Unione Montana dei Comuni del Monviso

Approvato con deliberazione del Consiglio dell'Unione n. 36 del 28/11/2019

Politiche aziendali per il trattamento dei dati e della strumentazione informatica

(Riferimenti: Reg. Europeo 679/2016, Provv. Garante 81 del 1 marzo 2008)

La nostra azienda ha analizzato la Deliberazione del Garante per la Protezione dei dati personali n. 13 del 1 marzo 2007 (pubblicata sulla Gu n.58 del 10 marzo 2007) avente come oggetto "**Posta elettronica e Internet: linee guida del Garante per posta elettronica e internet"** alla luce della nuova normativa europea sulla tutela e protezione del dati personali (Reg. Europeo 679/2016) pienamente attuativa dal 25 maggio 2018.

Abbiamo analizzato le seguenti considerazioni formulate in tale provvedimento dal Garante per la protezione dei dati personali:

- compete ai datori di lavoro assicurare la funzionalità e il corretto impiego di internet e posta elettronica da parte dei lavoratori, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa, tenendo conto della disciplina in tema di diritti e relazioni sindacali;
- spetta ad essi adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e di dati, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità;
- emerge l'esigenza di tutelare i lavoratori interessati anche perché l'utilizzazione dei predetti mezzi, già ampiamente diffusi nel contesto lavorativo, è destinata ad un rapido incremento in numerose attività svolte anche fuori della sede lavorativa;
- l'utilizzo di Internet da parte dei lavoratori può infatti formare oggetto di analisi, profilazione e integrale ricostruzione mediante elaborazione di *log file* della navigazione *web* ottenuti, ad esempio, da un *proxy server* o da un altro strumento di registrazione delle informazioni. I servizi di posta elettronica sono parametri suscettibili (anche attraverso la tenuta di *log file* di traffico *e-mail* e l'archiviazione di messaggi) di controlli che potrebbero giungere, se non correttamente inquadrati e gestiti, fino alla conoscenza del contenuto della corrispondenza;
- le informazioni così trattate contengono dati personali anche sensibili riguardanti lavoratori o terzi, identificati o identificabili.

Campo di applicazione

- Il Disciplinare 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.
- Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente e collaboratore in possesso di specifiche credenziali di

autenticazione sulla struttura informatica aziendale o suoi componenti. Tale figura potrà anche venir indicata quale “soggetto autorizzato al trattamento”.

Tutela del lavoratore

Il luogo di lavoro è una formazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati garantendo che, in una cornice di reciproci diritti e doveri, sia assicurata l'esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali (*artt. 2 e 41, secondo comma, Cost.; art. 2087 cod. civ.);*
Nell'organizzazione dell'attività lavorativa e degli strumenti utilizzati, l’azienda ha prefigurato una modalità d'uso che, tenendo conto del crescente lavoro in rete e di nuove tariffe di traffico forfettarie, assegna aree di lavoro riservate per appunti strettamente personali, ovvero consente usi moderati di strumenti per finalità private.
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 Europeo 679/2016 “dati personali” quando sono riferite a persone fisiche e, per la loro gestione (Trattamento), sia cartacea che digitale, è necessario che l’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.
Inoltre, nell’ambito della sua attività, l’azienda tratta “dati cartacei” ovvero informazioni su supporto cartaceo e “dati digitali” ovvero informazioni che vengono memorizzate o semplicemente transitano attraverso apparecchiature digitali.
In linea generale, ogni dato, nell’accezione più ampia sopra descritta, di cui il soggetto autorizzato al trattamento viene a conoscenza, nell’ambito della propria attività lavorativa, è da considerarsi riservato e non deve essere comunicato o diffuso a nessuno (anche una volta interrotto il rapporto lavorativo con l’organizzazione stessa o qualora parte delle informazioni siano di pubblico dominio) salvo specifica autorizzazione esplicita dell’azienda.

Anche tra colleghi, oppure tra dipendenti e collaboratori esterni, è necessario adottare la più ampia riservatezza nella comunicazione dei dati conosciuti, limitandosi solo a quei casi che si rendono necessari per espletare al meglio l'attività lavorativa richiesta.

La progressiva diffusione delle nuove tecnologie informatiche ed in particolare l'accesso alla rete internet dal computer aziendale espone l'azienda a possibili rischi di un coinvolgimento di rilevanza sia civile, sia penale, sia amministrativa, creando problemi alla sicurezza e all'immagine dell'organizzazione stessa.

Premesso che i comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, tra i quali rientrano l'utilizzo delle risorse informatiche e telematiche, devono sempre ispirarsi al principio di diligenza e correttezza, l'azienda ha adottato il presente Disciplinare Interno diretto ad evitare che condotte inconsapevoli possano innescare problemi o minacce alla sicurezza dei dati o delle attrezzature aziendali.

Il presente Disciplinare Interno si applica ai soggetti autorizzati al trattamento che si trovino ad operare con dati dell'azienda, una gestione dei dati cartacei, un uso dei COMPUTER e di altri dispositivi elettronici (di seguito DEVICE) 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.

