Regolamento per l'utilizzo della strumentazione informatica e della rete Internet

Rif. Regolamento UE 2016/679 (GDPR)

Titolare del Trattamento	Diocesi di Sabina – Poggio Mirteto (RI)
Indirizzo sede legale	Piazza Mario Dottori, 14 – 02047 Poggio Mirteto (RI)
Codice Fiscale	91000810571
PEC	diocesi@diocesisabina.it
Responsabile	S.E. Mons. Ernesto MANDARA
DPO	Giuliano PALOTTO

Edizione	Revisione	Data	Descrizione	il Titolare	il DPO
1	0	04/03/2024	Prima emissione	*approvato*	*verificato*

Documento di nr 12 pagine compresa la presente realizzato su format della

TITOLO I – PRINCIPI

Art. 1 – Introduzione, Definizioni e Finalità

Il presente regolamento ha l'obiettivo di definire l'ambito di applicazione, le modalità e le norme sull'utilizzo della strumentazione da parte degli utenti assegnatari (dipendenti, collaboratori ecc.) al fine di tutelare i beni aziendali ed evitare condotte inconsapevoli o scorrette che potrebbero esporre il Titolare del trattamento a problematiche di sicurezza, di immagine e patrimoniali per eventuali danni cagionati anche a terzi.
L'insieme delle norme comportamentali da adottare è ispirato ai principi di diligenza, informazione, correttezza nell'ambito dei rapporti di lavoro ed è inoltre finalizzato a prevenire eventuali comportamenti illeciti dei dipendenti, pur nel rispetto dei diritti a essi attribuiti dall'ordinamento giuridico italiano e comunitario.
A tale proposito si rileva che gli eventuali controlli previsti escludono finalità di monitoraggio diretto e intenzionale dell'attività lavorativa e sono disposti sulla base della vigente normativa, con particolare riferimento al Regolamento (UE) 2016/679, alla legge n. 300/1970 (Statuto dei lavoratori) e ai provvedimenti emanati dall'Autorità Garante (in particolare Provvedimento del 1 marzo 2007).

Art. 2 – Ambito di applicazione

Il presente regolamento si applica a ogni utente assegnatario di beni e risorse informatiche aziendali ovvero utilizzatore di servizi e risorse informative del Titolare del trattamento.
Per utente pertanto si intende, a titolo esemplificativo e non esaustivo, ogni dipendente, collaboratore, consulente, fornitore o altro che in modo continuativo non occasionale operi all'interno della struttura aziendale, ovvero in nome e per conto del Titolare del trattamento, utilizzandone beni e servizi informatici.
Per Titolare del trattamento si intende, invece l'organizzazione e in generale il titolare dei beni e delle risorse informatiche ivi disciplinate, il quale opererà per mezzo dei soggetti che ne possiedono la rappresentanza.

Art. 3 – Titolarità dei beni e delle risorse informatiche

I beni e le risorse informatiche, i servizi ICT e le reti informative costituiscono beni aziendali rientranti nel patrimonio sociale e sono da considerarsi di esclusiva proprietà del Titolare del trattamento.
Ciò considerato, il loro utilizzo è consentito solo per finalità di adempimento delle mansioni lavorative affidate a ciascun utente in base al rapporto in essere, ovvero per gli scopi professionali afferenti l'attività svolta per il Titolare del trattamento, e comunque per l'esclusivo perseguimento degli obiettivi sociali.
A tal fine si precisa sin d'ora che qualsivoglia dato o informazione trattato per mezzo dei beni e delle risorse informatiche di proprietà del Titolare del trattamento sarà dallo stesso considerato come avente natura aziendale e non riservata.

Art. 4 – Responsabilità personale dell'utente

Ogni utente è personalmente responsabile dell'utilizzo dei beni e delle risorse informatiche a lui affidati dal Titolare del trattamento nonché dei relativi dati trattati per finalità aziendali.
A tal fine ogni utente, nel rispetto dei principi di diligenza sottesi al rapporto instaurato con l Titolare del trattamento e per quanto di propria competenza, è tenuto a tutelare il patrimonio aziendale da utilizzi impropri o non autorizzati, danni o abusi anche derivanti da negligenza, imprudenza o imperizia. L'obiettivo è e rimane sempre quello di preservare l'integrità e la riservatezza dei beni, delle informazioni e delle risorse aziendali.
Ogni utente è tenuto a operare a tutela della sicurezza informatica aziendale, in relazione al proprio ruolo e alle mansioni in concreto svolte, riportando al proprio responsabile organizzativo diretto e senza ritardo eventuali rischi di cui è a conoscenza ovvero violazioni del presente regolamento. Sono vietati comportamenti che possano creare un qualsiasi danno, anche di immagine, al Titolare del trattamento.

