorie Pedo-Pornografia, Violenza, Razzismo e, in generale, è espressamente vietata la navigazione e ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
- introdursi abusivamente in un sistema informatico o telematico protetto da misure di sicurezza contro la volontà del titolare del diritto all'accesso anche al fine di acquisire informazioni riservate;
- accedere in maniera non autorizzata ai sistemi informativi della pubblica amministrazione o alterarne in qualsiasi modo il funzionamento o intervenire con qualsiasi modalità cui non si abbia diritto su dati, informazioni o programmi contenuti in sistema informatico o telematico o a questo pertinenti, per ottenere e/o modificare informazioni a vantaggio della Cooperativa o di terzi o comunque al fine di procurare un indebito vantaggio alla Azienda od a terzi;
- distruggere, deteriorare o rendere inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati utilizzati dallo Stato o da altro ente pubblico o ad esso pertinente o comunque di pubblica utilità;
- condurre, in una qualsiasi forma, attacchi telematici a terzi e/o strutture e/o strumenti digitali a loro appartenenti e, più in generale, qualsiasi azione in violazione delle leggi e delle normative vigenti in materia di Diritto della Privacy, dell'Informatica e delle Telecomunicazioni.

15. Utilizzo dispositivi mobili (smartphone/tablet)

Per "Dispositivo mobile" è da intendersi il telefono cellulare, il tablet, lo smartphone e ogni altro dispositivo che consenta la gestione di comunicazioni telefoniche, audio, video e di applicativi software "in mobilità".

In generale, i dispositivi mobili di proprietà aziendale non possono essere ceduti né fatti utilizzare a terzi, eccetto colleghi, collaboratori, consulenti o soggetti autorizzati. In particolare, alcuni telefoni sono di "uso individuale" e non possono essere ceduti né fatti utilizzare neppure ai colleghi.

In merito all'uso dei *dispositivi* mobili aziendali, quali strumenti di lavoro, si precisa che è proibito, senza alcuna eccezione, modificare la configurazione dei dispositivi mobili e/o installare applicazioni sospette o pirata, manualmente o da uno *store* di applicazioni (Apple Store, Google Play, ...).

Non è consentito l'uso di qualsiasi dispositivo esterno collegabile al dispositivo mobile, se non quelli aziendali o quelli autorizzati.

L'utilizzatore che abbia necessità di apportare modifiche software o hardware al dispositivo mobile aziendale in dotazione, installando nuovi programmi o dispositivi, deve farne preventiva richiesta alla funzione preposta dell'Area IT.

L'utente, ove possibile, deve mantenere aggiornato il sistema operativo e le *app* del dispositivo mobile attraverso le comuni procedure di *software update* messe a disposizione dai *Fornitori.*

L'utente non può forzare direttamente e/o indirettamente né installare sul dispositivo mobile sistemi e/o software che consentano di modificarne le funzionalità, di alterarne le caratteristiche o di "prenderne il controllo" del sistema operativo (ad es.: jailbreak, root, etc...).

I dispositivi mobile aziendali devono avere abilitato il codice di blocco e/o il PIN d'accesso e/o la Password personalizzata, secondo le linee guida generali precedentemente illustrate ai punti 4 e 5 e nella procedura gestione password (psw_01). Tale codice d'accesso dev'essere impostato al massimo del numero di

/

caratteri consentito dal sistema operativo dello strumento e l'eventuale password utilizzata non deve facilmente richiamare né date di nascita né altri riferimenti anagrafici. Si consiglia l'uso di password alfanumeriche composte anche di lettere maiuscole e simboli, sempre se ammessi dal sistema operativo del mobile in dotazione. La password prescelta dovrà essere comunicata alla funzione preposta dell'Area IT, sia al primo uso che ogni volta che si deciderà di mutarla.

- Ove possibile, l'utente dovrà attivare le funzionalità di remote wiping, per cancellare i dati una volta che il dispositivo mobile non dovesse più essere nella disponibilità del dipendente (ad es.: casi di furto e/o smarrimento).

