DISCIPLINARE INTERNO SULL'UTILIZZO DI INTERNET, DELLA POSTA ELETTRONICA E DELLE RISORSE INFORMATICHE

(redatto sulla base delle indicazioni contenute nel Regolamento in materia di protezione dei dati personali 2016/679, nel D. Lgs. 196/03 "Codice in materia di protezione dei dati personali" (novellato dal D. Lgs. n. 101/2018), nel Provvedimento Generale del Garante per la protezione dei dati personali del 1 marzo 2007, n. 13 "Lavoro: le linee guida del Garante per posta elettronica e internet", nella Legge 20/05/1970 n. 300 "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento")

INDICE

1) Premessa e finalità

Il presente disciplinare interno è redatto dal TITOLARE DEL TRATTAMENTO denominato per brevità, anche "l'intermediario" o "l'Azienda") sulla base delle prescrizioni contenute nel Regolamento Europeo in materia di protezione dei dati personali (Regolamento UE 2016/679), nel D. Lgs. 196/2003 "**Codice in materia di protezione dei dati personali**" (novellato dal D. Lgs. n. 101/2018), nel Provvedimento Generale del Garante per la protezione dei dati personali del 1 marzo 2007, n. 13 "**Lavoro: le linee guida del Garante per posta elettronica e internet**" e nella Legge 20/05/1970 n. 300 "**Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento**".

La finalità del presente disciplinare interno (di seguito denominato per brevità, anche "il Disciplinare" o "il Documento") è quella di specificare le modalità e le prescrizioni sull'utilizzo durante il rapporto di lavoro delle risorse informatiche, della posta elettronica e della rete internet da parte degli utenti assegnatari che a vario titolo operano nella struttura aziendale (in particolare, dei dipendenti e dei collaboratori) allo scopo di tutelare i beni aziendali ed evitare condotte scorrette che potrebbero esporre l'azienda a problematiche di sicurezza, di carattere patrimoniale e di immagine per i danni eventualmente cagionati a terzi.

Il presente documento, nella parte in cui contiene le regole per l'utilizzo dei beni e risorse informatiche aziendali vale:

- quale "disciplinare interno" ai sensi della Deliberazione 1° Marzo 2007, n. 13 dell'Autorità Garante per la protezione dei dati personali recante le "*Linee Guida per posta elettronica e Internet*";
- quale informativa ai sensi e per gli effetti dell'art. 13 del Regolamento (UE) 2016/679, così come disposta dal punto 3.3 delle Linee Guida citate.

2) Ambito di applicazione

Il presente disciplinare interno si applica a tutti i dipendenti e collaboratori dell'intermediario (di seguito, per brevità, anche gli "Utenti").

Tali prescrizioni integrano e si aggiungono alle specifiche istruzioni impartite dall'intermediario negli atti di autorizzazione al trattamento dei dati personali e nelle specifiche procedure e policy aziendali adottate in materia. L'intermediario si riserva di fornire ai dipendenti/collaboratori ulteriori istruzioni, ove necessario, in particolare in relazione a specifici incarichi e compiti affidati.

3) Normativa di riferimento

Il quadro normativo oggetto del presente disciplinare è il seguente:

- Legge 20.05.1970 n. 300, recante "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento";

-art. 23 del D. Lgs. n. 151/2015 (c.d. Jobs Act) che modifica e rimodula la fattispecie integrante il divieto dei controlli a distanza, nella consapevolezza di dover tener conto, nell'attuale contesto produttivo, oltre agli impianti audiovisivi, anche degli altri strumenti "dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori" e di quelli "utilizzati dal lavoratore per rendere la prestazione lavorativa";

-Regolamento (Ue) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
-D. Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" integrato con le modifiche introdotte dal Decreto Legislativo 10 agosto 2018, n. 101;
-D. Lgs. n. 101 del 10 agosto 2018 ("Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati");
-Provvedimenti del Garante per la protezione dei dati personali con riguardo agli Amministratori di Sistema (Provvedimento generale del 27 novembre 2008);
− Garante della privacy "Linee guida per posta elettronica e internet" del 01.03.2007.

4) Principi

I principi che sono a fondamento del presente disciplinare (cfr. "Linee guida per posta elettronica e internet" del 01.03.2007, articolo 2.3.) sono specificatamente:

a) il principio di necessità, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite;
b) il principio di correttezza, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori. L'azienda pertanto favorisce la formazione continua di tutto il personale al fine di acquisire la necessaria consapevolezza nell'uso delle tecnologie informatiche e più in generale del corretto utilizzo dei dati personali che per motivi di lavoro si trova a trattare;
c) i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime osservando il principio di pertinenza e non eccedenza.