Art. 5 – Controlli

Il Titolare del trattamento esclude la configurabilità di forme di controllo aziendali aventi come oggetto l'attività lavorativa dell'utente, in linea con quanto prescritto dall'ordinamento giuridico italiano (art. 4, Legge 300/70 – Statuto dei lavoratori).
Ciononostante non si esclude che si possano utilizzare sistemi informatici, impianti o apparecchiature dai quali derivi la possibilità di controllo a distanza dell'attività dei lavoratori per ragioni organizzative e produttive ovvero per esigenze dettate dalla sicurezza del lavoro. Per tali evenienze, eventualmente, sarà onere del Titolare del trattamento sottoporre tali forme di controllo all'accordo con le rappresentanze sindacali aziendali. In difetto di accordo e su istanza del Titolare del trattamento sarà l'ispettorato del lavoro a indicare le modalità per l'uso di tali impianti.
I controlli posti in essere saranno sempre tali da evitare ingiustificate interferenze con i diritti e le libertà fondamentali dei lavoratori e non saranno costanti, prolungati e indiscriminati.
Il Titolare del trattamento, riservandosi il diritto di procedere a tali controlli sull'effettivo adempimento della prestazione lavorativa nonché sull'utilizzo da parte degli utenti dei beni e dei servizi informatici aziendali (artt. 2086, 2087 e 2104 cod. civ.) agirà in base al principio della gradualità. In attuazione di tale principio:

- i controlli saranno effettuati inizialmente solo su dati aggregati riferiti all'intera struttura ovvero a singole aree lavorative;
- nel caso in cui si dovessero riscontrare violazioni del presente regolamento, indizi di commissione di gravi abusi o illeciti o attività contrarie ai doveri di fedeltà e diligenza, verrà 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 alle istruzioni ivi impartite;
- in caso siano rilevate ulteriori violazioni, si potrà procedere con verifiche più specifiche e puntuali, anche su base individuale.

Il Titolare del trattamento 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.

TITOLO II — MISURE ORGANIZZATIVE

Art. 6 – Amministratori di sistema

Il Titolare del trattamento conferisce all'amministratore di sistema il compito di sovrintendere ai beni e alle risorse informatiche aziendali. È compito dell'amministratore di sistema:

- gestire l'hardware e il software di tutta la strumentazione informatica di appartenenza dell'ente;
- gestire la creazione, l'attivazione, la disattivazione, e tutte le relative attività amministrative degli account di rete e dei relativi privilegi di accesso alle risorse, previamente assegnati agli utenti;
- monitorare il corretto utilizzo delle risorse di rete, dei computer e degli applicativi affidati agli utenti, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati;
- creare, modificare, rimuovere o utilizzare qualsiasi account o privilegio purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati;
- rimuovere software e/o componenti hardware dalle risorse informatiche assegnate agli utenti, purché attività rientranti nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati;
- provvedere alla sicurezza informatica dei sistemi informativi aziendali;
- utilizzare le credenziali di accesso di amministratore del sistema per accedere, anche da remoto, ai dati o alle applicazioni presenti su una risorsa informatica assegnata a un utente in caso di prolungata assenza, non rintracciabilità o impedimento dello stesso.

Tale ultima attività, tuttavia, deve essere disposta per mezzo di un soggetto che rivesta quantomeno la posizione di soggetto autorizzato al trattamento dei dati personali (incaricato) all'interno del Titolare del trattamento e deve essere limitata altresì al tempo strettamente necessario al compimento delle attività indifferibili per cui è stato richiesto.
Deve essere redatto un elenco completo degli amministratori di sistema, contenente tutti i dati rilevanti, aggiornato con cadenza annuale ovvero ogni volta che si rilevino modifiche.