L'uso promiscuo dei dispositivi mobili è consentito SOLO previa autorizzazione della Direzione Risorse Umane inoltre.

Se il dispositivo mobile consente l'attivazione dei servizi di Tethering ovvero consentire la configurazione dell'apparato come gateway per offrire accesso alla Rete ad altri dispositivi che ne sono sprovvisti, questo tipo di possibilità va usata solo per periodi limitati ed in assenza di ogni altra soluzione di connettività (UMTS, Wi-Fi, Rete Ethernet, etc.). Il servizio va immediatamente disattivato al termine dell'utilizzo e va protetto da password almeno alfanumeriche secondo quanto indicato nella procedura gestione password (psw_01).

Il Bluetooth ed ogni altro protocollo che consenta l'associazione di dispositivi diversi dallo strumento mobile, dev'essere abilitato per l'accoppiamento ai soli strumenti aziendali in dotazione. Inoltre, può essere usato, in particolare, per l'attivazione dell'auricolare personale e/o del kit viva-voce dell'auto. Il Bluetooth non va mai lasciato inutilmente attivo e le password d'associazione non devono mai essere quelle di default previste per il dispositivo.

È fatto espresso divieto d'utilizzare un qualsiasi dispositivo mobile aziendale durante la guida. L'uso in auto è consentito solo mediante kit "viva voce" e/o con auricolare.

L'eventuale periferica Wi-Fi va abilitata sul dispositivo mobile solo ed esclusivamente ai fini d'accesso alla rete aziendale e/o di altre reti protette. Non va mai lasciato inutilmente attivo.

Del dispositivo mobile deve essere fatto regolarmente un backup o attraverso specifiche istruzioni da parte della funzione preposta dell'Area IT.

In caso di guasti o malfunzionamenti, l'utilizzatore dovrà rivolgersi alla funzione preposta dell'Area IT a cui è demandata la relativa gestione in queste circostanze.

Il Responsabile dell'Area IT può disporre dei dispositivi mobile secondo necessità, sostituendo, aggiornando, rimuovendo o adeguando in tutto o in parte le componenti hardware e/o software di cui essi si compongono, senza necessità di preavviso e di richiesta di consenso da parte dell'utilizzatore.

Quanto memorizzato sui supporti interni al dispositivo mobile potrebbe essere oggetto di analisi, controllo e duplicazione da parte del Responsabile dell'Area IT o da personale tecnico autorizzato, per migliorare l'affidabilità, la disponibilità e l'efficienza del dispositivo.

Qualora fossero individuate componenti hardware e/o software (programmi, documenti, dispositivi esterni, etc.) non corrispondenti ai criteri di sicurezza e di operatività individuati dalla funzione preposta dell'Area IT o non esplicitamente autorizzati, tali componenti potrebbero essere rimossi e l'utilizzatore potrebbe essere coinvolto negli accertamenti e nelle verifiche del caso che potrebbero portare a sanzioni disciplinari come previsto dal CCNL di riferimento.

16. Dispositivi personali

Può essere previsto che alcune persone possono utilizzare temporaneamente, o per alcuni periodi di tempo, dei dispositivi personali (pratica altrimenti detta BYOD=Bring Your Own Device). L'uso deve avvenire in modo libero e non obbligatorio. Il lavoratore è tenuto ad utilizzarlo come definito negli accordi di lavoro e il reparto IT sarà tenuto a definire delle specifiche per la rete di collegamento e le regole di utilizzo.

L'utilizzatore deve:

-nel caso venga autorizzato temporaneamente da un suo superiore a scattare foto o riprendere dei clienti (che hanno dato il consenso) durante l'esercizio del proprio ruolo per rendicontare la propria attività, una volta

/

svolto il proprio incarico e consegnata la registrazione come richiesto dal superiore, sarà tenuto a cancellare immediatamente ogni informazione o dato audio-video dal proprio dispositivo personale
- proteggere i dati come definito nel sistema (dotare il dispositivo di un Antivirus/firewall come stabilito da IT).
- conoscere le regole di protezione dei dati che dovrà applicare anche da casa
- in caso di perdita o furto del dispositivo personale dovrà avvisare immediatamente il reparto IT e/o il responsabile della privacy.
- in caso di interruzione del rapporto di lavoro dovrà restituire tutti i dati e garantirne l'eliminazione definitiva dai propri dispositivi. Il reparto IT potrebbe richiedere di visionare con la persona l'assenza di tali dati.
- Rispettare le regole riportate dal reparto IT e/o definite dall'organizzazione.