5) Definizioni

- **trattamento:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- **dato personale:** qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- **dati relativi alla salute:** i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- **categorie particolari di dati personali:** i dati personali che rivelino l'origine razziale o

etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;

- **violazione dei dati personali**: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- **titolare del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
- **responsabile del trattamento**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- **profilazione**: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- **pseudonimizzazione**: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- **archivio**: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- **utente di posta elettronica**: persona autorizzata ad accedere al servizio di posta elettronica;
- **LOG**: archivio delle attività effettuate in rete dall'utente;
- **credenziali di autenticazione**: codice utente e password richieste dal sistema o dalla postazione di lavoro per verificare se l'utente è autorizzato ad accedere e con quali modalità.

6) Titolarità dei beni e delle risorse informatiche

I beni e le risorse informatiche, i servizi IT (Information and Technology) e le reti informative costituiscono beni aziendali rientranti nel patrimonio aziendale e sono da considerarsi di esclusiva proprietà dell'azienda.

Il loro utilizzo, pertanto, è consentito esclusivamente per lo svolgimento delle mansioni lavorative affidate e per il tempo necessario all'espletamento delle stesse.

7) Postazioni di lavoro: regole generali

Per postazione di lavoro si intende il complesso unitario di Personal Computer, notebook, smartphone, tablet e ogni altro device concesso dall'azienda in utilizzo all'utente **unicamente per svolgere la propria attività lavorativa**.

L'assegnatario di tali beni e strumenti informatici aziendali, pertanto, è tenuto ad usare la massima diligenza, nel rispetto degli obblighi di cui agli articoli 2104 e 2105 del codice civile, utilizzandoli esclusivamente per lo svolgimento dell'attività lavorativa. Comportamenti difformi possono causare gravi rischi alla sicurezza ed all'integrità dei sistemi aziendali e possono essere oggetto di valutazione da un punto di vista disciplinare.

Al fine di disciplinare un corretto utilizzo dei suddetti beni aziendali, l'azienda ha adottato le regole tecniche generali, che di seguito si riportano:

- ogni PC, notebook (accessori e periferiche incluse), e altro device, sia esso acquistato, noleggiato, o affidato in locazione, rimane di esclusiva proprietà dell'azienda, ed è concesso all'utente per lo svolgimento delle proprie mansioni lavorative e comunque per finalità strettamente attinenti l'attività lavorativa svolta;
- è dovere di ogni utente usare i computer e gli altri dispositivi a lui affidati in modo responsabile e professionale;
- le postazioni di lavoro non devono essere lasciate incustodite con le sessioni utenti attive;
- quando un utente si allontana dalla propria postazione di lavoro, deve bloccare tastiera e schermo con un programma salvaschermo (screensaver) protetto da password o effettuare il log-out dalla sessione;
- l'utente deve segnalare con la massima tempestività all'amministratore del sistema informativo e/o agli incaricati dell'amministrazione del sistema informativo e/o ai soggetti specificatamente indicati dall'azienda eventuali guasti tecnici, problematiche tecniche o il cattivo funzionamento delle apparecchiature.

8) Utilizzo del personal computer

Il personal computer affidato all'utente è uno strumento di lavoro. Tale dispositivo, infatti, può essere soggetto a smarrimento, furti, distruzione o compromissione dei dati, tentativi di frode e/o accesso non autorizzato ovvero essere "*infettato*" da virus informatico che potrebbe diffondersi e ripercuotersi all'intera rete informatica aziendale, una volta che tali dispositivi siano collegati direttamente alla rete interna.

Il personal computer affidato all'utente permette l'accesso alla rete aziendale solo attraverso specifiche credenziali di autenticazione come meglio descritto di seguito nel presente Disciplinare.

Le impostazioni dei personal computer e dei relativi programmi sono installate in funzione della qualifica dell'utente, delle mansioni nonché della politica di utilizzo di tali strumenti stabilita dall'intermediario

L'utente non può modificarle autonomamente e può ottenere cambiamenti nelle impostazioni solo previa autorizzazione da parte dell'intermediario.

L'installazione sui personal computer degli utenti di sistemi operativi e programmi applicativi e, in generale, di software, avviene seguendo i necessari criteri di sicurezza. L'uso di tali programmi deve avvenire nel rispetto dei contratti di licenza che li disciplinano e delle specifiche prescrizioni di volta in volta indicate dall'intermediario.

Il Personal Computer deve essere spento **ogni sera** prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo.

9) Utilizzo di pc portatili O TABLET

L'utente è responsabile del PC portatile assegnatogli dall'azienda e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro. Le impostazioni e i programmi installati sul PC portatile non possono essere modificati.

Ai PC portatili si applicano le regole di utilizzo previste dal presente disciplinare interno, con particolare attenzione alla rimozione di eventuali *file* che non devono essere salvati o archiviati.

