REGOLAMENTO INTERNO PER IL CORRETTO TRATTAMENTO DEI DATI PERSONALI E UTILIZZO DEI SISTEMI INFORMATICI

REV.	DATA	MOTIVO
00	Novembre 2018	Prima emissione

COMETI S.r.l. Società soggetta a direzione e coordinamento del socio unico Ecotech S.r.l.
Sede Legale: Via Tirso, 26 - 00198 Roma (RM) - Sede Operativa e Stab.: Via degli Industriali, 31 - Sansepolcro (AR) Italy - Tel. +39 0575 744211 - Fax +39 0575 744224
P.Iva e C.F. 13395161006 - Cap. Soc. EUR 20.000,00 i.v. - C.C.I.A.A. Roma N. 1444324
www.cometi.it • info@cometi.it • commerciale@cometisrl.telecompost.it

SOMMARIO

Premesso che:

- Lei ha ricevuto una lettera di nomina a Persona autorizzata al trattamento dei dati, ai sensi degli artt. 4 n. 10 e 29 del Reg. UE 2016/679,
- L'articolo 29 del GDPR prevede che *"il Responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del Titolare del trattamento, che abbia accesso a dati personali, non può trattare tali dati se non è istruito in tal senso dal Titolare del trattamento (…)",*
- Lei è autorizzato, come previsto nella nomina sopra citata, a effettuare le tipologie di trattamento - così come specificate nel Registro dei trattamenti del Titolare – per quanto di competenza dell'ufficio/funzione/settore aziendale nel quale Lei opera,

tutto ciò premesso, si dispone quanto segue.

1. Scopo e Campo di applicazione

Il presente documento contiene le istruzioni operative per le Persone autorizzate al trattamento dei dati personali dell'Azienda, conformemente al Regolamento (UE) 2016/679 (GDPR).
I dipendenti, i collaboratori e in generale tutte le persone autorizzate ad accedere ai dati personali e preposte allo svolgimento delle operazioni di trattamento relative ai dati, devono ispirarsi al principio generale di diligenza, correttezza e buona fede. Ogni utilizzo dei dati in possesso dell'Azienda diverso da finalità strettamente professionali, è espressamente vietato. Di seguito vengono esposte le regole comportamentali da seguire per evitare e prevenire condotte che, anche inconsapevolmente, potrebbero comportare rischi alla sicurezza dei dati e delle informazioni trattate nonché al sistema informativo e all'immagine dell'Azienda.

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet dai Personal Computer, espone l'Azienda e gli utenti (es. dipendenti e collaboratori della stessa) a rischi di natura patrimoniale, oltre alle responsabilità civili e penali conseguenti alla violazione di specifiche disposizioni di legge (es: legge sul diritto d'autore, normativa privacy, ecc.), creando evidenti problemi alla sicurezza e all'immagine dell'Azienda stessa.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi ai principi di diligenza, correttezza e buona fede, nonché ai principi applicabili al trattamento di dati personali, l'Azienda ha adottato il presente Regolamento interno al fine di evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati e delle informazioni.

Considerato inoltre che l'Azienda, nell'ottica di uno svolgimento proficuo e più agevole della propria attività, ha deciso di mettere a disposizione dei propri dipendenti e collaboratori, che ne necessitassero per il tipo di funzioni svolte, telefoni e mezzi di comunicazione efficienti (computer portatili, telefoni cellulari, etc.), sono state inserite nel regolamento alcune clausole relative alle modalità ed i doveri che ciascun collaboratore deve osservare nell'utilizzo di tale strumentazione.

2. Definizioni

Secondo l'articolo 4 del Regolamento (Ue) 2016/679 (GDPR), si definisce:

- **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;
- **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;
- **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.

Secondo l'articolo 9 paragrafo 1 del Regolamento (Ue) 2016/679 (GDPR), si definiscono *"dati particolari"* quei dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché 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.