L'utilizzatore NON è autorizzato a:
- stampare documenti aziendali (se non può garantire la distruzione del documento dopo l'uso)
- salvare in locale nel proprio dispositivo personale ALCUN riferimento a dati o attività affidategli con particolare attenzione se riferite a dati di persone fisiche
- far utilizzare/trattare i dati aziendali, presenti sul proprio dispositivo, a persone diverse non autorizzate
- far visionare i dati a persone non autorizzate

17. Utilizzo dei supporti cartacei con dati degli interessati

Ogni autorizzato al trattamento deve seguire le seguenti regole per il trattamento dei dati su supporto cartaceo:
- Non deve lasciarli incustoditi
- Deve verificare che siano protetti in caso di temporanea assenza di controllo (ad esempio in auto non lasciarli in vista e custodirli in bagagliaio)
- Se contengono dati sensibili devono essere riporti in armadi o stanze chiuse a chiave in caso di assenza del controllo).
- Ogni documento cartaceo contenente dati personali deve essere protetto (anche con cartelline e/o buste) riposti in appositi armadi e non devono essere lasciati incustoditi.
- **Al termine del loro utilizzo devono essere distrutti con apposito "trituratore"**
- Non devono essere comunicati dati a terzi se non rientrano nelle finalità dell'informativa.
- Nel caso venissero "scannerizzati", devono essere riposti in cartelle soggette a back-up e protette (vedi sezioni precedenti)

18. Utilizzo dei social

Per ogni dato che gli addetti al trattamento inseriscono e/o" postano" sui social deve essere stato autorizzato dall'interessato.

19. Utilizzo di dati giudiziari e/o dati biometrici e/o ultrasensibili

Atti giudiziari (o ogni informazione giudiziaria che non riporti solo la totale mancanza di atti riferiti agli interessati, tra cui quelle inerenti all' antipedofilia o simili) sono da ritirare in cartaceo e riporre in archivi con accessi limitati e consegnare solo al responsabile privacy. Se devono essere trattati/archiviati su supporto informatico devono essere posizionati in una cartella CRIPTATA o con accesso limitato.

20. Utilizzo occasionale di dati non necessari o non definiti esplicitamente nelle finalità

Se dovesse rendersi necessario l'uso occasionale di dati personali per esigenze non espressamente previste nelle finalità delle informative aziendali, l'addetto al trattamento deve comunicarlo al responsabile della privacy e devono provvedere ad emettere una specifica informativa che sarà relativa allo specifico caso, valutando la necessità di specifici consensi.

21. Estrazione temporanea di dati dai Data_base indicati nel registro dei trattamenti

Se dovesse rendersi necessario l'estrazione occasionale di dati per analizzarli e/o trattarli temporaneamente su file di supporto (come su applicative Office o simili), l'incaricato deve utilizzarli solo su "dispositivi" autorizzati e protetti.
In ogni caso tali esigenze devono rimanere occasionali e quindi i dati vanno eliminati appena possibile.

/

Se i dati estrapolati servissero per la gestione degli incarichi ricevuti, allora dovrebbero essere posizionati in cartelle protette e soggette a back-up.

22. Utilizzo di immagini

Ogni immagine che contiene persone fisiche potrà essere utilizzata solo se tutti gli interessati rappresentati hanno espresso il loro consenso per la finalità dell'uso.

Se si devono utilizzare delle immagini per specifici scopi non indicati espressamente nelle precedenti informative, si deve emettere una specifica informativa con il consenso per lo specifico trattamento.