Art. 7 – Assegnazione degli account e gestione delle password

Creazione e Gestione degli Account

Un account utente consente l'autenticazione dell'utilizzatore e di conseguenza ne disciplina l'accesso alle risorse informatiche aziendali per singola postazione lavorativa.
Gli account utenti vengono creati dagli amministratori di sistema e sono personali, cioè associati univocamente alla persona assegnataria. Ogni utente è responsabile dell'utilizzo del proprio account utente.
L'accesso al proprio account avviene tramite l'utilizzo delle "credenziali di autenticazione", solitamente username e password, comunicate all'utente dall'amministratore di sistema che le genera con modalità tali da garantirne la segretezza.
Le credenziali di autenticazione costituiscono dati aziendali da mantenere strettamente riservati e non è consentito comunicarne gli estremi a terzi, anche a soggetti in posizione apicale all'interno dell'ente.
Se l'utente ha il sospetto che le proprie credenziali di autenticazione siano state identificate da qualcuno, o il sospetto di un utilizzo non autorizzato del proprio account e delle risorse a questo associate, è tenuto a modificare immediatamente la password e a segnalare la violazione all'amministratore del sistema.
In caso di assenza improvvisa o prolungata del lavoratore e per improrogabili necessità legate all'attività lavorativa, per esigenze produttive aziendali o per la sicurezza e operatività delle risorse informatiche, il Titolare del trattamento si riserva la facoltà di accedere a qualsiasi dotazione o apparato assegnato in uso all'utente per mezzo dell'intervento dell'amministratore di sistema.
I beni e la strumentazione informatica oggetto del presente regolamento rimangono di esclusivo dominio del Titolare del trattamento, che in base ai rapporti instaurati con gli utenti ne disciplina l'assegnazione.

Gestione e Utilizzo delle Password

A seguito della prima comunicazione delle credenziali di autenticazione da parte dell'amministratore di sistema, l'utente ha il compito di modificare al primo utilizzo la propria password procedendo allo stesso modo ogni 6 mesi e, nel caso di trattamento di categorie particolari di dati personali (art. 9 GDPR) o relativi a condanne penali o reati (art. 10 GDPR), almeno ogni 3 mesi.
Si consiglia all'utente, nel definire il valore della password, di rispettare le seguenti regole:

- la password deve contenere almeno 8 caratteri alfanumerici e comprendere un carattere maiuscolo, un carattere minuscolo, un numero e un carattere speciale (es. @#$£$%...);
- evitare di includere parti del nome, cognome o comunque elementi riconducibili all'utilizzatore;
- evitare l'utilizzo di password comuni o prevedibili;
- proteggere con la massima cura la riservatezza della password ed utilizzarla entro i limiti di autorizzazione concessi;
- scrivere la password su post-it o altri supporti compromette in maniera pressoché totale le misure di sicurezza previste, pertanto costituisce violazione del presente regolamento e comporta l'applicazione di sanzioni.

Cessazione Degli Account

In caso di interruzione del rapporto di lavoro con l'utente, le credenziali di autenticazione verranno disabilitate entro un periodo massimo di 30 (trenta) giorni da quella data; entro 90 (novanta) giorni, invece, si disporrà la definitiva e totale cancellazione dell'account utente.

Art. 8 – Postazioni di lavoro

Per postazione di lavoro si intende il complesso unitario di personal computer (di seguito pc), notebook, tablet, smartphone, accessori, periferiche e ogni altro dispositivo (device) concesso in utilizzo all'utente. L'assegnatario di tali beni e strumenti informatici aziendali ha il compito di farne un uso compatibile con i principi di diligenza sanciti nel codice civile.
Al fine di disciplinare un corretto utilizzo di tali beni l'ente ha adottato le seguenti regole tecniche:

- ogni pc, notebook (accessori e periferiche incluse), tablet, smartphone o altro dispositivo (device), sia esso acquistato, noleggiato o affidato in locazione, rimane di esclusiva proprietà dell'ente ed è concesso all'utente per lo svolgimento delle proprie mansioni lavorative e comunque per finalità strettamente attinenti l'attività svolta;
- è dovere di ogni utente usare i computer e gli altri dispositivi a lui affidati responsabilmente e professionalmente;
- il pc e gli altri dispositivi di cui sopra devono essere utilizzati con hardware e software autorizzati dall'ente. Per utilizzare software o applicativi non presenti nella dotazione standard fornita è necessario presentare espressa richiesta scritta al proprio responsabile di riferimento, il quale ne valuterà i requisiti tecnici, l'aderenza alle policy interne e al ruolo ricoperto in azienda;
- 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 di sistema o al proprio responsabile di riferimento eventuali guasti e problematiche tecniche rilevati o il cattivo funzionamento delle apparecchiature;
- è fatto divieto di cedere in uso, anche temporaneo, le attrezzature e i beni informatici aziendali a soggetti terzi;
- l'ente si riserva la facoltà di rimuovere d'ufficio e senza alcun preavviso qualsiasi elemento hardware o software la cui installazione non sia stata appositamente e preventivamente prevista o autorizzata;
- gli apparecchi di proprietà personale dell'utente quali computer portatili, telefoni cellulari, smartphone, agende palmari, hard disk esterni, penne USB, lettori musicali o di altro tipo, fotocamere digitali e qualsiasi altro dispositivo non potranno essere collegati ai computer o alle reti informatiche aziendali salvo preventiva autorizzazione scritta del Titolare del trattamento.