3. Adempimenti della persona autorizzata al trattamento

Ciascuna persona autorizzata al trattamento è tenuta a:

- rispettare i principi generali del Regolamento (Ue) 2016/679 (GDPR), con particolare riferimento alla liceità e correttezza del proprio agire, all'obbligo di procedere alla raccolta e alla registrazione dei dati per scopi determinati, espliciti e legittimi;
- rispettare l'obbligo di riservatezza e segretezza e conseguentemente il divieto di comunicazione e diffusione dei dati trattati, nello svolgimento delle attività previste nell'ambito della mansione ricoperta;
- utilizzare i dati, cui abbia accesso, solamente per finalità compatibili all'esecuzione delle proprie mansioni o dei compiti affidati, per cui è autorizzato ad accedere alle informazioni e ad utilizzare gli strumenti aziendali;
- rispettare le misure di sicurezza idonee adottate dalla società, atte a salvaguardare la riservatezza, l'integrità e la disponibilità dei dati;
- segnalare eventuali malfunzionamenti di strumenti elettronici, violazioni di dati (in particolare si rimanda alla procedura *"Data Breach"* per le opportune specifiche) o esigenze sia di natura organizzativa, sia tecnica, che possano migliorare lo svolgimento delle operazioni affidate;
- accedere ai dati strettamente necessari all'esercizio delle proprie funzioni e competenze;
- in caso di interruzione del lavoro, anche temporanea, verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- mantenere riservate le proprie credenziali di autenticazione;
- svolgere le attività previste dai trattamenti secondo le direttive del Titolare del trattamento dei dati; non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del Titolare del trattamento dei dati;
- informare il Titolare e il Responsabile Privacy interno in caso di incidente di sicurezza che coinvolga dati particolari e

non;

– eseguire le operazioni di trattamento che le competono, nei limiti delle proprie mansioni e nel rispetto delle norme di legge e del presente regolamento.

4. Utilizzo del Personal Computer

4.1 Il Personal Computer affidato all'utente **è uno strumento di lavoro**. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza dei dati e delle informazioni trattate. Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.

4.2 Il personal computer dato in affidamento all'utente permette l'accesso alla rete aziendale solo attraverso specifiche **credenziali di autenticazione** come meglio descritto al successivo punto 5 del presente Regolamento.

4.3 L'Azienda rende noto che all'interno dell'organizzazione è presente, in qualità di Amministratore di Sistema interno, un referente che si interfaccia con le società esterne che erogano servizi di natura informatica (assistenza e manutenzione HW e SW), e che collabora con il personale delle stesse nell'erogazione del Servizio di *Information and Communication Technology*[1] (di seguito e per brevità riportato come "Servizio ICT").
Il personale di cui sopra è stato appositamente nominato per le operazioni di trattamento effettuate sui dati, e autorizzato a compiere interventi nel sistema informativo aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso e delle informazioni trattate, nonché per motivi tecnici e/o manutentivi necessari (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware etc.) richiesti dal Titolare del trattamento. Detti interventi, fatti salvi i divieti di cui ai successivi punti n. 9.2 e 10.1 e nel rispetto dei principi di necessità, pertinenza e non eccedenza del trattamento, potranno comportare l'accesso, in qualunque momento, ai dati trattati da ciascuna persona autorizzata al trattamento, ivi compresi gli archivi di posta elettronica. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Azienda, si applica anche in caso di assenza prolungata od impedimento dell'utente.

4.4 Il personale autorizzato della funzione ICT ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato esclusivamente dietro autorizzazione dell'utente e in nessun caso senza che questo abbia fornito esplicito consenso. Il personale autorizzato della funzione ICT provvede a notificare all'utente sia l'inizio che la fine del collegamento in remoto.

4.5 Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dal personale della funzione ICT per conto dell'Azienda né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre Virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone l'Azienda a gravi responsabilità civili; si evidenzia

[1] I servizi di natura informatica sono stati affidati in esterno a società informatiche, appositamente nominate come Responsabili del trattamento, con specifica attribuzione delle responsabilità inerenti le attività svolte sul sistema informativo aziendale.
Il personale esterno che accede al sistema informativo aziendale del Titolare, in forza delle attività previste contrattualmente, è stato individuato e appositamente nominato Amministratore di Sistema esterno. Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco analitico delle funzioni ad essi attribuite, è riportato in un documento interno mantenuto aggiornato a cura di ciascun Responsabile, reso disponibile su richiesta del Titolare e in caso di accertamenti da parte dell'Autorità competente.

inoltre che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore, vengono sanzionate anche penalmente.

4.6 Salvo preventiva ed espressa autorizzazione del personale della funzione ICT, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, …).