Si deve ricordare che l'uso di immagini su alcuni documenti comportano la "diffusione" delle stesse.

L'uso di immagini raccolte durante eventi o manifestazioni pubbliche (per i quali è impossibile raccogliere il consenso all'uso) sono vietate se l'immagine può recare pregiudizio all'interessato. In ogni caso in tali eventi è preferibile esporre l'informativa che comunichi la finalità delle eventuali immagini raccolte. Prima della pubblicazione verificare che non ci siano persone perfettamente riconoscibili e di cui non si ha il consenso.

La regola generale, che deve essere sempre tenuta presente, è che il ritratto di una persona non può essere esposto, riprodotto o messo in commercio senza il consenso di questa

23. Trattamento e gestione di dati di cui si viene in possesso per esigenze degli interessati

Durante l'erogazione dei servizi, si potrebbero trattare delle informazioni/dati di persone che non sono richiesti dalla nostra organizzazione, ma di cui l'interessato ci ha messo a conoscenza. Questi dati devono essere trattati nella stessa modalità definita per i punti precedenti nel rispetto dei principi di correttezza, liceità, trasparenza e riservatezza:

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 autorizzato al trattamento dei dati ai sensi del Regolamento UE 2016/679 (GDPR).

Poiché in caso di violazioni contrattuali e giuridiche, sia la Azienda, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'Azienda verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico.

Si ritiene necessario informare che:

- Come già anticipato nei precedenti capitoli la Direzione potrà effettuare un monitoraggio periodico dell'hardware e del software installato nei dispositivi informatici e mobili aziendali. Tale operazione viene effettuata, in modo completamente automatico per i dispositivi ed i sistemi operativi che lo consentono ed in modo manuale per tutti gli altri. Il monitoraggio, necessario per finalità organizzative (inventario del parco macchine e contabilità delle licenze d'uso del software), non coinvolge in alcun modo i dati personali ed i documenti presenti sui dispositivi, ma permette la rilevazione di software installato in violazione di questo Regolamento.
- La nostra organizzazione può incaricare dei responsabili che possono accedere ai dati trattati dall'utente tramite posta elettronica o navigazione in rete esclusivamente per motivi di sicurezza e protezione del sistema informatico (ad es., contrasto virus, malware, intrusioni telematiche, fenomeni quali *spamming*, *phishing*, *spyware*, etc.), ovvero per motivi tecnici e/o manutentivi e/o di regolare svolgimento dell'attività lavorativa (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione *hardware*). Fatta eccezione per gli interventi urgenti che si rendano necessari per affrontare situazioni di emergenza e massima sicurezza, il personale incaricato accederà ai dati su richiesta dell'utente e/o previo avviso al medesimo.
- Ove sia necessario per garantire la sicurezza, l'assistenza tecnica e la normale attività operativa, il personale incaricato avrà anche la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni. Lo stesso Responsabile IT e/o i suoi incaricati possono, nei casi su indicati, procedere a tutte le operazioni di configurazione e gestione necessarie a garantire la corretta funzionalità del sistema informatico aziendale (ad es. rimozione di file o applicazioni pericolosi).
- Come già anticipato nel capitolo 14, in previsione della possibilità che, in caso di assenza improvvisa o

prolungata e per improrogabili necessità legate all'attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica delle caselle elencate nel registro "REG_UT -Registro Utenti e assegnazione" l'utente può formalmente delegare un altro lavoratore (Fiduciario, così come definito dal Provvedimento del Garante della Privacy Nr. 13 del 1 marzo 2007 "Lavoro: le linee guida del Garante per posta elettronica e internet") a verificare il contenuto dei messaggi, a gestire le strette necessità operative e/o ad inoltrare quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. In assenza della nomina di un fiduciario, da effettuarsi entro tempi adeguati a l'espletamento della richiesta avanzata da parte del Responsabile d'ufficio, con la presenza di quest'ultimo e di personale appositamente incaricato (ad esempio gli amministratori dei sistemi come il Responsabile IT o i tecnici incaricati), il Titolare o persona da lui delegata, può legittimamente verificare il contenuto dei messaggi al fine da estrarre le informazioni ritenute rilevanti per lo svolgimento dell'attività lavorativa. Di tale attività informato il lavoratore interessato alla prima occasione utile precisando di cambiare la password di accesso della casella.