TITOLO III – CRITERI DI UTILIZZO DEGLI STRUMENTI INFORMATICI

Art. 9 – Dispositivi (devices): Desktop, Laptop, Tablet, Smartphone, etc.

Per l'espletamento delle proprie mansioni gli utenti utilizzano dispositivi (devices) di proprietà del Titolare del trattamento e sono tenuti al rispetto delle seguenti regole:

- non è consentito modificare la configurazione hardware e software del proprio dispositivo (device), se non previa esplicita autorizzazione del Titolare del trattamento che la esegue per mezzo dell'amministratore del sistema;
- non è consentito rimuovere, danneggiare o asportare componenti hardware;
- non è consentito installare autonomamente programmi informatici, applicativi e ogni altro software non autorizzato espressamente dal Titolare del trattamento;
- è onere dell'utente, in relazione alle sue competenze lavorative, eseguire richieste di aggiornamento sulla propria postazione di lavoro derivanti da software antivirus nonché sospendere ogni attività in caso di minacce virus o altri malfunzionamenti, segnalando prontamente l'accaduto all'amministratore del sistema;

- è onere dell'utente spegnere il proprio PC al termine del lavoro. Per quanto concerne la gestione dei computer e degli altri dispositivi portatili, l'utente ha l'obbligo di custodirli con diligenza e in luogo protetto durante gli spostamenti, rimuovendo gli eventuali files elaborati prima della loro riconsegna;
- non è consentito all'utente caricare o inserire all'interno del computer o di altri dispositivi portatili qualsiasi dato personale non attinente con l'attività lavorativa svolta.

In ogni caso, al fine di evitare o almeno ridurre al minimo la possibile circolazione di dati personali sul medesimo apparecchio, gli utenti devono cancellare tutti quelli eventualmente presenti prima di consegnare il dispositivo agli uffici competenti per la restituzione o la riparazione.

Art. 10 – Software

Premesso che l'installazione di software privi di regolare licenza non è consentita in nessun caso, gli utenti dovranno ottenere espressa autorizzazione del Titolare del trattamento per installare o comunque utilizzare qualsiasi programma o software dotato di licenza non proprietaria, ad esempio freeware o shareware.
Il personale deve prestare attenzione ad alcuni aspetti fondamentali che ciascun utente è tenuto a osservare per un corretto utilizzo del software in azienda:

- le licenze d'uso del software sono acquistate da vari fornitori esterni. L'utente è pertanto soggetto a limitazioni nell'utilizzo di tali programmi e della relativa documentazione e non ha il diritto di riprodurlo in deroga a tali diritti. Tutti gli utenti sono quindi tenuti a utilizzare il software entro i limiti specificati nei rispettivi contratti di licenza;
- non è consentito eseguire il download o l'upload di software non autorizzato;
- considerato quanto disposto dalle normative a tutela della proprietà intellettuale e del diritto d'autore, le persone coinvolte nella riproduzione illegale del software sono responsabili sia civilmente che penalmente e quindi soggette alle sanzioni previste dalla legge che comprendono il risarcimento del danno, il pagamento di multe e, nei casi gravi, la reclusione;
- la duplicazione illegale del software non è giustificabile e non è tollerata, costituisce violazione del presente regolamento ed espone alle sanzioni disciplinari previste.