Esclusione dall'uso degli strumenti informatici

All'inizio del rapporto lavorativo o di consulenza, l'azienda valuta la presenza dei presupposti per l'autorizzazione all'uso dei vari device aziendali, di internet e della posta elettronica da parte dei soggetti autorizzati al trattamento.

Successivamente e periodicamente l'azienda valuta la permanenza dei presupposti per l'utilizzo dei device aziendali, di internet e della posta elettronica.

E' fatto esplicito divieto ai soggetti non autorizzati di accedere agli strumenti informatici aziendali.

I casi di esclusione possono riguardare:

- L'utilizzo del COMPUTER o di altri DEVICE;
- l'utilizzo della posta elettronica;
- l'accesso a internet.

Le eventuali esclusioni sono strettamente connesse al principio della natura aziendale e lavorativa degli strumenti informatici nonché al principio di necessità di cui al Codice Privacy. Più specificatamente hanno diritto all'utilizzo degli strumenti e ai relativi accessi solo i soggetti autorizzati al trattamento che, per funzioni lavorative, ne abbiano un effettivo e concreto bisogno.

I casi in cui le esclusioni dovranno risultare operative in forza di tali motivazioni verranno comunicati individualmente e potranno riguardare sia tutti i casi sopra descritti, sia solo uno o due degli stessi.
Si informa che tali esclusioni sono divenute necessarie alla luce del Provvedimento del Garante 1° marzo 2007 che indica di ridurre a titolo cautelativo e preventivo l'utilizzo degli strumenti informatici in considerazione dei pericoli e delle minacce indicate in questo documento.

Titolarità degli strumenti e dei dati e finalità

L'azienda è l'unica esclusiva titolare e proprietaria di tutte le informazioni, le registrazioni ed i dati contenuti e/o trattati mediante i propri device digitali o archiviati in modo cartaceo nei propri locali.
Il soggetto autorizzato al trattamento non può presumere o ritenere che le informazioni, le registrazioni ed i dati da lui trattati o memorizzati nei device aziendali (inclusi i messaggi di posta elettronica e/o chat inviati o ricevuti, i file di immagini, i files di filmati o altre tipologie di files) siano privati o personali, né può presumere che dati cartacei in suo possesso possano essere da lui copiati, comunicati o diffusi senza l'autorizzazione dell'organizzazione.
I device assegnati sono uno strumento lavorativo nelle disponibilità del soggetto autorizzato al trattamento esclusivamente per un fine di carattere lavorativo. I device, quindi, non devono essere utilizzati per finalità private e diverse da quelle aziendali, se non eccezionalmente e nei limiti evidenziati dal presente Disciplinare. Qualsiasi eventuale tolleranza da parte di questa azienda, apparente o effettiva, non potrà, comunque, legittimare comportamenti contrari alle istruzioni contenute nel presente Disciplinare
Restituzione degli strumenti e dei dati cartacei
A seguito di una cessazione del rapporto lavorativo o di consulenza del soggetto autorizzato al trattamento con l'organizzazione o, comunque, al venir meno, ad insindacabile giudizio dell'azienda, della permanenza dei presupposti per l'utilizzo dei device aziendali, i soggetti autorizzati al trattamento hanno i seguenti obblighi:

- Procedere immediatamente alla restituzione dei device in uso;
- Divieto assoluto di formattare o alterare o manomettere o distruggere i device assegnati o rendere inintelligibili i dati in essi contenuti tramite qualsiasi processo.

Normativa in materia di protezione dei dati e discipline di settore

La disciplina di protezione dei dati va coordinata con regole di settore riguardanti il rapporto di lavoro e il connesso utilizzo di tecnologie. In questo modo I trattamenti rispettano le garanzie in materia di protezione dei dati e si svolgono nell'osservanza di cogenti principi:

- il principio di *privacy by default o di minimizzazione* , secondo cui qualsiasi iniziativa che comporta un trattamento di dati personali deve essere condotta riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (*art. 25 del GDPR*);
- i principi di "liceità, correttezza e trasparenza nei confronti dell'interessato" (*art. 5, comma 1, lett. A) del GDPR*). Le tecnologie dell'informazione (in modo più marcato rispetto ad apparecchiature tradizionali) permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa. Ciò non deve avvenire all'insaputa o senza la piena consapevolezza dei lavoratori;
- i trattamenti devono essere effettuati per finalità *determinate*, *esplicite* e *legittime* (*art. 5, comma 1 lettera b), del GDPR*), osservando il principio di *pertinenza* e *non eccedenza*. Il datore di lavoro deve trattare i dati *"nella misura meno invasiva possibile"*; le attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere *"mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza"* (Parere del Garante n. 8/2001*, cit., punti 5 e 12*).