I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni. L'intermediario può autorizzare l'uso di **PC personali** previa autorizzazione.

La manutenzione del PC, in questo caso, è a completo carico dell'utente sia dal punto di vista hardware che software. Il collegamento del PC personale alla rete aziendale ed il relativo utilizzo è possibile dietro autorizzazione dell'intermediario , d'intesa con l'amministratore di sistema.

Resta salvo che l'utilizzo della rete aziendale e l'accesso alla rete esterna tramite l'infrastruttura dell'intermediario comporta necessariamente che il PC proprio sia dotato di software antivirus e firewall adeguato.

10) Gestione ed assegnazione delle credenziali di autenticazione

Ad ogni utente vengono assegnate delle credenziali di autenticazione che consistono in una User-ID e una Password. Lo User-ID permette di identificare l'utente all'interno del sistema informatico in modo specifico.

Gestione Password

Parole chiave deboli

Le parole chiave di facile individuazione hanno le seguenti caratteristiche:

• La parola chiave contiene meno di 8 caratteri, anche se il sistema può accettare parole chiave di 8 caratteri ed oltre;

• La parola chiave e una parola di uso comune, come ad esempio il nome di qualche membro della famiglia, di animali da salotto, di amici, di collaboratori o di caratteri di fantasia;

• Sono da ritenere insoddisfacenti anche parole chiave legate a espressioni informatiche, hardware e software, come pure quelle legate a date di nascita od altre informazioni, come l'indirizzo, il numero telefonico e simili.

Parole chiave sicure

Sono da ritenere parole chiave di soddisfacente sicurezza quelle che hanno le seguenti caratteristiche:

- Sono composte da caratteri maiuscoli e minuscoli. Utilizzano anche caratteri di interpunzione. come; | . j . * " . ed una miscela di numeri e lettere;
- Devono avere una lunghezza minima di 8 caratteri alfanumerici se il sistema consente raggiungere questa lunghezza;
- Non devono essere basate su informazioni personali, come nomi di membri della famiglia e simili.

Le parole sicure non devono mai essere scritte o archiviate in linea (non ci devono essere file con il nome password.doc o pwd.xls).

La Password è personale e non può essere comunicata ad altre persone. **E' severamente vietato usare la password e lo User-ID di un altro utente.**

È necessario procedere alla modifica della password al primo utilizzo e, successivamente, almeno ogni
a **tre mesi**.

I codici identificativi e le password dei dipendenti saranno disattivati nel caso in cui i dipendenti cessino il loro rapporto di lavoro, oltre che nei casi espressamente e tassativamente previsti dalla normativa.

11) Utilizzo della rete aziendale

Per l'accesso alla rete aziendale ogni utente deve essere in possesso della specifica credenziale di autenticazione.

È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parole chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite dall'intermediario.

L'azienda si riserva la facoltà di procedere alla rimozione di ogni *file* o applicazione che riterrà pericolosi per la sicurezza del sistema informatico ovvero acquisiti o installati in violazione del presente disciplinare.

12) Utilizzo di fax, fotocopiatrici, scanner e stampanti aziendali

L'utente è consapevole che gli strumenti di stampa sono di proprietà dell'azienda e sono resi disponibili al medesimo per rendere la prestazione lavorativa. L'utilizzo, pertanto, di tali strumenti è concesso esclusivamente per tale fine.

È vietato l'utilizzo delle fotocopiatrici per fini personali, salvo preventiva ed esplicita autorizzazione da parte dell'azienda. In particolare, durante l'utilizzo delle stampanti in parola, gli utenti sono tenuti a stampare documenti solo se strettamente necessari per lo svolgimento delle proprie mansioni e a prediligere la stampa in bianco/nero e fronte/retro al fine di evitare sprechi di carta e costi inutili, se possibile.

Nella fattispecie in cui si rendesse necessaria la stampa di informazioni riservate l'utente dovrà presidiare il dispositivo di stampa per evitare la possibile perdita o divulgazione di tali informazioni e persone terze non autorizzate.