ART 11 – Dispositivi mobili di connessione (internet key)

Agli assegnatari di computer o dispositivi portatili può essere concessa in dotazione anche una chiavetta per la connessione alla rete aziendale per consentire lo svolgimento delle mansioni lavorative anche da remoto.
I suddetti dispositivi mobili di connessione devono essere utilizzati esclusivamente sui computer forniti in dotazione dal Titolare del trattamento e non è consentito concederne l'utilizzo a soggetti terzi né utilizzarli su altri computer sia personali che di terzi.
Le specifiche relative ai limiti entro cui l'utente potrà utilizzare il servizio offerto tramite la chiavetta sono riportate nella scheda tecnica consegnata all'utente unitamente al dispositivo.
L'utente dovrà attenersi ai suddetti limiti; in caso contrario potrà essere richiesto il rimborso dei costi sostenuti per il loro eventuale superamento.

Art. 12 – Dispositivi di memoria portatili

Per dispositivi di memoria portatili si intendono tutti quei dispositivi che consentono di copiare o archiviare dati, files, o documenti esternamente al computer: cd-rom, dvd, pen-drive USB, riproduttori musicali mp3, fotocamere digitali, dischi rigidi esterni, ecc.
L'utilizzo di tali supporti risponde alle direttive di seguito riportate:

- non è consentito utilizzare supporti rimovibili personali, se non preventivamente autorizzati per iscritto dall'ente (per le modalità operative fare riferimento a quanto riportato all'art. 19 – Comunicazioni);
- è onere dell'utente custodire i supporti contenenti categorie particolari di dati (art. 9 GDPR) o dati relativi a condanne penali e a reati (art. 10 GDPR) in armadi chiusi a chiave, onde evitare che il loro contenuto possa essere trafugato o alterato o distrutto;

- se autorizzati in base alle procedure previste, una volta connessi all'infrastruttura informatica dell'ente, i dispositivi saranno soggetti (ove ciò sia compatibile) al presente regolamento.

Art. 13 – Stampanti, fotocopiatrici e fax

L'utilizzo di tali strumenti deve avvenire sempre per scopi professionali. Non è consentito un utilizzo per fini diversi o privati, salvo una specifica autorizzazione da parte del Titolare del trattamento.
Quando si inviano documenti contenenti dati personali o informazioni riservate su una stampante condivisa è richiesta una particolare attenzione; ciò al fine di evitare che persone non autorizzate possano venire a conoscenza del contenuto della stampa. Bisogna evitare quindi di lasciare le stampe incustodite e ritirare immediatamente le copie appena stampate.
L'utilizzo di fax per l'invio di documenti che hanno natura strettamente confidenziale è generalmente da evitare. In caso ciò sia necessario si deve preventivamente avvisare il destinatario in modo da ridurre il rischio che persone non autorizzate possano venire a conoscenza del contenuto della comunicazione e successivamente chiedere la conferma telefonica di avvenuta ricezione.
Gli strumenti dotati di memoria, connessi o meno in rete, sono gestiti dall'Amministratore di Sistema che provvede alla cancellazione periodica del loro contenuto e a tutte le operazioni ritenute necessarie per garantirne la sicurezza.

Art. 14 – Strumenti di fonia mobile o di connettività in mobilità

A seconda del ruolo o della funzione del singolo utente, il Titolare del trattamento potrebbe rendere disponibili impianti di telefonia fissa e mobile e inoltre dispositivi quali smartphone e tablet che consentono di usufruire sia della navigazione in internet tramite rete dati che del servizio di telefonia tramite rete mobile.
Le specifiche relative ai limiti entro cui l'utente potrà utilizzare tali strumenti sono riportate nella scheda tecnica consegnata unitamente al dispositivo. L'utente dovrà attenersi ai suddetti limiti e in caso contrario potrà essere richiesto il rimborso dei costi sostenuti per il loro superamento.
Come per qualsiasi altra dotazione aziendale, il dispositivo mobile rappresenta un bene aziendale concesso in uso per scopi esclusivamente lavorativi. È tuttavia permesso un utilizzo personale sporadico e moderato dei telefoni aziendali utilizzando la "*diligenza del buon padre di famiglia*" prevista dalla normativa e comunque tale da non ledere il rapporto fiduciario instaurato con il proprio datore di lavoro.
Al fine di controllo del corretto utilizzo dei servizi di fonia aziendale l'ente può esercitare i diritti di cui al ex art. 124 D.Lgs. 196/2003 (fatturazione dettagliata) richiedendo ai provider di telefonia i dettagli necessari agli accertamenti sull'uso e relativo costo del traffico effettuato nel tempo.
I controlli saranno eseguiti secondo criteri e modalità descritte all'art. 5 del presente regolamento. Qualora dall'esame del traffico di una singola utenza si rilevi uno scostamento significativo rispetto alla media del consumo sarà richiesto il tabulato analitico delle chiamate effettuate dalla SIM in incarico all'utente per il periodo interessato.
L'utilizzo dei dispositivi mobili risponde alle seguenti regole:

- ciascun 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, per esempio codice PIN del dispositivo, che ne impedisca l'utilizzo da parte di altri soggetti. A tal fine si precisa che il codice PIN:
  - dovrà essere composto da quattro o cinque cifre numeriche, altri codici di accesso dovranno garantire analoga protezione;
  - o altri codici di accesso dovranno essere modificati dall'assegnatario con cadenza al massimo semestrale;
- 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 al Titolare del trattamento.

- in caso di furto, danneggiamento o smarrimento del dispositivo mobile l'utente assegnatario dovrà darne immediato avviso al Titolare del trattamento; se tali eventi siano riconducibili a un comportamento negligente o imprudente dell'utente stesso 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'ente si riserva la facoltà di attuare la procedura di cancellazione da remoto di tutti i dati sul dispositivo, rendendo il dispositivo stesso inutilizzabile e i dati in esso contenuti del tutto irrecuperabili;
- non è consentito all'utente caricare o inserire all'interno del dispositivo o SIM qualsiasi dato personale non attinente con l'attività lavorativa svolta. In ogni caso, al fine di evitare o almeno ridurre la circolazione di dati personali sull'apparecchio, è obbligatorio cancellare tutti i dati eventualmente presenti prima di consegnare il dispositivo agli uffici competenti per la restituzione o la riparazione;
- non è consentito all'utente effettuare riprese, fotografie, registrazioni di suoni con qualsiasi tipologia di apparecchiatura elettronica adatta a tali scopi a meno che non siano strettamente connesse con il proprio compito lavorativo e siano preventivamente autorizzate dall'ente;
- l'installazione di applicazioni, gratuite o a pagamento, su smartphone e tablet deve essere espressamente autorizzata, rimanendo in caso contrario a carico dell'utente le responsabilità derivanti dall'installazione non autorizzata che costituisce violazione del presente regolamento;
- salvo diversi specifici accordi derivanti da esigenze di servizio, al momento della consegna di tablet o smartphone l'utente è tenuto a verificare la disattivazione del sistema di geolocalizzazione potenzialmente attivabile sugli smartphone e tablet, consapevole che in caso contrario l'ente potrebbe venire a conoscenza, seppur incidentalmente, dei dati relativi alla posizione del dispositivo stesso e del suo assegnatario.

TITOLO IV — GESTIONE DELLE COMUNICAZIONI TELEMATICHE

Art. 15 – Gestione utilizzo della rete internet

Ciascun utente potrà essere abilitato alla navigazione Internet e pertanto si richiamano tutti gli utenti a una particolare attenzione al suo utilizzo consapevole così come dei servizi collegati, in quanto ogni operazione posta in essere è associata all'"Indirizzo Internet Pubblico" assegnato al Titolare del trattamento.

La connessione a Internet, in quanto strumento a disposizione degli utenti per uso professionale, deve essere utilizzata in maniera appropriata, tenendo presente che ogni sito web può essere governato da leggi diverse da quelle vigenti in Italia; ciò deve essere tenuto in considerazione in modo da prendere ogni precauzione conseguente.

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

- l'utilizzo è consentito esclusivamente 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 espressamente autorizzati dall'ente;
- è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
- non sono permesse, se non per motivi professionali, la partecipazione a forum, l'utilizzo di chat-line o di bacheche elettroniche e le registrazioni in guest-book, anche utilizzando pseudonimi (o nicknames);
- non è consentita la navigazione in siti e la memorizzazione di documenti informatici di natura oltraggiosa, pornografica, pedopornografica o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale o politica;
- è consentito l'utilizzo di soluzioni di Instant Messenger o chat esclusivamente per scopi professionali e attraverso strumenti e software messi a disposizione dall'ente;

- non è consentito l'utilizzo di sistemi di social network sul luogo di lavoro o durante l'orario lavorativo, fatto salvo le attività istituzionali;
- non è consentito lo scambio o la condivisione di materiale audiovisivo, cinematografico, fotografico, informatico o altro anche se non protetto da copyright utilizzando sistemi Peer-to-Peer, a qualsiasi titolo e anche se non a scopo di lucro, fatto salvo le attività istituzionali;
- non è consentito sfruttare i marchi registrati, i segni distintivi e ogni altro bene immateriale di proprietà dell'ente in una qualsiasi pagina web o pubblicandoli su Internet, a meno che tale azione non sia stata preventivamente ed espressamente approvata;
- è altresì proibito rigorosamente qualsiasi uso del Web che non trasmetta un'immagine positiva o che possa essere in qualunque modo essere nocivo all'immagine del Titolare del trattamento.