- Al fine di prevenire, per quanto e ove possibile, comportamenti scorretti durante la navigazione in Internet, l'azienda si potrà avvalere di appositi filtri che impediscono l'accesso a siti non ritenuti idonei ed il download di files multimediali non attinenti all'attività lavorativa. Tali sistemi consentono anche la raccolta e la conservazione dell'attività di navigazione dei singoli utenti in appositi registri chiamati "file di log".
- L'eventuale controllo sui *file* di *log* da parte dei responsabili incaricati (ad. Esempio l'amministratore di sistema o Resp. IT) non è comunque continuativo ed è limitato ad alcune informazioni (es. Posta elettronica: l'indirizzo del mittente e del destinatario, la data e l'ora dell'invio e della ricezione e l'oggetto – Navigazione internet: il nome dell'utente, l'identificativo della postazione di lavoro, indirizzo IP, la data e ora di navigazione, il sito visitato e il totale degli accessi effettuati) ed i file stessi vengono conservati per il periodo strettamente necessario per il perseguimento delle finalità di sicurezza della azienda, e comunque non oltre 12 mesi, fatti salvi in ogni caso specifici obblighi di legge. Il sistema di registrazione dei *log* è configurato per cancellare periodicamente ed automaticamente (attraverso procedure di sovra registrazione) i dati personali degli utenti relativi agli accessi internet e al traffico telematico. Eventuali comportamenti anomali saranno segnalati genericamente alle aree interessate (uffici, servizi) e, solo qualora tali comportamenti dovessero continuare, la Direzione potrà procedere, nel rispetto delle norme legali e contrattuali, a controlli individuali, come previsto al punto presente del presente Disciplinare.
- I responsabili incaricati sono altresì abilitati ad accedere ai dati contenuti negli strumenti informatici restituiti dall'utente all'Azienda per cessazione del rapporto, sostituzione delle apparecchiature, etc.

Il trattamento dei dati, così come descritto, è obbligatorio, pena l'impossibilità di utilizzare qualunque dispositivo informatico, digitale e/o mobile.

La nostra organizzazione garantisce la non effettuazione di alcun trattamento mediante sistemi hardware e software specificatamente preordinati al controllo a distanza.

Nell'ambito delle misure di controllo del livello di sicurezza del sistema informativo, è possibile che il Titolare del trattamento o persona da lui delegata, effettui tentativi di violazione delle password degli utenti. Nel caso il tentativo abbia esito positivo, verrà chiesto all'utente di sostituire immediatamente la password.

25. Regole per la protezione dei locali e degli accessi

Al fine di garantire l'integrità e la disponibilità dei dati e la protezione delle aree e dei locali, si definiscono le seguenti misure di sicurezza:

- L'autorizzato che è in possesso delle chiavi della Azienda e/o codici antifurto ha l'obbligo di conservare le chiavi in modo che non siano accessibili ad altri e non deve comunicare a terzi i codici di ingresso se non espressamente autorizzato dal responsabile (si ricorda che alla fine del rapporto di lavoro tali chiavi aziendali dovranno essere sempre restituite al responsabile).
- In caso una chiave venga smarrita o sottratta ha l'obbligo di segnalarlo al responsabile che provvederà alla sostituzione delle serrature relative ed alla sostituzione delle altre chiavi già distribuite.
- Al termine dell'utilizzo dei locali e/o della Sede della quale possiede le chiavi questi dovranno essere lasciati chiusi e le chiavi rimosse dalla serratura e custodite o in luogo protetto e/o personalmente.
- In caso trovasse aperto un locale o un dispositivo che avrebbe dovuto essere chiuso è pregato di segnalarlo al responsabile.
- Deve identificare ciascuna persona richiedente l'ingresso, per qualsiasi motivo, ai locali della Azienda.