4.7 Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale della funzione ICT nel caso in cui siano rilevati virus ed adottando quanto previsto dal successivo punto 11 del presente Regolamento relativo alle procedure di protezione antivirus.

4.8 Il Personal Computer deve essere sempre spento prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. In ogni caso, lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso [2].

5. Gestione ed assegnazione delle credenziali di autenticazione

5.1 Le credenziali di autenticazione per l'accesso alla rete vengono assegnate dal personale della funzione ICT, previa richiesta del Responsabile dell'ufficio/funzione/settore nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente. Nel caso di collaboratori a progetto e coordinati e continuativi la preventiva richiesta, se necessaria, verrà inoltrata direttamente dalla Direzione aziendale (o dal Responsabile dell'ufficio/area con il quale il collaboratore si coordina nell'espletamento del proprio incarico).

5.2 Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user ID), assegnato dal Servizio ICT, associato ad una parola chiave (password) riservata che dovrà venir custodita dalla persona autorizzata al trattamento con la massima diligenza e non divulgata. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte della funzione ICT.

5.3 La parola chiave, formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili alla persona autorizzata al trattamento.

5.4 È necessario procedere alla modifica della parola chiave, a cura della persona autorizzata al trattamento, al primo utilizzo e, successivamente, almeno ogni sei mesi (ogni tre mesi nel caso di trattamento di dati c.d. "particolari" attraverso l'ausilio di strumenti elettronici).

5.5 Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, si procederà in tal senso d'intesa con il personale della funzione ICT.

[2] Una modalità automatica che evita di lasciare incustodito il pc, anche in caso di mancato spegnimento da parte dell'utente è quello di adottare il salvaschermo a tempo con obbligo di reintrodurre la password per l'accesso.

5.6 In caso di interruzione del rapporto di lavoro con l'utente, le credenziali di accesso ai sistemi informatici dell'Azienda verranno disabilitate entro un periodo massimo di 30 giorni dalla medesima interruzione. In tale periodo verrà reso operativo su detto account un messaggio in modalità auto-responder con indicato un diverso indirizzo email a cui recapitare la corrispondenza. In ogni caso l'Azienda si riserva il diritto di conservare i messaggi di posta elettronica che riterrà di rilevante importanza ai fini delle attività aziendali per un tempo massimo pari a 6 mesi dall'interruzione.

6. Utilizzo della rete aziendale

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

6.2 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.

6.3 Le cartelle utenti presenti nei server aziendali sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità vengono svolte regolari attività di controllo, amministrazione e back-up da parte del personale della funzione ICT.
Il salvataggio di dati di interesse aziendale in unità locali deve essere limitato allo stretto indispensabile e per il minor tempo possibile. Concluso il trattamento il dato locale deve essere eliminato dai dischi locali e/o riportato su unità del server. Si ricorda che tutti i dischi o altre unità di memorizzazione locali non sono soggette a salvataggio da parte del personale incaricato della funzione ICT. La responsabilità del salvataggio dei dati ivi contenuti è pertanto a carico del singolo utente.

6.4 Il personale della funzione ICT può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC delle persone autorizzate al trattamento sia sulle unità di rete.

6.5 Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

7. Utilizzo e conservazione dei supporti rimovibili e dati

7.1 E' vietato l'utilizzo di supporti rimovibili personali.

7.2 Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati personali, ciascun utente dovrà contattare il personale dell'ufficio competente e ICT e seguire le istruzioni impartite.

7.3 In ogni caso, i supporti magnetici contenenti dati personali devono essere dagli utenti adeguatamente custoditi in armadi chiusi.

7.4 L'utente è responsabile della custodia dei supporti forniti dall'azienda e contenenti dati aziendali.

7.5 È fatto obbligo conservare e custodire all'interno dell'azienda i supporti informatici removibili contenenti dati personali, informazioni, notizie o immagini di attinenza aziendale, affinché nessun soggetto terzo ne prenda visione o possesso.

8. Utilizzo di PC portatili

8.1 E' vietato caricare o inserire all'interno del portatile qualsiasi dato personale non attinente con l'attività lavorativa svolta. In ogni caso, al fine di evitare e/o ridurre al minimo la possibile circolazione di dati personali sull'apparecchio, si ricorda ai dipendenti della Società di cancellare tutti i dati eventualmente presenti prima di consegnare il portatile agli uffici competenti per la restituzione o la riparazione.