La nostra azienda procedendo dalle soprastanti considerazioni decide di adottare e di divulgare le seguenti linee guida inerenti l'utilizzo della strumentazione informatica, e dell'uso della posta elettronica e di internet. Le linee guida procedono affrontando e sviluppando i seguenti temi:

PASSWORD

Le password possono essere un metodo di autenticazione assegnato dall'organizzazione per garantire l'accesso protetto ad uno strumento hardware oppure ad un applicativo software.

La prima caratteristica di una password è la segretezza, e cioè il fatto che non venga svelata ad altri soggetti. La divulgazione delle proprie password o la trascuratezza nella loro conservazione può causare gravi danni al proprio lavoro, a quello dei colleghi e dell'azienda nel suo complesso. Nel tempo anche la password più sicura perde la sua segretezza. Per questo motivo è buona norma cambiarle con una certa frequenza.

L'azienda ha implementato alcuni meccanismi che permettono di aiutare e supportare gli Soggetti autorizzati al trattamento in una corretta gestione delle password, in particolare, per quanto riguarda le password di accesso al Dominio (ove previsto), è in funzione un sistema automatico di richiesta di aggiornamento delle stesse impostato dall'azienda secondo il livello di sicurezza richiesto dall'azienda stessa e, comunque, in linea con quanto richiesto dalla normativa privacy.

Altra buona norma è quella di non memorizzare la password su supporti facilmente intercettabili da altre persone. Il miglior luogo in cui conservare una password è la propria memoria.

Le password che non vengono utilizzate da parte dei soggetti autorizzati al trattamento per un periodo superiore ai sei mesi verranno disattivate dall'azienda.
In qualsiasi momento l'organizzazione si riserva il diritto di revocare al soggetto autorizzato al trattamento il permesso di accedere ad un sistema hardware o software a cui era precedentemente autorizzato, rimuovendo user id o modificando/cancellando la password ad esso associata.
Il soggetto autorizzato al trattamento, da parte sua, per una corretta e sicura gestione delle proprie password deve rispettare le regole seguenti:

- Le password sono assolutamente personali e non vanno mai comunicate ad altri;
- Occorre cambiare immediatamente una password non appena si abbia dubbio che sia diventata poco "sicura";
- Le password devono essere lunghe almeno 8 caratteri e devono contenere anche lettere maiuscole, caratteri speciali e numeri;
- Le password non devono essere memorizzate su alcun tipo di supporto, quali, ad esempio, Post-It (sul monitor o sotto la tastiera) o agende (cartacee, posta elettronica, telefono cellulare);
- Le password devono essere sostituite almeno nei tempi indicati dalla normativa, a prescindere dall'esistenza di un sistema automatico di richiesta di aggiornamento password (nello specifico ogni mese);
- Evitare di digitare la propria password in presenza di altri soggetti che possano vedere la tastiera, anche se collaboratori o dipendenti dell'azienda.

In alcuni casi, sono implementati meccanismi che consentono al soggetto autorizzato al trattamento fino ad un numero limitato di tentativi errati di inserimento della password oltre ai quali il tentativo di accesso viene considerato un attacco al sistema e l'account viene bloccato per alcuni minuti. In caso di necessità contattare il Titolare.

UTILIZZO DEL PERSONAL COMPUTER

L'utilizzo del personal computer comporta l'uso di archivi contenenti dati generici e/o sensibili di cui non è consentita la divulgazione e si deve prevenire l'eventualità di virus che attaccherebbero l'integrità di tali dati.
Il computer consegnato al soggetto autorizzato al trattamento è uno strumento di lavoro e contiene tutti i software necessari a svolgere le attività affidate. Ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, rallentamenti del sistema, costi di manutenzione e, soprattutto, minacce alla sicurezza. Per necessità aziendali, gli amministratori di sistema utilizzando la propria login con privilegi di amministratore e la password dell'amministratore, potranno accedere, con le regole indicate nel presente

documento, sia alla memoria di massa locali di rete (repository e backup) che ai server aziendali nonché, previa comunicazione al dipendente, accedere al computer, anche in remoto.

Per questi motivi la linea guida da seguire per l'utilizzo di tali strumentazioni è la seguente:

- è consentito installare programmi provenienti dall'esterno solo se espressamente autorizzati dall'azienda, per evitare il pericolo di virus informatici;
- non è consentito l'uso di programmi non distribuiti ufficialmente dall'azienda (v., in proposito, gli obblighi imposti dal d.lgs 29 dicembre 1992, n. 518, sulla tutela giuridica del software e dalla legge 18 agosto 2000, n. 248, contenente nuove norme di tutela del diritto d'autore);
- non è consentito utilizzare strumenti software e/o hardware atti a interpretare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;
- non è consentito modificare le configurazioni impostate sul proprio pc dagli "amministratori di sistema" preposti dall'azienda;
- non è consentita l'installazione sul proprio pc di mezzi di comunicazione propri (come per esempio i modem);
- sui pc dotati di scheda audio e/o di lettore cd è consentito l'ascolto di programmi, file audio o musicali, etc.. limitandone l'uso a fine prettamente lavorativi;
- non dare accesso al proprio computer ad altri utenti, a meno che siano soggetti autorizzati al trattamento con cui condividono l'utilizzo dello stesso Pc o a meno di necessità stringenti e sotto il proprio costante controllo;
- se si allontana dalla propria postazione dovrà mettere in protezione il suo device affinché persone non autorizzate non abbiano accesso ai dati protetti (l'azienda ha quindi impostato la protezione in automatico dopo 15 minuti di inutilizzo del device);
- bloccare il suo device prima delle pause e, in generale, ogni qualvolta abbia bisogno di allontanarsi dalla propria postazione;
- chiudere la sessione (Logout) a fine giornata;
- spegnere il PC dopo il Logout ;
- controllare sempre che non vi siano persone non autorizzate alle sue spalle che possano prendere visione delle schermate del suo device.

