REGOLAMENTO
PER L'UTILIZZO DEI
SISTEMI INFORMATICI

Indice

Changelog

Versione	Data	Cambiamenti effettuati dall'ultima versione
1.00	17/08/2018	Prima versione
2.00	20/08/2019	Seconda versione aggiornata con testi segnalati dallo Studio Paci (incarico Maggioli)
2.10	05/09/2019	Terza versione aggiornata con testi segnalati dallo Studio Paci (incarico Maggioli)
2.11	02/10/2019	Correzioni minori sulle condizioni di accesso alle caselle di posta elettronica

Premessa

Il presente Regolamento intende fornire ai dipendenti e collaboratori, denominati anche incaricati o utenti, del Comune di San Michele al Tagliamento le indicazioni per una corretta e adeguata gestione delle informazioni personali, in particolare attraverso l'uso di sistemi, applicazioni e strumenti informatici dell'Ente .
Si specifica che tutti gli strumenti utilizzati dal lavoratore, intendendo con ciò i PC, notebook, risorse, e-mail ed altri strumenti con relativi software e applicativi (di seguito più semplicemente "Strumenti"), sono messi a disposizione dall'Ente per rendere la prestazione lavorativa. Gli Strumenti, nonché le relative reti dell'Ente a cui è possibile accedere tramite gli stessi, sono domicilio informatico del Comune di San Michele al Tagliamento.
I dati personali e le altre informazioni dell'Utente che sono registrati negli Strumenti o che si possono eventualmente raccogliere tramite il loro uso, sono utilizzati per finalità istituzionali, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente. Per tutela del patrimonio dell'Ente si intende altresì la sicurezza informatica e la tutela del sistema informatico dell'Ente. Tali informazioni sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, visto che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo 679/16 sulla protezione dei dati personali.
Viene, infine, precisato che non sono installati o configurati sui sistemi informatici in uso agli utenti apparati hardware o strumenti software aventi come scopo il controllo a distanza dell'attività dei lavoratori.

1 Oggetto e finalità

Il presente Regolamento è redatto:

- alla luce della Legge 20.5.1970, 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";
- in attuazione del Regolamento Europeo 679/16 sulla protezione dei dati personali (d'ora in avanti Reg. 679/16 o GDPR);
- ai sensi delle "Linee guida del Garante per posta elettronica e internet" in Gazzetta Ufficiale n. 58 del 10 marzo 2007;
- alla luce dell'articolo 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»*.

La finalità è quella di promuovere in tutto il personale dell'Ente una corretta "cultura informatica" affinché l'utilizzo degli Strumenti informatici e telematici forniti dall'Ente, quali la posta elettronica, internet e i personal computer con i relativi software, sia conforme alle finalità dell'Ente e nel pieno rispetto della legge. Si vuole fornire a tutto il personale le indicazioni necessarie con l'obiettivo principale di evitare il verificarsi di qualsiasi abuso o uso non conforme, muovendo dalla convinzione che la prevenzione dei problemi sia preferibile rispetto alla loro successiva correzione.

2 Principi generali e di riservatezza nelle comunicazioni

2.1 I principi che sono a fondamento del presente Regolamento sono gli stessi espressi nel GDPR, e, precisamente:

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 (art. 5 e 6 del Reg. 679/16);
b) **il principio di correttezza**, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori. Le tecnologie dell'informazione (in modo più marcato rispetto ad apparecchiature tradizionali) permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all'attività lavorativa. Ciò, all'insaputa o senza la piena consapevolezza dei lavoratori, considerate anche le potenziali applicazioni di regola non adeguatamente conosciute dagli interessati;
c) **i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime** (art.5 commi 1 e 2), osservando il principio di pertinenza e non eccedenza. Il datore di lavoro deve trattare i dati "nella misura meno invasiva possibile"; le attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere "mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza".

2.2 Anche informazioni di normale quotidianità lavorative o ritenute non riservate all'interno dell'interscambio tra incaricati, assumono diversa importanza, e quindi necessitano di una maggiore tutela, se comunicate all'esterno a

soggetti terzi. La salvaguardia delle informazioni e dei dati, oltre ad essere un requisito fondamentale per la sicurezza del *patrimonio informativo comunale*, è anche un espresso obbligo di legge nei confronti di qualsiasi soggetto definito "interessato".