8.2 L'utente è responsabile del PC portatile assegnatogli dal Titolare e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro. Il pc assegnato (la registrazione avviene attraverso il "Modulo consegna dispositivi") non potrà mai essere ceduto a nessun titolo a terzi o a colleghi, ne lasciato incustodito in nessun luogo pubblico o privato.

8.3 Ai PC portatili si applicano le regole di utilizzo previste dal presente regolamento, con particolare attenzione alla rimozione di eventuali file elaborati prima della riconsegna. Ogni PC portatile deve essere protetto da password in accordo al punto 5. del presente regolamento/procedura.

8.4 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. Qualora venga smarrito o rubato un dispositivo mobile occorre effettuare tempestiva denuncia alle Autorità competenti e farne pervenire una copia all'Ufficio del Consegnatario il primo giorno lavorativo successivo all'evento criminoso.

8.5 Tali disposizioni si applicano anche nei confronti di utenti esterni quali agenti, ecc.

8.6 Qualsiasi file/dato estraneo all'attività lavorativa o non espressamente autorizzato, non può, nemmeno in via transitoria, essere salvato sul pc dato in dotazione all'Utente.

9. Uso della posta elettronica

9.1 La casella di posta elettronica assegnata all'utente **è uno strumento di lavoro.** Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

9.2 È fatto divieto di utilizzare le caselle di posta elettronica ***nomecognome@nomeazienda.it*** [3] per motivi diversi da quelli strettamente legati all'attività lavorativa. In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:

- l'invio e/o il ricevimento di allegati contenenti filmati o brani musicali (es.mp3) non legati all'attività lavorativa;

[3] Ovvero potrà essere realizzato un sistema di indirizzi di posta elettronica condivisi tra più utenti (ad es. *ufficiovendite@nomeazienda.it*, *ufficioreclami@nomeazienda.it* al posto di un sistema basato sull'identità personale)**.**

– l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
– la partecipazione a catene telematiche (o di Sant'Antonio). Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al personale della funzione ICT. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.

9.3 La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti.[4]

9.4 Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per l'Azienda ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere visionata od autorizzata dal Responsabile d'ufficio.

9.5 È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario. Si evidenzia però che le comunicazioni ufficiali, da inviarsi mediante gli strumenti tradizionali (fax, posta, ecc.), devono essere autorizzate e firmate dalla Direzione Generale e/o dai Responsabili di ufficio, a seconda del loro contenuto e dei destinatari delle stesse.

9.6 È obbligatorio porre la massima attenzione nell'aprire i file allegati di posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti). Qualora si ricevano mail contenenti allegati "sospetti" se ne deve dare immediata comunicazione al personale ICT che impartirà le opportune istruzioni operative.

9.7 Al fine di garantire la funzionalità del servizio di posta elettronica aziendale e di ridurre al minimo l'accesso ai dati, nel rispetto del principio di necessità e di proporzionalità, il sistema, in caso di assenze programmate (ad es. per ferie o attività di lavoro fuori sede dell'assegnatario della casella) invierà automaticamente messaggi di risposta contenenti le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto della struttura. In tal caso, la funzionalità deve essere attivata dall'utente e non è accettabile l'inoltro automatico della mail in arrivo a un altro utente.

9.8 In caso di assenza non programmata (ad es. per malattia) la procedura - qualora non possa essere attivata dal lavoratore avvalendosi del servizio webmail entro n. due giorni - verrà attivata a cura dell'azienda.

9.9 Sarà comunque consentito al superiore gerarchico dell'utente o, comunque, in accordo con l'utente, a persona individuata dall'azienda, accedere alla casella di posta elettronica dell'utente per ogni ipotesi in cui si renda necessario (ad es.: mancata attivazione della funzionalità di cui al punto 9.7; assenza non programmata ed impossibilità di attendere i n. due giorni di cui al punto 9.8).

9.10 Il personale della funzione ICT, nell'impossibilità di procedere come sopra indicato e nella necessità di non pregiudicare la necessaria tempestività ed efficacia dell'intervento, potrà accedere alla casella di posta elettronica per le sole finalità indicate al punto 4.3.