CONNESSIONE DEL PROPRIO PERSONAL COMPUTER ALLA RETE AZIENDALE

Per la connessione del proprio pc alla rete aziendale si necessita di rispettare le vigenti norme:

- 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;
- l'azienda si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema ovvero acquisiti o installati in violazione delle disposizioni contenute nel presente documento.
- I files creati, elaborati o modificati sul computer assegnato devono essere poi sempre salvati a fine giornata sul sistema di repository documentale centralizzato. L'azienda non effettua il backup dei dati memorizzati in locale.

UTILIZZO SUPPORTI MAGNETICI

Ai Soggetti autorizzati al trattamento può essere assegnata una memoria esterna (quale una chiave USB, un hard disk esterno, una memory card, …) su cui copiare temporaneamente dei dati per un facile trasporto, o altri usi (es. macchine fotografiche con memory card, videocamere con dvd, …).

Questi dispositivi devono essere gestiti con le stesse accortezze di cui all'articolo precedente e devono essere utilizzati esclusivamente dalle persone a cui sono state affidate e, in nessun caso, devono essere consegnate a terzi.

Le norme da rispettare in tal merito sono:

- tutti i file di provenienza incerta o esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti al controllo e relativa autorizzazione all'utilizzo da parte dell'azienda.

ANTIVIRUS

I virus possono essere trasmessi tramite scambio di file via internet, via mail, scambio di supporti removibili, filesharing, chat, via mail …

L'azienda impone su tutte le postazioni di lavoro l'utilizzo di un sistema antivirus correttamente installato, attivato continuamente e aggiornato automaticamente con frequenza almeno quotidiana.

Il soggetto autorizzato al trattamento, da parte sua, deve impegnarsi a controllare il corretto funzionamento e aggiornamento del sistema antivirus installato sul proprio computer, e, in particolare, deve rispettare le regole seguenti:

1. Comunicare all'azienda ogni anomalia o malfunzionamento del sistema antivirus;
2. Comunicare all'azienda eventuali segnalazioni di presenza di virus o file sospetti.

Inoltre, al soggetto autorizzato al trattamento:

- È vietato accedere alla rete aziendale senza servizio antivirus attivo e aggiornato sulla propria postazione;
- E' vietato ostacolare l'azione dell'antivirus aziendale;
- E' vietato disattivare l'antivirus senza l'autorizzazione espressa dall'azienda anche e soprattutto nel caso sia richiesto per l'installazione di software sul computer;
- E' vietato aprire allegati di mail provenienti da mittenti sconosciuti o di dubbia provenienza o allegati di mail di persone conosciute ma con testi inspiegabili o in qualche modo strani.

Contattare i sistemi informativi prima di procedere a qualsiasi attività potenzialmente in conflitto con quanto sopra.

POSTA ELETTRONICA

Il contenuto dei messaggi di posta elettronica, come pure i dati esteriori delle comunicazioni e i file allegati, riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente, la cui ratio risiede nel proteggere il nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali; un'ulteriore protezione deriva dalle norme penali a tutela dell'inviolabilità dei segreti (artt. 2 e 15 Cost.; Corte cost. 17 luglio 1998, n. 281 e 11 marzo 1993, n. 81; art. 616, quarto comma, c.p.; art. 49 Codice dell'amministrazione digitale).

Tuttavia, con specifico riferimento all'impiego della posta elettronica nel contesto lavorativo e in ragione della veste esteriore attribuita all'indirizzo di posta elettronica nei singoli casi, il lavoratore, in qualità di destinatario o mittente, deve utilizzare la posta elettronica operando esclusivamente quale espressione dell'organizzazione datoriale evitandone gli usi personali.