13) Utilizzo dei supporti di memorizzazione

L'utilizzo di supporti di memorizzazione personali (come ad esempio, penne o chiavi di memoria USB, etc.) soggiace alle istruzioni di seguito riportate:

- E' vietato l'utilizzo di supporti di memorizzazione personali (penne o chiavi di memoria USB, etc.) salvo specifiche autorizzazioni rilasciate per iscritto dall'intermediario;
- è fatto assoluto divieto di copiare o duplicare files di dati personali ricevuti dall'azienda e/o comunque raccolti per lo svolgimento dei propri compiti nonché i dati personali trattati nello svolgimento o per effetto della propria attività lavorativa; deroga al presente divieto deve essere espressamente concordata per iscritto con l'azienda;

- in nessun caso, inoltre, tali dati potranno essere copiati e/o duplicati su qualunque tipo di supporto esterno di memorizzazione (per esempio, chiavette USB, etc.) e/o mediante accesso ai sistemi di file hosting e/o cloud storage (ad esempio, Dropbox; Google Drive; SkyDrive, etc.), salvo specifiche autorizzazioni rilasciate per iscritto dall'intermediario;
- nell'esercizio delle proprie mansioni lavorative l'accesso ai sistemi di file hosting e/o cloud storage non è in alcun modo consentito, salva diversa indicazione scritta dell'azienda.

14) Utilizzo della posta elettronica aziendale

La casella di posta elettronica assegnata all'utente è uno strumento di lavoro, pertanto le persone assegnatarie di caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. Ad ogni dipendente titolare di un *account* utente, viene assegnata una casella di posta elettronica individuale (per esempio, nome.cognome@azienda.it).

Nei termini e modalità stabilite dall'azienda, alla stessa persona può/possono essere assegnata/e ulteriore/i caselle di posta elettronica che possono essere condivise con altre persone della stessa area/gruppo/dipartimento (per esempio, amministrazione@azienda.it).

È fatto divieto di utilizzare le caselle di posta elettronica ufficiali per motivazioni diverse da quelle strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:

- 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 catene telematiche (o di Sant'Antonio). Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

Nel caso di mittenti sconosciuti o messaggi insoliti, per non correre il rischio di essere infettati da virus, occorrerà cancellare i messaggi senza aprirli.

Nel caso di messaggi provenienti da mittenti conosciuti ma che contengono allegati sospetti (file con estensione **.exe .scr .pif .bat .cmd**), questi ultimi non devono essere aperti.

Si richiede, inoltre, di prestare particolare attenzione ad e-mail nelle quali sono richiesti dati personali (ad esempio numeri di carte di credito, codici di identificazione, etc.) in quanto potrebbero essere tentativi di phishing; tali e-mail devono essere spostate nella cartella di posta indesiderata.

E' fatto divieto di inviare messaggi completamente estranei al rapporto di lavoro.

La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.

Occorre, inoltre, che i messaggi di posta elettronica contengano un avvertimento ai destinatari nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi, precisando se le risposte potranno essere conosciute nell´organizzazione di appartenenza del mittente.

Accesso alla casella di posta elettronica del lavoratore assente

Sono messe a disposizione di ciascun utente, con modalità di agevole esecuzione, apposite funzionalità del sistema di posta elettronica che consentano di inviare automaticamente, in caso

di assenze programmate (ad esempio, per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" di un altro soggetto cui trasmettere le comunicazioni e-mail di contenuto lavorativo o altre utili modalità di contatto in caso di assenza dell'utente.

In caso di eventuali assenze non programmate (ad es., per malattia), qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi *webmail*), l'azienda, perdurando l´assenza oltre un determinato limite temporale (pari a 3 giorni), disporrà lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (ad es., l´amministratore di sistema oppure, se presente, un incaricato aziendale per la protezione dei dati), l´attivazione di un analogo accorgimento (risposta automatica o re-indirizzamento, avvertendo l'assente.

Laddove l'azienda necessiti di conoscere il contenuto dei messaggi di posta elettronica dell'utente assente per cause improvvise o prolungate e per improrogabili necessità legate all'attività lavorativa, si procederà nei termini di seguito indicati:

- la verifica del contenuto dei messaggi di posta elettronica (e l'inoltro al titolare del trattamento di quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa) sarà effettuata per il tramite di idoneo "fiduciario", da intendersi quale lavoratore previamente nominato/incaricato (per iscritto) dall'utente assente;
- di tale attività sarà redatto apposito verbale da parte dell'azienda e informato l'utente interessato alla prima occasione utile.

Gestione dell'account di posta elettronica successivamente alla cessazione del rapporto di lavoro e/o collaborazione

Successivamente alla cessazione del rapporto di lavoro e/o collaborazione, si procederà nei termini di seguito delineati:

1) immediata disattivazione e rimozione degli account di posta elettronica aziendale riconducibili all'ex dipendente (in un tempo ragionevole commisurato ai tempi tecnici di predisposizione delle misure da definire con l'amministratore di sistema e/o con gli incaricati dell'amministrazione del sistema informativo e comunque entro un periodo massimo di 30 giorni dalla data di cessazione del rapporto di lavoro/collaborazione);
2) adozione contestuale di sistemi automatici di informazione ai soggetti terzi e indicazione agli stessi di uno o più indirizzi alternativi riferiti all'attività professionale dell'azienda;
3) introduzione di accorgimenti tecnici per impedire la visualizzazione dei messaggi in arrivo sui predetti account durante il periodo in cui tale sistema automatico è in funzione.