2.3 Il dipendente si attiene pertanto alle seguenti regole di trattamento:

a) È vietato comunicare (di persona, per telefono o per via telematica) a soggetti sconosciuti o non specificatamente autorizzati i dati personali comuni, sensibili, giudiziari, sanitari o altri dati, elementi e informazioni dell'Ente, dei quali il dipendente / collaboratore viene a conoscenza nell'esercizio delle proprie funzioni e mansioni all'interno dell'Ente. È infatti indispensabile osservare ogni cautela nel trasferire all'esterno qualsiasi informazione, in maniera proporzionale al contenuto della stessa ed in base all'attendibilità dell'interlocutore ed al personale ambito lavorativo assegnato. In caso di dubbio, è necessario accertarsi che il soggetto cui devono essere comunicati i dati sia o meno autorizzato a riceverli, mediante richiesta preventiva al proprio Responsabile di area/funzione.
b) È vietata l'estrazione di originali e/o copie cartacee ed informatiche per uso personale di documenti, manuali, fascicoli, lettere, data base e quant'altro.
c) È vietato lasciare incustoditi documenti, lettere, fascicoli, appunti e quant'altro possa contenere dati personali e/o informazioni dell'Ente quando il dipendente/collaboratore si allontana dalla postazione di lavoro. È vietato lasciare sulla postazione di lavoro (scrivania, bancone ecc.) materiali che non siano inerenti la pratica che si sta trattando in quel momento. Ciò vale soprattutto nel caso di lavoratori con mansioni di front-office.
d) Per le riunioni e gli incontri con utenti, cittadini, clienti, fornitori, consulenti e collaboratori dell'Ente è necessario utilizzare le apposite sale dedicate.

3 Tutela del lavoratore

3.1 Alla luce dell'art. 4, comma 1, L.n. 300/1970, la regolamentazione della materia indicata nell'art. 1 del presente Regolamento, non è finalizzata all'esercizio di un controllo a distanza dei lavoratori da parte del datore di lavoro ma solo a permettere a quest'ultimo di utilizzare sistemi informativi per fare fronte ad esigenze produttive od organizzative e di sicurezza nel trattamento dei dati personali.

3.2 È garantito al singolo lavoratore il controllo sui propri dati personali secondo quanto previsto dagli articoli 15-16-17-18-20-21-78 del Reg. 679/16.

4 Campo di applicazione

4.1 Il presente regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o di livello, nonché a tutti i collaboratori dell'Ente a prescindere dal rapporto contrattuale con la stessa intrattenuto.

4.2 Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, *per "utente" deve intendersi ogni dipendente e collaboratore in possesso di specifiche credenziali di autenticazione*. Tale figura potrà anche venir indicata come "incaricato del trattamento".

5 Gestione, assegnazione e revoca delle credenziali di accesso ("password")

5.1 Le credenziali di autenticazione per l'accesso alle risorse informatiche vengono assegnate dal personale del Servizio CED, previa formale richiesta del Responsabile dell'ufficio/servizio nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente. Nel caso di collaboratori esterni la richiesta dovrà essere inoltrata direttamente dal Segretario Generale dell'Ente o dal Responsabile dell'Ufficio/Servizio con il quale il collaboratore si coordina nell'espletamento del proprio incarico. La richiesta di attivazione delle credenziali dovrà essere completa di generalità dell'utente ed elenco dei sistemi informativi per i quali deve essere abilitato l'accesso. Ogni successiva variazione delle abilitazioni di accesso ai sistemi informativi dovrà essere richiesta formalmente al Servizio CED dal Responsabile di riferimento.

5.2 Se si è in possesso di più credenziali di autenticazione, fare attenzione ad accedere ai dati unicamente con la credenziale relativa al trattamento in oggetto, rispettando l'ambito di competenza (i dati cui poter accedere) ed il profilo di autorizzazione (tipi di trattamento consentito) indicate nella propria Nomina ad Incaricato;

5.3 Le credenziali di autenticazioni consistono in un codice per l'identificazione dell'utente (altresì nominati Username, Nome Utente o User Id), assegnato dal Servizio CED, ed una relativa password. La password è personale e riservata e dovrà essere conservata e custodita dall'incaricato con la massima diligenza e *non divulgata* (*non è cedibile per nessuna ragione*), affinché nessun altro possa utilizzare le sue risorse o possa farlo a suo nome.

5.4 Ai fini della sicurezza informatica (visto che il più semplice metodo per l'accesso illecito ad un sistema consiste nell'indovinare la password dell'utente legittimo), la password deve essere di adeguata robustezza (ovvero una password "forte"): deve essere composta da almeno 8 caratteri, formata da lettere maiuscole, minuscole, numeri o simboli (è più sicuro che per tali caratteri da un quarto alla metà siano di natura numerica). Non deve contenere riferimenti agevolmente riconducibili all'utente (username, nomi o date relative alla persona o ad un famigliare).

5.5 È necessario procedere da parte dell'utente alla modifica della password ricevuta al primo accesso e, successivamente, almeno ogni sei mesi. Nel caso in cui l'utente svolga mansioni che, in astratto, possano comportare il trattamento di dati personali sensibili e/o giudiziari, è obbligatorio il cambio password almeno ogni tre mesi.

5.6 La password scelta non deve essere possibilmente presente nei dizionari (anche di altre lingue), né dovrà contenere il proprio Nome Utente, né preferibilmente contenere parole legate all'utente stesso come, ad esempio, il proprio nome o cognome, quello di parenti stretti (moglie/marito e figli), il nome degli animali di compagnia, della data di nascita, dei propri numeri di telefono, ecc.

5.7 È assolutamente vietato scrivere ed appuntare la propria password in maniera visibile (soprattutto vicino al computer), in modo da non renderla facilmente accessibile. Inoltre, quando si immette la password, non si deve consentire a nessuno di sbirciare quanto si sta digitando sulla tastiera.