La presente policy fissa pertanto le regole da seguire nell'utilizzo della posta elettronica aziendale:

- Dato il carattere aziendale delle caselle postali Internet, gli utenti devono evitare di inoltrare messaggi non direttamente inerenti alle proprie competenze. Inoltre gli utenti devono prestare attenzione a quanto espresso nei contenuti soprattutto riguardo altre persone o organizzazioni: il messaggio potrebbe essere diffuso e/o inoltrato ad altri con facilità.
- 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;

- la posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei e, dunque, non deve essere usata per inviare documenti di lavoro «strettamente riservati» che possono essere recapitati con altre modalità più sicure;
- non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, forum o mail-list, salvo diversa ed esplicita autorizzazione scritta dell'azienda.
- Non è ammesso l'uso del sistema di posta per attività commerciali o a scopo di lucro, ed in genere per scopi non previsti dalle norme statutarie dell'azienda.
- Non si deve usare un linguaggio irrispettoso o comunque non apprezzato. Evitare di spedire messaggi provocatori. Evitare di rispondere a messaggi provocatori.
- Includere sempre la propria firma in fondo ai messaggi. La firma dovrebbe includere nome, funzione, organizzazione di appartenenza e l'indirizzo di posta elettronica, e opzionalmente l'indirizzo postale e un recapito telefonico. È buona norma includere, in calce alla firma, anche un disclaimer di riservatezza sul contenuto dei messaggi fornito dall'azienda.

  <<Avvertenze ai sensi Regolamento Europeo 679/2016. Le informazioni contenute in questo messaggio sono riservate, confidenziali ed a uso esclusivo del destinatario ed è vietata la loro diffusione. Qualora riceveste il presente messaggio per errore e non ne siate destinatari, Vi preghiamo di darcene notizia via e-mail, di astenervi dal consultare il messaggio stesso e gli eventuali files allegati e di cancellare il messaggio dal Vs. sistema informatico. Costituisce comportamento contrario ai principi del Regolamento Europeo 679/2016 trattenere il messaggio, diffonderne il contenuto, inviarlo ad altri soggetti, copiarlo in tutto od in parte, utilizzarlo da parte di soggetti diversi dal destinatario. L'Unione Monviso garantisce la massima riservatezza dei dati da Voi comunicati; gli stessi saranno trattati in ottemperanza alle normative vigenti. L'interessato può esercitare i propri diritti di soggetto interessato dandone comunicazione all'indirizzo e-mail privacy@unionemonviso.it. L'Unione Monviso non si assume alcuna responsabilità per eventuali intercettazioni, modifiche o danneggiamenti del presente messaggio e-mail.>>
- ci si assicuri della grandezza del messaggio inviato. Allegare ampi file come un documento o un programma potrebbe impedire l'arrivo del messaggio stesso o un eccessivo utilizzo di risorse. Buona regola è non inviare mai file superiori a qualche 1-2 Mb. In tal caso, considerare come alternativa "lo zip" (compressione) dei file o la riduzione a diversi file più piccoli da inviare come messaggi separati.
- il contenuto e la gestione di una mailbox è sotto la responsabilità dell'utente incaricato al presidio della stessa. In particolare questi dovrà di norma controllare la posta in arrivo almeno una volta al giorno e, se necessario, smistare correttamente e tempestivamente la posta in entrata.

- in generale, è una buona idea controllare tutti i "Subject" (Oggetto) dei messaggi ricevuti prima di aprire le e-mail e rispondere. In tal modo si può fare un preventivo controllo che il messaggio a cui si sta per rispondere sia diretto proprio a noi. Porre attenzione anche al fatto che il messaggio si può riceverlo per CC anziché come destinatario principale. In tal caso occorre valutare se è nostro compito rispondere o meno.
- fare attenzione quando s'inserisce l'indirizzo del ricevente. Ci sono indirizzi che individuano un gruppo di persone (lista di distribuzione) ma sembra appartengano ad una persona soltanto. In tal caso si valuti sempre se è necessario rispondere all'intero gruppo o solo a qualcuno dei suoi componenti.
- quando si invia un'e-mail a più indirizzi che tra di loro non devono venire a conoscenza l'uno del altro per esigenze di riservatezza, inserire gli indirizzi in CCN (copia conoscenza nascosta);
- avvisare l'azienda quando alla propria posta personale siano allegati files eseguibili e/o di natura incomprensibile o non conosciuta;
- non aprire e-mail inviate da mittenti sconosciuti o con indirizzi strani oppure mail con in allegato dei file zip o programmi eseguibili, in questi casi avvisare l'amministratore di sistema per una verifica;
- è vietato sollecitare donazioni di beneficenza, propaganda elettorale o altre voci non legate al lavoro.
- è vietato utilizzare il servizio di posta elettronica per trasmettere a soggetti esterni dell'organizzazione informazioni riservate o comunque documenti aziendali, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte;

Nel caso di assenza prolungata sarebbe buona norma attivare il servizio di risposta automatica (Auto-reply). In alternativa e in tutti i casi in cui sia necessario un presidio della casella di e-mail per ragioni di operatività aziendale, il soggetto autorizzato al trattamento deve nominare un collega fiduciario con lettera scritta che in caso di assenza inoltri i files necessari a chi ne abbia urgenza.