Per mezzo dell'Amministratore di Sistema e al fine di facilitare il rispetto delle predette regole il Titolare del trattamento si riserva la facoltà di configurare specifici filtri che inibiscono l'accesso ai contenuti non consentiti, con esclusione dei siti istituzionali, e che prevengono operazioni non correlate all'attività lavorativa: a titolo esemplificativo e non esaustivo upload, restrizione nella navigazione, download di file o software.

Art. 16 – Gestione e utilizzo della posta elettronica aziendale

Principi Guida

Per ciascun utente titolare di un account, il Titolare del trattamento provvede ad assegnare una casella di posta elettronica individuale.

I servizi di posta elettronica devono essere utilizzati a scopo professionale: l'account e-mail è uno strumento di proprietà del Titolare del trattamento ed è conferito in uso esclusivo per lo svolgimento delle mansioni lavorative affidate.

Ad uno stesso utente possono essere assegnate più caselle di posta elettronica, che possono anche essere condivise con altri utenti dello stesso gruppo/ufficio/dipartimento. Tali caselle di posta elettronica devono essere utilizzate esclusivamente per la ricezione dei messaggi mentre per le risposte o gli invii deve sempre essere utilizzata la casella personale.

Il Titolare del trattamento valuterà caso per caso, previa richiesta dell'utente, la possibilità di attribuire allo stesso un diverso indirizzo destinato ad uso privato.

Attraverso le caselle e-mail aziendali gli utenti rappresentano pubblicamente il Titolare del trattamento e per questo motivo viene richiesto di utilizzare tale sistema in modo lecito, professionale e comunque tale da riflettere positivamente l'immagine aziendale.

Gli utenti sono responsabili del corretto utilizzo delle caselle di posta elettronica aziendale conformemente alle presenti regole. Gli stessi devono:

- conservare la password nella massima riservatezza e con la massima diligenza;
- mantenere la casella in ordine, cancellando documenti inutili e allegati ingombranti;
- utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario;
- prestare attenzione alla dimensione degli allegati per la trasmissione di file all'interno della struttura nonché alla posta ricevuta. Gli allegati provenienti da mittenti sconosciuti non devono essere aperti in quanto possono essere utilizzati come veicolo per introdurre programmi dannosi (agenti di alterazione, ad esempio virus);
- inviare preferibilmente files in formato PDF;
- accertarsi dell'identità del mittente e controllare a mezzo di software antivirus i *files attachment* di posta elettronica prima del loro utilizzo;
- rispondere alle e-mail pervenute solo da emittenti conosciuti e cancellare preventivamente le altre;
- collegarsi a siti internet contenuti all'interno di messaggi solo per motivate ragioni e quando vi sia comprovata la sicurezza sul contenuto degli stessi.

Inoltre, non è consentito agli utenti:

- diffondere il proprio indirizzo e-mail aziendale attraverso la rete internet;
- utilizzare la casella di posta elettronica aziendale per inviare, ricevere o scaricare allegati contenenti video, brani musicali, ecc., salvo che questo non sia funzionale all'attività prestata in favore dell'ente, per esempio presentazioni o materiali video aziendali.

Salvo l'utilizzo di appositi strumenti di cifratura i sistemi di posta elettronica non possono garantire la riservatezza delle informazioni trasmesse. Pertanto si richiede agli utenti di valutare con attenzione l'invio di informazioni classificabili quali "riservate" o aventi comunque carattere "strettamente confidenziale".
Occorre infine che i messaggi di posta elettronica contengano un avvertimento ai destinatari, nel quale sia dichiarata l'eventuale natura non personale dei messaggi stessi e precisato che le risposte potranno essere conosciute da altri nell'organizzazione di appartenenza del mittente.
Nei casi in cui l'ente si doti di posta elettronica certificata si applicheranno, ove compatibili, le presenti disposizioni.