/

- Al Visitatore è fatto divieto di trattamento, anche accidentale, di qualsiasi dato personale sia affidato alla Azienda per l'adempimento ai propri obblighi e/o ai propri fini, fatti salvi specifici contratti di servizio e/o di mandato.

Nel caso di banca dati cartacea, gli schedari (o altro contenitore) di dati personali devono essere protetti da lucchetti, serrature o misure di protezione equivalenti e specificatamente autorizzato l'accesso al trattamento.
Nel caso di banca dati in formato elettronico i dati sono protetti tramite la predisposizione di un apposito sistema di credenziali di accesso.
La documentazione dell'Area Commerciale, comprendente proposte commerciali e preventivi, conferme d'ordine, copia dei contratti di fornitura conclusi con i clienti, corrispondenza dei clienti è trattata e conservata presso l'ufficio amministrativo-commerciale.
Allo stesso modo la documentazione dell'area Amministrativa (ad es.: fatture, estratto conto, cassa, scontrini rimborsi spese, documenti societari, ricevute, documenti per il controllo fiscale libro fiscale, verbale, documentazione relativa al Personale, ecc.) è trattata e conservata sempre presso l'ufficio Amministrativo.
Tutti i dati sensibili (ad esempio i certificati medici dei dipendenti) sono custoditi in armadi protetti da serratura.
Tutti i dati sensibili non devono essere lasciati incustoditi. I file con dati sensibili devono essere riposti in cartelle informatiche visibili solo agli incaricati con specifici profili di autorizzazione.
Dopo la cessazione degli incarichi ricevuti dal Cliente o dei rapporti contrattuali con Fornitori, Dipendenti e/o altri soggetti, si procede alla conservazione dei soli Dati pertinenti e strettamente necessari alle finalità di:

a. gestione amministrativo-contabile del contratto, dell'ordine e/o della commessa/progetto;
b. adempimento ad obblighi di legge, regolamenti, normativa comunitaria (ad es. in materia fiscale, contabile, di pubblica sicurezza, antiriciclaggio);
c. attività commerciale e/o di marketing promozionale nei limiti consentiti ed eventualmente specificatamente autorizzati;
d. gestione reclami e difesa di propri diritti in sede giudiziale.

Gli altri Dati, non pertinenti né strettamente necessari alle suddette finalità, vengono cancellati o resi anonimi.
Durante la consultazione degli archivi il personale autorizzato sovrintende che nessun soggetto terzo, non autorizzato, acceda ai locali, anche temporaneamente, o richieda di prendere visione o estrarre copia della documentazione ivi archiviata.
Deroghe in tal senso possono essere autorizzate solo per iscritto da parte del Titolare del Trattamento e/o al Referente interno Privacy.

26. Sistemi di controllo graduali

In caso di anomalie che coinvolgessero i dati personali, il personale incaricato del servizio ICT effettuerà controlli preliminari su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree che si concluderanno con avvisi generalizzati diretti ai dipendenti di detta struttura o aree in cui sia 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 individuale potranno essere compiuti solo in caso di successive ulteriori anomalie (come previsto dal p. 6.1 della Delibera Nr. 13 del 1/3/2007 Garante Privacy *"Lavoro: le linee guida del Garante per posta elettronica e internet"*).
In alcun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

27. Divieti e regole comportamentali fondamentali

Gli autorizzati **NON POSSONO**:

- Utilizzare i computer e sistemi informatici e di comunicazione aziendali per accedere a siti personali o servizi e-mail personali o altri sistemi non autorizzati;
- scaricare/installare software se non autorizzati;
- utilizzare supporti di archiviazione esterni se non autorizzati;
- collegare alla rete aziendale "dispositivi" personali senza specifica autorizzazione;
- utilizzare immagini aziendali e/o recuperate negli ambienti di lavoro, per scopi non autorizzati o definiti dal sistema di gestione della privacy dell'Azienda;
- comunicare a persone diverse dall'interessato informazioni se non autorizzate dall'interessato stesso, in caso di necessità si deve rispondere al richiedente "*di rilasciare un recapito per ricontattarlo dopo che*

abbiamo verificato l'informazione che chiede". Si verifica la legittimità della richiesta e l'autorizzazione del richiedente e solo dopo tali accertamenti si procede con le comunicazioni richieste (eventualmente esplicitare la necessità di una richiesta formale dei dati da comunicare);
- postare su social dati di cui non si ha specifica autorizzazione;
- lasciare dati e/o supporti contenente dati nei mezzi di trasporto, se si rendesse necessario lasciare dei documenti o altri supporti con dati nei mezzi di trasporto (solo temporaneamente), non devono essere lasciati in vista, ma riposti nel bagagliaio.

Gli autorizzati **DEVONO**:

- In caso di necessità di trattamento di dati non previsti nella informativa, si deve definire una informativa specifica ed un consenso specifico (ad esempio: uso di immagini e/o dati non necessari per gli incarichi ricevuti).
- Rispettare sempre i principi di riservatezza, correttezza, trasparenza, liceità ed in caso di dubbio chiedono al responsabile della privacy.
- Segnalare immediatamente ogni anomalia e/o sospetto di errato trattamento e/o violazione dei dati al referente privacy.
- Verificare costantemente che i dati che si stanno trattando non siano "disponibili" a terzi non autorizzati.
- Concedere l'accesso da remoto/esterno alla nostra rete solo se sono a conoscenza delle "REGOLE PER PERMETTERE COLLEGAMENTI DA REMOTO/ESTERNO ALLA NOSTRA RETE" e ne hanno verificato il rispetto.
- Leggere file tutti i file/documenti di PRESTA ATTENZIONE predisposti dalla Azienda (solo se presenti).

28. Identificazione ed incarico ai Responsabili del trattamento (art.28 del GDPR)

Tutti gli autorizzati sono informati del fatto che i dati di persone fisiche, possono essere trattati esclusivamente da soggetti autorizzati con adeguati profili (Inc-21) o da Responsabili del trattamento specificatamente incaricati al rispetto dei requisiti di cui all'art. 28 del GDPR (Inc-Gen_01).
Per questo la nostra organizzazione ha definito regole precise per identificare e qualificare i potenziali Responsabili, a cui gli autorizzati possono affidare il trattamento dei dati solo dopo l'iter di qualifica.
Sono Responsabili del trattamento tutte le strutture e/o persone a cui vengono affidati dei trattamenti al di fuori dei sistemi di gestione della nostra organizzazione e/o con strumenti informatici/supporti non controllati dalla nostra organizzazione (nel caso in cui il trattamento da parte del soggetto avvenisse esclusivamente all'interno del sistema della nostra organizzazione allora verrebbe autorizzato al trattamento, ma non identificato come Responsabile). Si riporta un elenco, non esaustivo dei possibili responsabili: medico competente, consulente del lavoro, RSPP, etc). In sostanza sono soggetti ai quali affidiamo dati di persone per adempiere ad un trattamento per una nostra finalità (per dettagli si rimanda alla definizione di cui all'art. 28 del GDPR).
Chi dovesse avere l'esigenza di coinvolgere tali soggetti, deve prima comunicarlo al Referente identificato per la gestione del registro dei Responsabili. Tale referente effettua una verifica del possesso dei requisiti riportati nel documento "incarico responsabile esterno" e definisce le integrazioni contrattuali da inserire nei contratti in essere, o proposti, per il soggetto da incaricare.
Solo dopo aver ottenuto adeguate garanzie da parte del "candidato" responsabile, si procede con l'aggiornamento del registro e alla comunicazione dei dati per il trattamento richiesto a seguito della sottoscrizione del contratto e delle specifiche in riferimento alla responsabilità nel trattamento dei dati.
Al termine del trattamento si richiede al Responsabile di rispettare quanto indicato nella suddetta lettera di incarico in riferimento alle regole di restituzione e/o eliminazione dei dati.