Qualora il soggetto autorizzato al trattamento non abbia provveduto ad individuare un collega fiduciario o questi sia assente o irreperibile, l'organizzazione, mediante personale appositamente incaricato, potrà verificare il contenuto dei messaggi di posta elettronica del soggetto autorizzato al trattamento, informandone il soggetto stesso e redigendo apposito verbale.

NAVIGAZIONE IN INTERNET

Il datore di lavoro, per ridurre il rischio di usi impropri della "navigazione" in Internet (consistenti in attività non correlate alla prestazione lavorativa quali la visione di siti non pertinenti, l'upload o il download di file,

l'uso di servizi di rete con finalità ludiche o estranee all'attività), ha adottato opportune misure che possono, così, prevenire controlli successivi sul lavoratore. Tali misure, possono determinare il trattamento di informazioni personali, anche non pertinenti o idonei a rivelare convinzioni religiose, filosofiche o di altro genere, opinioni politiche, lo stato di salute o la vita sessuale (art. 8 l. n. 300/1970; Provv. 2 febbraio 2006).
Tenendo conto che l'azienda effettua l'individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa, e che ha disposto il blocco di alcuni siti ritenuti di natura oltraggiosa, le principali norme da seguire da parte del lavoratore sono:

- non è consentito lo scarico di software gratuiti (freeware) e shareware prelevati da siti internet, se non espressamente autorizzati dall'azienda;
- non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- 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 dal Titolare e con il rispetto delle normali procedure di acquisto;
- è vietata la partecipazione a forum non professionali, l'utilizzo di chat line, di bacheche elettroniche o partecipare a gruppi di discussione o lasciare commenti ad articoli o iscriversi a mailing list spendendo il marchio o la denominazione dell'organizzazione, salvo specifica autorizzazione dell'organizzazione stessa;
- è vietato al soggetto autorizzato al trattamento di promuovere utile o guadagno personale attraverso l'uso di Internet o della posta elettronica aziendale;
- è vietato accedere dall'esterno alla rete interna dell'organizzazione, salvo con le specifiche procedure previste dall'azienda stessa;
- è vietato, infine, creare siti web personali sui sistemi dell'organizzazione nonché acquistare beni o servizi su Internet a meno che l'articolo acquistato non sia stato approvato a titolo di spesa professionale;
- è vietato accedere ad alcuni siti internet mediante azioni inibenti dei filtri, sabotando o comunque superando o tentando di superare o disabilitando i sistemi adottati dall'azienda per bloccare accessi non conformi all'attività lavorativa. In ogni caso è vietato utilizzare siti o altri strumenti che realizzino tale fine;
- è vietato utilizzare l'accesso ad internet in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore (es. legge 22 aprile 1941, n. 633 e successive modificazioni, d.lgs. 6 maggio 1999, n. 169 e legge 18 agosto 2000, n. 248). In particolare, è vietato il download di

materiale soggetto a copyright (testi, immagini, musica, filmati, file in genere, …) se non espressamente autorizzato dall'organizzazione;

- è vietato l'utilizzo L'accesso ai social network (Ex: facebook, twitter, linkedin, etc..). Se l'utilizzo dei social network deve avvenire per esigenze strettamente lavorative dovrà essere effettuata una richiesta scritta alla direzione la quale fornirà a sua volta una autorizzazione scritta.

Ogni eventuale navigazione di questo tipo, comportando un illegittimo utilizzo di Internet, nonché un possibile illecito trattamento di dati personali e sensibili è posta sotto la personale responsabilità del soggetto autorizzato al trattamento inadempiente.

L'UTILIZZO DEL NOTEBOOK, TABLET O SMARTPHONE

Il computer portatile, il tablet e il cellulare (di seguito generalizzati in "device mobile") possono venire concessi in uso dall'organizzazione agli Soggetti autorizzati al trattamento che durante gli spostamenti necessitino di disporre di archivi elettronici, supporti di automazione e/o di connessione alla rete dell'organizzazione.

Il soggetto autorizzato al trattamento è responsabile dei device mobili assegnatigli dall'organizzazione e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai device mobili si applicano le regole di utilizzo previste per i computer connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna. In particolare i files creati o modificati sui device mobili devono essere trasferiti sulle memorie di massa aziendali al primo rientro in ufficio e cancellati in modo definitivo dai device mobili (Wiping). Sui device mobili è vietato installare applicazioni (anche gratuite) se non espressamente autorizzate dall'ente. I device mobili utilizzati all'esterno (convegni, visite in azienda, ecc…), in caso di allontanamento, devono essere custoditi in un luogo protetto. In caso di perdita o furto dei device mobili deve far seguito la denuncia alle autorità competenti. Allo scopo si deve avvisare immediatamente l'azienda che provvederà – se del caso – ad occuparsi delle procedure connesse alla privacy. Anche di giorno, durante l'orario di lavoro, al soggetto autorizzato al trattamento non è consentito lasciare incustoditi i device mobili.

Al soggetto autorizzato al trattamento è vietato lasciare i device mobili incustoditi e a vista dentro l'auto o in una stanza d'albergo o nell'atrio dell'albergo o nelle sale d'attesa delle stazioni ferroviarie e aeroportuali.