[4] Sarebbe opportuno introdurre un limite massimo della dimensione del database di posta: ad es. 200 MB.

9.11 Al fine di ribadire agli interlocutori la natura esclusivamente aziendale della casella di posta elettronica, i messaggi devono contenere un avvertimento standardizzato nel quale sia dichiarata la natura non personale dei messaggi stessi precisando che, pertanto, il personale debitamente autorizzato potrà accedere al contenuto del messaggio inviato alla stessa casella secondo le regole fissate nella propria policy aziendale.

10. Navigazione Internet

10.1 Il PC assegnato al singolo utente ed abilitato alla navigazione 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.

10.2 In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare internet per:

- l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, quando non strettamente attinenti all'attività lavorativa (filmati e musica) e previa verifica dell'attendibilità dei siti in questione (nel caso di dubbio, dovrà venire a tal fine contattato il personale della funzione ICT);
- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dalla Direzione Generale (o eventualmente dal Responsabile d'ufficio e/o della funzione ICT) e comunque nel rispetto delle normali procedure di acquisto;
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa;
- la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Responsabile d'ufficio;
- l'accesso, tramite internet, a caselle webmail di posta elettronica personale.

10.3 Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'azienda rende peraltro nota l'adozione di uno specifico sistema di blocco o filtro automatico che prevengano determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una black list.[5]

10.4 Gli eventuali controlli, compiuti dal personale autorizzato della funzione ICT ai sensi del precedente punto 4.3, potranno avvenire mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati per massimo 12 mesi, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'azienda.

11. Protezione antivirus

11.1 Il sistema informatico aziendale è protetto da software antivirus aggiornato periodicamente. 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.

[5] Indicare eventualmente in modo più dettagliato il sistema a tal fine utilizzato. Si evidenzia, comunque, che l'utilizzo di sistemi automatizzati preventivi diretti a filtrare l'accesso bloccando determinate categorie di siti potrebbe a volte non rivelarsi del tutto idoneo alla piena ed efficace fruizione del sistema informatico e delle modalità di navigazione, rallentandone in modo rilevante la funzionalità: in questa ipotesi pertanto, si renderebbero necessari controlli successivi all'attività di navigazione diretti a tutelare l'azienda ed i suoi responsabili da responsabilità anche penali connesse a reati commessi con modalità informatiche e telematiche.

11.2 Nel caso 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 al personale della funzione ICT.

11.3 Ogni dispositivo magnetico 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 al personale della funzione ICT.

12. Utilizzo dei telefoni, dispositivi mobili, fotocopiatrici aziendali e fax

12.1 Il telefono aziendale e/o dispositivo mobile (es: tablet) 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 e utilizzi a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di telefonate personali è consentito solo nel caso di comprovata necessità ed urgenza, mediante il telefono fisso aziendale messo a disposizione dell'utente.

12.2 In caso di assegnazione di un cellulare aziendale e/o dispositivo mobile (es: tablet) all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Ai dispositivi si applicano le medesime regole sopra previste per l'utilizzo del telefono aziendale: in particolare è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere SMS o MMS o email di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa. L'eventuale uso di diversa natura (anche per fini personali) del telefono cellulare aziendale e/o del dispositivo mobile è possibile soltanto in presenza di preventiva autorizzazione scritta e in conformità delle istruzioni al riguardo impartite dal personale della funzione ICT.

12.3 È vietato l'utilizzo dei fax aziendali per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte del Responsabile di ufficio.

12.4 È vietato l'utilizzo delle fotocopiatrici aziendali per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile di ufficio.

13. Accesso ai dati trattati dall'utente

13.1 Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà della Direzione Aziendale, tramite il personale della funzione ICT o Partner esterni addetti alla manutenzione, accedere direttamente, nel rispetto della

normativa sulla privacy, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

14. Lavoro a distanza

14.1 L'Azienda non ha tra le proprie tipologie contrattuali il telelavoro, ma in caso di necessità personale autorizzato può accedere da remoto tramite VPN, per l'esecuzione dei compiti loro spettanti . Tali accessi sono come di seguito regolati:

- Dato il carattere di sporadicità della connessione è ammesso il collegamento in remoto anche attraverso reti diverse da quella lavorativa;
- I dispositivi attraverso cui avviene l'accesso devono essere protetti tramite firewall e attraverso opportuno antivirus mantenuto aggiornato, oppure attraverso il collegamento con dispositivi appropriati ed immuni dalle più comuni minacce informatiche (es. unix, linux, mac osx, ecc.). Inoltre devono essere utilizzati dispositivi e tipologie di collegamento, che evitino la memorizzazione delle informazioni riservate e trattate;
- L'accesso avviene tramite server dedicato, con divieto di salvataggio di informazioni sui dispositivi remoti utilizzati;
- Prima dell'accesso da remoto l'Utente deve assicurarsi che nelle vicinanze non siano presenti estranei all'attività lavorativa, ivi compresi i propri familiari.

Il controllo circa le corrette modalità di collegamento alla rete VPN avviene con cadenza annuale all'interno della relazione redatta dagli Amministratori di Sistema, in cui viene valutato il rischio relativo alla connessione da remoto degli utenti al sistema informativo aziendale. Le verifiche effettuate non saranno mai nominative.

15. Sistemi di controlli graduali

15.1 In caso di anomalie, il personale autorizzato della funzione ICT effettuerà controlli rigorosamente anonimi che si concluderanno con un avviso generalizzato diretto ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. I controlli non saranno in nessun caso nominativi.

15.2 Non verranno in nessun caso compiuti controlli prolungati, costanti o indiscriminati.

16. Osservanza delle disposizioni previste

16.1 Ciascun dipendente/collaboratore è tenuto al rispetto delle disposizioni previste nel presente Regolamento, delle istruzioni impartite dal Titolare del trattamento dati e della normativa vigente in materia di privacy.

16.2 Il mancato rispetto o la violazione delle regole previste sarà sanzionato con provvedimenti disciplinari come previsto nel vigente Contratto Collettivo applicato, nonché con tutte le azioni civili e penali consentite.[6]

17. Aggiornamento e revisione

17.1 Ciascun dipendente e/o collaboratore può proporre, quando ritenuto necessario, integrazioni motivate al presente Regolamento. Le proposte verranno esaminate dalla Direzione Generale e dal Servizio ICT.

17.2 Il presente Regolamento è soggetto a revisione con frequenza annuale.

18. Validità del regolamento e pubblicità

18.1 Il regolamento interno è valido a decorrere da 01/03/2019 Con l'entrata in vigore del presente regolamento interno tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.

18.2 Copia del regolamento, oltre ad essere affisso nella bacheca aziendale, verrà consegnato a ciascuna persona autorizzata[7] ed è disponibile sulla rete intranet aziendale.

Sansepolcro, 1 marzo 2019

COMETI SRL
Il Presidente
Massimo Castellani

[6] Si rammenta che il potere disciplinare non può comunque essere esercitato nei confronti dei collaboratori coordinati e continuativi, dei collaboratori a progetto e dei tirocinanti, mentre nei confronti dei lavoratori somministrati (ex interinali) va esercitato per il tramite dell'agenzia di somministrazione.
Con riferimento ai collaboratori, qualora questi per l'espletamento del loro incarico si servissero degli strumenti aziendali considerati dal Regolamento, si propone di prevedere nell'ambito del contratto a progetto l'obbligo per il collaboratore di rispettare il Regolamento in questione, con diritto della Committente, nei casi di violazione di particolare gravità, di risolvere il contratto stesso.

[7] La consegna di una copia a ciascun collaboratore è una scelta facoltativa del datore di lavoro: in caso di consegna a mano, la premessa del presente regolamento può anche essere riportata in un'eventuale lettera di accompagnamento.
Si ricorda infatti che ai sensi dell'art. 7 Legge n. 300/1970 l'unico obbligo a carico del datore di lavoro, **ai fini dell'esercizio del potere disciplinare**, è quello di dare adeguata pubblicità delle norme mediante l'affissione in luogo accessibile a tutti: per poter agire disciplinarmente nei confronti del **dipendente**, il regolamento dovrà pertanto essere affisso in luogo accessibile a tutti.
Si rammenta che il potere disciplinare non può comunque essere esercitato nei confronti dei collaboratori coordinati e continuativi, dei collaboratori a progetto e dei tirocinanti, mentre nei confronti dei lavoratori somministrati (ex interinali) va esercitato per il tramite dell'agenzia di somministrazione.