Accesso alla casella di posta elettronica del lavoratore assente

Saranno messe a disposizione di ciascun utente, con modalità di agevole esecuzione, apposite funzionalità del sistema di posta elettronica che in caso di assenze programmate consentano di inviare automaticamente messaggi di risposta contenenti le coordinate di altro soggetto cui trasmettere le comunicazioni e-mail di contenuto lavorativo o altre utili modalità di contatto in caso di assenza del lavoratore.
In caso di assenze non programmate, ad esempio per malattia, qualora il lavoratore non possa attivare la procedura descritta anche avvalendosi di servizi webmail da remoto e perdurando l'assenza oltre il limite temporale di 7 (sette) giorni l'ente disporrà, lecitamente e mediante personale appositamente incaricato (l'Amministratore di Sistema oppure un suo incaricato), l'attivazione di un analogo accorgimento (risposta automatica o re-indirizzamento), avvertendo l'assente.
Nel caso in cui l'ente necessiti di conoscere il contenuto dei messaggi di posta elettronica dell'utente resosi assente per cause improvvise o per improrogabili necessità legate all'attività lavorativa, si procederà come segue:

- la verifica del contenuto dei messaggi sarà effettuata per il tramite di idoneo "fiduciario", da intendersi quale lavoratore previamente nominato e/o incaricato per iscritto dall'utente assente;
- di tale attività sarà redatto apposito verbale e informato l'utente interessato alla prima occasione utile.

Cessazione dell'indirizzo di Posta Elettronica Aziendale

In caso di interruzione del rapporto di lavoro con l'utente, l'indirizzo di posta elettronica verrà disabilitato entro un periodo massimo di 30 (trenta) giorni da quella data ed entro 90 (novanta) giorni si disporrà la definitiva e totale cancellazione dello stesso. In ogni caso, il Titolare del trattamento si riserva il diritto di conservare i messaggi di posta elettronica ritenuti rilevanti per le proprie attività.

TITOLO V — VIOLAZIONI, COMUNICAZIONI, APPROVAZIONE

Art. 17 – Violazioni

La violazione di quanto previsto dal presente regolamento, rilevante anche ai sensi degli artt. 2104 e 2105 cod.civ., potrà comportare applicazioni disciplinari in base a quanto previsto dall'art. 7 (contestazione dell'addebito) della Legge 20 maggio 1970 n.300 (Statuto dei Lavoratori).
Nel caso venga commesso un reato o la cui commissione sia ritenuta probabile o solo sospettata il Titolare del trattamento avrà cura di informare senza ritardo, e senza necessità di preventive contestazioni o addebiti formali, le autorità competenti dell'utilizzo illecito o non conforme dei beni e degli strumenti informatici aziendali.
In caso di violazione accertata delle regole e degli obblighi esposti in questo regolamento da parte degli utenti l'ente si riserva la facoltà di sospendere, bloccare o limitare gli accessi di un account, quando appare ragionevolmente necessario per proteggere l'integrità, la sicurezza o la funzionalità dei propri beni e strumenti informatici e inoltre per impedire il reitero di tale violazione.

Art. 18 – Informativa agli utenti ex art. 13 Regolamento (UE) 2016/679

Il presente regolamento, nella parte in cui contiene le regole per l'utilizzo dei beni e degli strumenti informatici aziendali e relativamente al trattamento di dati personali svolti dall'ente finalizzato all'effettuazione di controlli leciti, così come definiti nell'art. 5, vale quale informativa ex art. 13 del Regolamento (UE) 2016/679.

Art. 19 – Comunicazioni

Contestualmente all'assegnazione di un account il presente regolamento è messo a disposizione degli utenti per la consultazione. La versione più aggiornata dello stesso è pubblicata sia in formato digitale che in formato cartaceo allo scopo di facilitarne la diffusione a tutti gli interessati.
Le richieste di autorizzazione o concessione previste dal presente regolamento possono essere inoltrate all'ente per mezzo di qualsiasi strumento che ne garantisca la tracciabilità, ad esempio tramite e-mail, a cui è riconosciuto il valore di forma scritta in modo del tutto analogo rispetto a quella cartacea.

Art. 20 – Approvazione del Regolamento

Il presente regolamento è stato approvato dal Legale Rappresentante del Titolare del trattamento e reso operativo il primo giorno lavorativo successivo.

Sommario