I device mobili che permettono l'attivazione di una procedura di protezione (PIN) devono sempre essere abilitabili solo con la digitazione del PIN stesso e non possono essere lasciti privi di PIN.

Laddove il device mobile sia accompagnato da un'utenza, il soggetto autorizzato al trattamento è chiamato ad informarsi preventivamente dei vincoli ad essa associati (es. numero minuti massimo, totale gigabyte dati,

…) e a rispettarli. Qualora esigenze lavorative richiedessero requirements differenti il soggetto autorizzato al trattamento è tenuto ad informare tempestivamente e preventivamente l'zienda.

In relazione alle utenze mobili, salvo autorizzazione dell'organizzazione, è espressamente vietato ogni utilizzo all'estero e anche in caso di autorizzazione dell'organizzazione, gli utilizzi all'esterno devono essere preventivamente comunicati all'organizzazione per permettere l'attivazione di opportuni contratti di copertura con l'operatore mobile di riferimento.

In particolare le principali regole sull'utilizzo degli smartphone sono:

- l'uso della password o di codici di sblocco,
- imporre agli utenti l'uso di software di remote wiping per cancellare i dati una volta che il dispositivo dovesse cadere in mani sbagliate;
- inibire l'uso di dispositivo con jailbreack (Apple) o root (Android), cioè quei sistemi che consentono di modificare funzionalità del sistema operativo di un dispositivo mobile;
- potranno essere effettuati in attuazione di eventuali controlli sull'utilizzo dei smartphone concessogli in uso per esclusive finalità professionali;
- tale strumento è aziendale e in quanto tale deve essere utilizzato solo per attività collegate all'azienda e in caso di furto e/o smarrimento va immediatamente comunicato ai responsabili;
- è consentito installare programmi provenienti dall'esterno solo se espressamente autorizzati dall'azienda, per evitare il pericolo di virus.

UTILIZZO DI SMARTPHONES PERSONALI

In caso di utilizzo di uno smartphone o device personale (BYOD) per accesso alla rete o posta aziendale (o alle informazioni aziendali), il dipendente deve garantire:

- l'uso della password o di codici di sblocco;
- l'uso di software di remote wiping per cancellare i dati una volta che il dispositivo dovesse cadere in mani sbagliate;
- che non vi siano dispositivi con jailbreack (Apple) o root (Android), cioè quei sistemi che consentono di modificare funzionalità del sistema operativo di un dispositivo mobile;
- la possibilità di predisporre il device al Titolare e/o Responsabile Privacy per poter effettuare eventuali controlli sull'utilizzo della sim aziendale e dei relativi dati professionali;
- in caso di furto e/o smarrimento va immediatamente comunicato al Titolare e/o al Responsabile Privacy;
- installazione di un antivirus.

L'UTILIZZO DEL NOTEBOOK, TABLET O SMARTPHONE PERSONALI

Ai dipendenti non è permesso svolgere la loro attività su PC fissi, portatili, device personali.

Ai dipendenti, se espressamente autorizzati dall'ente, è permesso solo l'utilizzo della posta elettronica aziendale sui loro device personali. In tal caso è necessario che il device abbia password di sicurezza stringenti approvate dall'ente e l'eventuale furto o smarrimento del device deve essere immediatamente segnalato anche all'ente per eventuali provvedimenti di sicurezza.

Al collaboratore è vietato l'utilizzo di memorie esterne personali (quali chiavi USB, memory card, cd-rom, DVD, macchine fotografiche, videocamere, tablet, …).

Durante l'orario di lavoro, comprese le eventuali pause, ai Soggetti autorizzati al trattamento è concesso l'utilizzo del telefono cellulare personale ma solo per comunicazioni di emergenza o strettamente collegate all'ambito lavorativo.

In caso di trasferte lavorative all'esterno degli uffici dell'organizzazione, il telefono personale può rimanere acceso, anche per facilitare la comunicazione con l'organizzazione stessa ove fosse necessario.

In questo caso si invita, comunque, a non utilizzarlo per fini personali, in modo particolare alla presenza di clienti o fornitori.

UTILIZZO DI SISTEMI CLOUD

E' vietato ai soggetti autorizzati al trattamento l'utilizzo di sistemi cloud non espressamente approvati dall'azienda. Per essere approvati i sistemi cloud devono rispondere ad almeno i seguenti requisiti:

- Essere sistemi cloud esclusivi e non condivisi;
- Essere sistemi cloud posizionati fisicamente in Italia;
- L'azienda che fornisce il sistema in cloud deve essere preventivamente nominata Responsabile al Trattamento dei dati da parte dell'azienda;
- L'azienda che fornisce il sistema in cloud deve comunicare all'azienda, almeno una volta all'anno, i nominativi degli amministratori di sistema utilizzati.