15) Utilizzo della rete internet

La rete internet può e deve essere utilizzata dall'utente a supporto all'attività lavorativa.

Il PC assegnato al singolo utente ed abilitato alla navigazione in Internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa.

È quindi assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa in quanto potrebbe esporre il PC fornito in uso a rischi per la sicurezza del dispositivo e dei dati trattati.

Le norme di comportamento da osservare nell'utilizzo delle connessioni ad Internet sono le seguenti:

- L'utilizzo è consentito per scopi aziendali e, pertanto, non è consentito navigare in siti non attinenti allo svolgimento delle proprie mansioni lavorative.
- Non è consentita l'effettuazione di ogni genere di transazione finanziaria, ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi in cui tali operazioni siano attinenti allo svolgimento delle proprie mansioni. L'azienda non è responsabile dell'integrità e della sicurezza delle credenziali personali del dipendente nel corso delle operazioni sopra descritte svolte a fini personali.
- È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.
- Non è consentita la navigazione in siti e la memorizzazione di documenti informatici di natura oltraggiosa, pornografica, pedopornografica e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

Per facilitare il rispetto delle suddette regole, l'azienda si riserva, per mezzo dell'amministratore di sistema e/o degli incaricati dell'amministrazione del sistema informativo, la facoltà di configurare specifici ulteriori filtri che inibiscono l'accesso ai contenuti ivi non consentiti (con esclusione dei siti istituzionali) e che prevengono operazioni non correlate all'attività lavorativa (ad esempio, upload, restrizione nella navigazione, download di file o software).

In particolare, nel suddetto ambito inerente la navigazione sul web, l'azienda adotta specifiche misure al fine di prevenire controlli successivi sull'utente quali:

- trattamento di dati in forma anonima o tale da precludere l´immediata identificazione di utenti mediante loro opportune aggregazioni (ad es., con riguardo ai *file* di *log* riferiti al traffico *web*, su base collettiva o per gruppi sufficientemente ampi di lavoratori);
- eventuale conservazione nel tempo dei dati strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza.

16) Lavoro "agile"

Per l'esecuzione della prestazione lavorativa in modalità "Smart working", si devono osservare le seguenti prescrizioni:

Regole generali e strumenti non elettronici

- adottare ogni necessaria cautela per impedire l'accesso non autorizzato o il trattamento non consentito di dati personali a persone non autorizzate (per esempio, familiari o soggetti che frequentano il luogo in cui si svolge lo smart working);
- evitare che le conversazioni telefoniche aventi ad oggetto informazioni inerenti l'attività lavorativa siano oggetto di ascolto da parte di soggetti non autorizzati, i quali devono essere mantenuti ad una distanza che consenta di proteggere la confidenzialità delle informazioni;
- l'asporto dagli archivi aziendali di documenti cartacei contenenti dati personali presso la postazione di lavoro in cui si svolge lo smart working deve essere autorizzata dall'azienda;
- in tale fattispecie, previa autorizzazione del Titolare, l'utente sarà tenuto al controllo ed alla custodia degli stessi in maniera tale da impedire a chiunque non autorizzato di accedere agli stessi; a tal fine, ogni qual volta l'utente dovesse per qualsiasi ragione allontanarsi dal posto di lavoro in cui si svolge lo smart working, dovrà riporre i documenti contenenti i dati di cui sopra in

luoghi non accessibili da persone non autorizzate, come cassetti o archivi dotati di serratura;

- i documenti cartacei contenenti dati personali prima di essere cestinati devono essere resi non decifrabili e/o non ricostruibili;

Dispositivi aziendali

- qualora l'utente dovesse allontanarsi dagli strumenti elettronici aziendali utilizzati per il trattamento dei dati durante una sessione di lavoro, questi non dovranno mai essere lasciati incustoditi e/o accessibili e, a tale scopo, l'utente dovrà attivare lo screen saver associato ad una password;
- utilizzare gli strumenti elettronici aziendali solo ed esclusivamente per l'esecuzione della prestazione lavorativa;
- è fatto divieto di inserire nel dispositivo aziendale device esterni (per esempio, chiavette USB, etc.), salvo espressa autorizzazione del Titolare;
- è fatto divieto di trasferire documenti inerenti l'attività lavorativa in dispositivi personali, salvo esplicita autorizzazione del Titolare e previa adozione delle misure tecniche di sicurezza indicate dal Titolare (per esempio, sistemi di crittografia, etc.);
- sugli strumenti hardware in uso per l'attività lavorativa l'utente avrà cura di non utilizzare ovvero installare applicativi non autorizzati dal Titolare;
- accedere alle banche dati esistenti su elaboratori mediante le credenziali di autenticazione previste (Codice di Identificazione e Parola Chiave), curando che le stesse rimangano riservate e siano altresì aggiornate nei termini previsti dal presente Disciplinare;
- la parola chiave non dovrà essere condivisa con alcun soggetto e sarà gestita come informazione strettamente personale;
- l'utilizzo della rete internet attraverso gli strumenti elettronici aziendali dovrà essere limitato alle operazioni strettamente necessarie all'espletamento dell'attività lavorativa. È fatto divieto, pertanto, di servirsi di tale strumento per proprio uso personale;
- è fatto divieto di comunicare e/o condividere con i colleghi documenti aziendali e/o attinenti l'attività lavorativa tramite mezzi e/o piattaforme diverse da quelle espressamente indicate e autorizzate dal Titolare;