29. Dati di Interessati comunicati alla nostra Azienda da altri titolari.

Quando altri clienti e/o imprese/enti ci comunicano dati di persone fisiche (per qualsiasi motivo), la nostra organizzazione è comunque responsabile del corretto trattamento, mentre è titolare dei dati chi li comunica alla nostra organizzazione.
In questi casi l'autorizzato deve richiedere al titolare una dichiarazione che ha verificato e ottenuto le autorizzazioni dagli interessati per la comunicazione/diffusione del dato.
Al Titolare si inviano le specifiche previste per il trattamento e si richiede di informare la nostra organizzazione

di eventuali restrizioni e/o limitazioni rispetto a quanto riportato nelle nostre comunicazioni.

30. Comunicazioni anomalie

In caso di anomalie, il personale autorizzato deve **attivarsi nel più breve tempo possibile** e comunicare al referente della privacy l'anomalia rilevata.

Tale anomalia sarà gestita come una non conformità e il referente si attiva per definire il trattamento da attivare, analizza se l'anomalia ha comportato la perdita di dati, o situazioni di "data-breach" attivando quanto indicato nella istruzione "gestione data-breach e analizza l'esigenza di azioni correttive per eliminare le fonti dell'anomalie ed evitare che le stesse si possano ripetere.

Le modifiche al sistema saranno comunicate agli incaricati. Le anomalie saranno utilizzate come elementi formativi e di confronto con gli autorizzati coinvolti e non per condividere le casistiche e le soluzioni.

31. Modifiche ai consensi e recettività del regolamento

Ogni interessato può ritirare e/o variare il proprio consenso al trattamento dei dati.

Le comunicazioni relative alle procedure del presente Sistema di Gestione Privacy vengono inviate tramite i canali aziendali si intendono conosciute e accettate dal ricevente

32. Non osservanza del presente regolamento

L'inosservanza, da parte del lavoratore, delle disposizioni contenute nel presente regolamento potrà dar luogo in relazione alla gravità dell'infrazione commessa, all'applicazione di una sanzione proporzionale alla violazione commessa e all'applicazione dei provvedimenti disciplinari previsti dal CCNL adottato in Azienda, al quale si rinvia in ogni caso anche per le ipotesi non contemplate nel presente Regolamento,

Si specifica inoltre che il mancato rispetto o la violazione del regolamento potrà essere perseguibile anche con le azioni civili e penali consentite dalla legge vigente.

In ogni caso nelle situazioni di anomalia/violazione trattamento del dato di qualsiasi tipo deve essere attivata. La gestione dell'anomalia entro 24 ore utilizzando il modulo gestione anomalia (come descritto nella procedura di sistema) informando il Referente.

33. Aggiornamento e revisione

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dalla Direzione.

Il presente Regolamento, essendo un documento recettizio, viene inviato via e-mail ai dipendenti ed è soggetto a revisione con frequenza annuale.

34. Allegati

ALL01-SGSI-REG01 Vademecum per la Classificazione, Gestione e Protezione delle Informazioni commerciali e sensibili Rev0
ALL02-SGSI-REG01 Vademecum per la Gestione e Raccolta dei Consensi Privacy Rev0
ALL03-SGSI-REG01 Vademecum per la Gestione Violazioni di Informazioni Commerciali Riservate (Piano di Risposta agli Incidenti - IRP)
ALL04-SGSI-REG01 Vademecum Flusso Dati Commessa
All04-SGSI-REG01 Vademecum Flusso Dati Commessa
All05-SGSI-REG01 Vademecum Flusso Dati Commessa
All06a/b/c-SGSI-REG01 Vademecum Flusso Dati Commessa Prodotti Eyeware Rev0
All06d SGSI-REG01 Vademecum Flusso Dati Commessa Cartotecnica Rev0
All07 SGSI-REG01 Vademecum per la Sicurezza delle Informazioni — Terze Parti (Due Diligence)

Crocetta del Montello, 30 Gennaio 2026

Grafiche Antiga s.p.a.
L'amministratore Delegato
Antiga Silvio

/