Dovranno essere verificate tutte le indicazioni e prescrizioni previste dal Garante della Privacy nei suoi provvedimenti sugli Amministratori di Sistema e sul cloud.

GESTIONE DATI CARTACEI

Tenendo conto che l'azienda effettua ancora una buona parte di trattamenti dati su supporti cartacei:

- si esorta la massima attenzione alla conservazione e protezione di tali documenti presso la propria postazione di lavoro durante l'orario di lavoro;

- tali documenti devono essere riposti negli archivi e contenitori preposti (armadi, locale archivio, cassettiere) al di fuori dell'orario di lavoro.

Chi esce dall'ufficio al termine dell'attività lavorativa deve accertarsi se qualcuno è ancora presente in ufficio; in caso negativo deve provvedere alla chiusura dei locali.

I Soggetti autorizzati al trattamento sono responsabili del controllo e della custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.

I Soggetti autorizzati al trattamento sono invitati dall'organizzazione ad adottare una "politica della scrivania pulita". Ovvero si richiede ai soggetti autorizzati al trattamento di trattare dati cartacei solo se necessario, privilegiando, ove possibile, l'utilizzo degli strumenti digitali messi a disposizione dell'azienda.

I principali benefici di una politica della scrivania pulita sono:

- Una buona impressione a utenti e fornitori che visitano la nostra organizzazione;
- la riduzione della possibilità che informazioni confidenziali possano essere viste da persone non abilitate a conoscerle;
- la riduzione della possibilità che documenti confidenziali possano essere sottratti all'organizzazione.

In particolare, si invita a non lasciare in vista sulla propria scrivania dati cartacei quando ci si allontana dalla stessa oppure quando è previsto un incontro con un soggetto non abilitato alla conoscenza dei dati in essi contenuti.

Prima di lasciare la propria postazione (per esempio per la pausa pranzo o per una riunione) sarà cura dei soggetti autorizzati al trattamento riporre in luogo sicuro (armadio, cassettiera, archivio, …) i dati cartacei ad esso affidati, affinché gli stessi non possano essere visti da terzi non autorizzati (es. addetti alle pulizie) o da terzi (visitatori) presenti nell'azienda.

A fine giornata deve essere previsto il riordino della scrivania e la corretta archiviazione di tutte le pratiche d'ufficio, in modo da lasciare la scrivania completamente sgombra.

Ove possibile, si invita ad evitare la stampa di documenti digitali, anche ai fini di ridurre l'inquinamento ed il consumo delle risorse in ottica ecologica.

Ove possibile, si invita ad effettuare la scansione dei documenti cartacei ed archiviarli digitalmente.

E' necessario rimuovere immediatamente ogni foglio stampato da una stampante o da un'apparecchiatura fax, per evitare che siano prelevati o visionati da soggetti non autorizzati.

Ove possibile, è buona norma eliminare i documenti cartacei attraverso apparecchiature trita documenti.

APPLICAZIONE E CONTROLLO

L'azienda, in qualità di Titolare degli strumenti informatici, dei dati ivi contenuti e/o trattati, si riserva la facoltà di effettuare i controlli che ritiene opportuni per le seguenti finalità:

- tutelare la sicurezza e preservare l'integrità degli strumenti informatici e dei dati;
- evitare la commissione di illeciti;
- verificare la funzionalità del sistema e degli strumenti informatici.

Le attività di controllo potranno avvenire anche con audit e vulnerability assesment del sistema informatico. Per tali controlli l'organizzazione si riserva di avvalersi di soggetti esterni.

Si precisa, in ogni caso, che l'organizzazione non adotta "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori" (ex art. 4, primo comma, l. n. 300/1970), tra cui sono certamente comprese le strumentazioni hardware e software mirate al controllo dell'utente.

L'azienda informa di non adottare sistemi che determinano interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.

In particolare eventuali sistemi atti a monitorare eventuali violazioni di legge o comportamenti anomali da parte dei soggetti autorizzati al trattamento avvengono nel rispetto del principio di pertinenza e non eccedenza, con esclusione di registrazioni o verifiche con modalità sistematiche.

I sistemi software sono stati programmati e configurati in modo da cancellare periodicamente ed automaticamente i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

SANZIONI

È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente disciplinare. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente e dei collaboratori con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL, nonché con tutte le azioni civili e penali consentite.

VALIDITA'

Il presente Disciplinare ha validità a partire dall' 1 dicembre 2019.

Il presente Disciplinare sarà oggetto di aggiornamento ogni volta che se ne ravvisi la necessità, in caso di variazioni tecniche dei sistemi dell'organizzazione o in caso di modifiche legislative. Ogni variazione del presente Disciplinare sarà comunicata ai soggetti autorizzati al trattamento.

FIRMA TITOLARE O RESPONSABILE DEL TRATTAMENTO DEI DATI

_____

Data _____

In data _____

il presente documento è stato consegnato a _____ (nome persona autorizzata),

che dichiara di averlo ricevuto e di averne preso visione.

_____

Firma della persona autorizzata