Dispositivi personali

- utilizzare l'accesso a connessioni Wi-Fi adeguatamente protette;
- effettuare il log-out dall'applicativo/portale/infrastruttura aziendale utilizzati al termine di ogni sessione lavorativa;
- è fatto divieto di trasferire documenti inerenti l'attività lavorativa dall'applicativo/portale/infrastruttura aziendale utilizzato per l'esecuzione della prestazione lavorativa in cartelle e/o directory personali, salvo esplicita autorizzazione del Titolare;
- accedere all'applicativo/portale/infrastruttura aziendale tramite un PC o notebook sul quale è installato un software antivirus e antimalware;
- aggiornare in modo costante i software di protezione (in particolare, antivirus, e antimalware) ai fini di una protezione adeguata del dispositivo;
- eseguire costantemente gli aggiornamenti del sistema operativo in uso;
- accedere alle banche dati esistenti su elaboratori mediante le credenziali di autenticazione previste (Codice di Identificazione e Parola Chiave), curando che le stesse rimangano riservate e siano altresì aggiornate nei termini previsti dal presente Disciplinare;
- la parola chiave utilizzata per accedere ai dati personali trattati non dovrà essere condivisa con alcun soggetto e sarà gestita come informazione strettamente personale;
- non installare software provenienti da fonti non ufficiali o sconosciute;
- qualora l'utente dovesse allontanarsi dagli strumenti elettronici utilizzati per il

trattamento dei dati durante una sessione di lavoro, questi non dovranno mai essere lasciati incustoditi e/o accessibili e, a tale scopo, l'utente dovrà attivare lo screen saver associato ad una password.

17) Social network, chat e forum

L'utilizzo dei profili ufficiali dell'azienda e l'utilizzo privato dei social networking da parte degli utenti è regolato dalle linee guida stabilite dalla "*Social media policy interna*" che costituisce parte integrante del presente Disciplinare.

Non è consentito l'utilizzo di sistemi di social networking sul luogo di lavoro o durante l'orario lavorativo, fatta eccezione del personale specificatamente autorizzato alla creazione e gestione dei profili ufficiali dell'azienda e dei soggetti specificatamente autorizzati per iscritto dalla medesima in relazione alle specifiche funzioni svolte.

La partecipazione a forum, blog, chat o bacheche elettroniche anche utilizzando pseudonimi (o nicknames) diversi da quelli messi a disposizione dall'azienda è consentita esclusivamente per motivi professionali previa autorizzazione per iscritto dell'azienda.

Per l'installazione e utilizzo di eventuali applicativi (per esempio, skype, Microsoft Teams, etc.), ritenuti utili o necessari dall'azienda per la comunicazione fra gli utenti, è necessaria la previa autorizzazione scritta dell'intermediario.

18) Protezioni antivirus, antispam, anti spyware

Il sistema informatico aziendale è protetto da software di sicurezza (antivirus, antispyware, etc.) al fine di evitare l'infezione da parte di virus informatici dei dispositivi tecnologici e l'eventuale propagazione alla rete aziendale.

Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.

E' fatto divieto di disabilitare, accidentalmente o con dolo, prodotti e applicativi di sicurezza (software antivirus, filtri antispam, etc.) installati sui personal computers o sulla rete locale senza previa autorizzazione dell'azienda per il tramite dell'amministratore del sistema informativo e/o dei soggetti specificatamente indicati dall'azienda.

Laddove il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto all'intermediario, per il tramite dell'amministratore del sistema informativo e/o agli incaricati dell'amministrazione del sistema informativo e/o dei soggetti specificatamente indicati dall'azienda.

Ogni dispositivo di supporto di memorizzazione elettronico di provenienza esterna all'azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato all'amministratore del sistema informativo e/o agli incaricati dell'amministrazione del sistema informativo e/o ai soggetti specificatamente indicati dall'azienda.

L'utente utilizzatore del personal computer verifica periodicamente lo stato di aggiornamento dell'antivirus aziendale installato.

A fronte di eventuali anomalie, l'utente è tenuto a informare prontamente l'azienda tramite l'amministratore del sistema ovvero e/o gli incaricati dell'amministrazione del sistema

informativo e/o i soggetti specificatamente indicati dalla medesima.

19) Amministratore di sistema

Il Provvedimento del Garante per la privacy del 27 novembre 2008 ha prescritto delle "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*".

L'amministratore di sistema è una figura professionale finalizzata alla "gestione e alla manutenzione di un impianto di elaborazione o di sue componenti".

Pertanto, ai fini del provvedimento generale possono essere considerate anche altre "*figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati*", quali gli amministratori di banche dati, di reti e di apparati di sicurezza, nonché quelli, per espressa previsione del Garante, di sistemi software complessi.

L'attività degli amministratori di sistema può riguardare anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori.

L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico.

In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

Si rende noto che l'amministratore di sistema è stato autorizzato a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (per esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.).

20) Strumenti di fonia e dispositivi in mobilità

L'utilizzo degli impianti di telefonia fissa e mobile, nonché dispositivi - quali smartphone e tablet - che consentono di usufruire della navigazione in internet tramite rete dati e/o del servizio di telefonica tramite rete cellulare, messi a disposizione dell'azienda deve avvenire in ottemperanza alle regole e limitazioni riportate nella scheda tecnica consegnata all'utente unitamente ai dispositivi di cui sopra.

Il dispositivo mobile affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa, salvo specifiche autorizzazioni rilasciate per iscritto dall'azienda.

Per l'utilizzo della posta elettronica e della rete internet attraverso i dispositivi mobili o smartphone, si applicano le regole stabilite dal suddetto Disciplinare.

Si informano gli utilizzatori dei servizi di fonia aziendale, che l'azienda eserciterà i diritti di cui
all'art. 124 D .Lgs. 196/2003 (cd. *fatturazione dettagliata*), richiedendo ai provider di telefonia i dettagli necessari ad effettuare controlli sull'utilizzo ed i relativi costi di traffico effettuato nel tempo. I controlli saranno eseguiti secondo le modalità descritte nel presente Disciplinare.

L'azienda si riserva la facoltà, qualora dall'esame del traffico di una singola utenza rilevi uno scostamento significativo rispetto alla media del consumo, di richiedere un tabulato analitico

delle
chiamate effettuate dalla SIM in incarico all'utente per il periodo interessato. L'utilizzo dei dispositivi mobili risponde alle regole che di seguito si riportano:

- ogni utente assegnatario del dispositivo è responsabile dell'uso appropriato dello stesso, e, conseguentemente, anche della sua diligente conservazione.
- I dispositivi devono essere dotati di password di sicurezza (cd. codice pin del dispositivo) che ne impedisca l'utilizzo da parte di soggetti non autorizzati. A tal fine si precisa che ogni utente deve adottare le necessarie e dovute cautele per assicurare la segretezza della password e, qualora ritenga che un soggetto non autorizzato possa esserne venuto a conoscenza, dovrà provvedere immediatamente a cambiarla dandone comunque comunicazione all'azienda.
- In caso di furto, danneggiamento o smarrimento del dispositivo mobile in oggetto, l'utente assegnatario dovrà darne immediato avviso all'azienda; ove detti eventi siano riconducibili ad un comportamento negligente, imprudente dell'utente e/o comunque a sua colpa nella custodia del bene, lo stesso sarà ritenuto unico responsabile dei danni derivanti.
- In caso di furto o smarrimento l'azienda si riserva la facoltà di attuare la procedura di remote-wipe (cancellazione da remoto di tutti i dati sul dispositivo), rendendo il dispositivo inutilizzabile e i dati in esso contenuti irrecuperabili.
- L'eventuale installazione di applicazioni, sia gratuite che a pagamento, sugli smartphone e tablet deve essere espressamente autorizzata dall'azienda, rimanendo, diversamente, a carico dell'utente le spese che l'azienda dovrà sostenere, nonché le responsabilità derivanti dall'installazione non autorizzata.

21) Gestione delle violazioni di dati personali: data breach

Per quanto concerne gli incidenti che possono determinare una violazione dei dati personali, cioè la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati (cd. "data breach"), l'art. 33 del GDPR prevede che in caso di violazione dei dati personali, "il titolare del trattamento notifica la violazione all'autorità di controllo senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo".

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento ai sensi dell'art. 34 del GDPR comunica la violazione all'interessato senza ingiustificato ritardo.

La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).

Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:
a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in

particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia"

A tal fine, ogni incidente (per esempio, l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati; il furto o la perdita di dispositivi informatici contenenti dati personali; l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, etc.; la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità; la divulgazione non autorizzata dei dati personali) deve essere segnalato dall'utente nei termini di cui alla procedura di data breach adottata dallo scrivente intermediario che costituisce parte integrante del presente Disciplinare.

22) La graduazione dei controlli sulla posta elettronica e sulla navigazione internet

L'azienda, in linea con quanto prescritto dall'ordinamento giuridico (art. 4 dello Statuto dei Lavoratori), esclude la configurabilità di forme di controllo aziendali aventi direttamente ad oggetto l'attività lavorativa del dipendente.

Ciò premesso, non si esclude che, per ragioni organizzative e produttive ovvero per esigenze dettate dalla sicurezza del lavoro e di tutela del patrimonio aziendale, siano utilizzati sistemi informatici, impianti o apparecchiature dai quali derivi la possibilità di controllo a distanza dell'attività dei lavoratori.

I controlli posti in essere, pertanto, saranno sempre tali da evitare ingiustificate interferenze con i diritti e le libertà fondamentali dei lavoratori e non saranno costanti, prolungati e indiscriminati. Tali controlli saranno effettuati secondo il principio della "gradualità" coerentemente con quanto stabilito dal Garante nelle "Linee guida per posta elettronica e internet" del 01.03.2007, all'articolo 6.1. rubricato "Graduazione" a mente del quale:

- I controlli saranno effettuati dall'amministratore del sistema ovvero e/o dagli incaricati dell'amministrazione del sistema informativo inizialmente solo su dati aggregati riferiti all'intera struttura aziendale ovvero a singole aree lavorative;
- qualora si dovessero riscontrare violazioni del presente disciplinare interno, indizi di commissione di gravi abusi o illeciti o attività contrarie ai doveri di fedeltà e diligenza, utilizzi anomali degli strumenti aziendali, sarà diffuso un avviso generalizzato, o circoscritto all'area o struttura lavorativa interessata relativo all'uso anomalo degli strumenti informatici aziendali, con conseguente invito ad attenersi scrupolosamente ai compiti e alle istruzioni impartite;
- controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie. In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

Controlli non autorizzati

In ogni caso l'azienda non può in alcun caso utilizzare sistemi da cui derivino forme di controllo a distanza dell'attività lavorativa che permettano di ricostruire l'attività del lavoratore.
Per tali s'intendono, a titolo meramente esemplificativo e non esaustivo:

- la lettura e la registrazione sistematica dei messaggi di posta elettronica, al di là di quanto necessario per fornire e gestire il servizio di posta elettronica stesso;
- la riproduzione e memorizzazione sistematica delle pagine web visualizzate da ciascun utente, dei contenuti ivi presenti, e del tempo di permanenza sulle stesse;
- la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- l'analisi occulta di computer portatili affidati in uso.

23) Conservazione dei dati relativi all'uso degli strumenti elettronici

I sistemi *software* sono programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovraregistrazione come, ad esempio, la cd. rotazione dei *log file*) i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

In assenza di particolari esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all´uso degli strumenti elettronici è giustificata esclusivamente da una finalità specifica e comprovata e limitata al tempo necessario –e predeterminato– a raggiungerla.

Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e ha luogo solo in relazione:

- ad esigenze tecniche o di sicurezza del tutto particolari;
- all´indispensabilità del dato rispetto all´esercizio o alla difesa di un diritto in sede giudiziaria;
- all´obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell´autorità giudiziaria o della polizia giudiziaria.

In questi casi, il trattamento dei dati personali (tenendo conto della normativa vigente e delle prescrizioni adottate dal Garante per la protezione dei dati personali) è limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

24) Sanzioni

L'eventuale violazione di quanto previsto dal Disciplinare interno – rilevante anche ai sensi degli art. 2104 e 2105 c.c. - potrà comportare l'applicazione di sanzioni disciplinari in base a quanto previsto dall'art. 7 dello Statuto dei Lavoratori.

L'azienda avrà cura di informare senza ritardo (e senza necessità di preventive contestazioni e/o addebiti formali) le autorità competenti, nel caso venga commesso un reato, o la cui commissione sia ritenuta probabile o solo sospettata, tramite l'utilizzo illecito o non conforme dei beni e degli strumenti informatici aziendali.

In caso di violazione accertata da parte degli utenti delle regole e degli obblighi di cui al presente Disciplinare, l'intermediario si riserva la facoltà di sospendere, bloccare o limitare gli accessi di un account, quando appare ragionevolmente necessario per proteggere l'integrità, la sicurezza e/o la funzionalità dei propri beni e strumenti informatici.