5.8 Nel caso di cessazione del rapporto di lavoro con il dipendente/collaboratore, il Responsabile dell'Ufficio/Servizio di riferimento dovrà comunicare formalmente e preventivamente al Servizio CED la data effettiva a partire dalla quale le credenziali saranno disabilitate.

6 Utilizzo della rete del Comune di San Michele al Tagliamento

6.1 Per l'accesso alle risorse informatiche del Comune di San Michele al Tagliamento attraverso la rete locale, ciascun utente deve essere in possesso di credenziali di autenticazione secondo l'art. 5.

6.2 È proibito accedere alla rete e nei sistemi informativi utilizzando credenziali di altre persone.

6.3 L'accesso alla rete garantisce all'utente la disponibilità di condivisioni di rete (cartelle su server) nelle quali vanno inseriti e salvati i file di lavoro, organizzati per area/ufficio o per diversi criteri o per obiettivi specifici di lavoro. Ciascun utente poi dispone di un'area riservata e personale denominata "Documenti Personali" (all'interno dell'unità di rete "H"). Tutte le cartelle di rete, siano esse condivise o personali, possono ospitare esclusivamente contenuti professionali. Pertanto è vietato il salvataggio sui server dell'Ente, ovvero sugli Strumenti, di documenti non inerenti l'attività lavorativa, anche se per brevi periodi (a titolo esemplificativo documenti, fotografie, video, musica, pratiche personali, SMS, mail personali, film e quant'altro). Ogni materiale personale rilevato dall'Amministratore di Sistema o dal Servizio CED a seguito di interventi di sicurezza informatica ovvero di manutenzione/aggiornamento su server ed anche su Strumenti viene rimosso secondo le regole previste nel successivo punto 12 del presente Regolamento, ferma ogni ulteriore responsabilità civile, penale e disciplinare. Tutte le risorse di memorizzazione, diverse da quelle citate al punto precedente, non sono sottoposte al controllo regolare degli Amministratori di Sistema e non sono oggetto di backup periodici automatici. A titolo di esempio e non esaustivo si citano: il "disco C" o altri dischi locali dei singoli PC, gli eventuali dispositivi di memorizzazione locali o di disponibilità personale come Hard disk portatili o NAS ad uso esclusivo. Tutte queste aree di memorizzazione non devono ospitare dati di interesse dell'Ente, poiché non sono garantite la sicurezza e la protezione contro la eventuale perdita di dati. Pertanto la responsabilità dei salvataggi dei dati ivi contenuti è a carico del singolo utente.

6.4 Senza il consenso del Titolare, è vietato trasferire documenti elettronici dai sistemi informativi e Strumenti dell'Ente a dispositivi esterni (hard disk, chiavette USB, CD, DVD ed altri supporti removibili) personali o di terzi.

6.5 Senza il consenso del Servizio CED è vietato salvare documenti elettronici dell'Ente (ad esempio pervenuti via mail o salvati sul server o sullo Strumento in dotazione) su *repository esterne* (quali ad esempio Dropbox, GoogleDrive, OneDrive, ecc.) ovvero inviandoli a terzi via posta elettronica o con altri sistemi.

6.6 Con regolare periodicità (almeno una volta al mese), ciascun utente provvede 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.

6.7 Il Comune di San Michele al Tagliamento mette a disposizione a determinate tipologie di utenti la possibilità di accedere alle proprie risorse informatiche anche dall'esterno dei confini dell'Ente, mediante rete VPN (Virtual Private Network), un canale privato e criptato verso la rete interna. L'accesso mediante VPN viene concesso a professionisti, tecnici e fornitori che nell'ambito di un rapporto contrattuale con il Comune di San Michele al Tagliamento necessitino di accedere a determinate risorse informatiche. Viene concesso, altresì, a dipendenti e dirigenti del Comune di San Michele al Tagliamento che necessitino di svolgere compiti specifici, pur non essendo presenti in sede. Le richieste di abilitazione all'accesso mediante VPN dovranno seguire le prescrizioni del punto 5.

6.8 All'interno di alcune sedi del Comune di San Michele al Tagliamento è resa disponibile anche una rete senza fili, c.d. "Wi-Fi". Tali reti consentono l'accesso alle risorse dell'Ente e ad Internet per i dispositivi non connessi alla rete LAN mediante cavo. L'accesso mediante rete Wi-Fi viene concesso a professionisti, tecnici e fornitori che nell'ambito di un rapporto contrattuale con il Comune di San Michele al Tagliamento necessitino di accedere a determinate risorse informatiche. Viene concesso, altresì, a dipendenti e dirigenti del Comune di San Michele al Tagliamento che necessitino di svolgere compiti specifici che non possono essere svolti dalle postazioni fisse. L'impostazione della connessione Wi-Fi sarà effettuata da personale del Servizio CED.

6.9 Il Servizio CED si riserva la facoltà di negare o interrompere l'accesso alla rete mediante dispositivi non adeguatamente protetti e/o aggiornati, che possano costituire una concreta minaccia per la sicurezza informatica dell'Ente.

I log relativi all'uso del File System e della Intranet dell'Ente, nonché i file salvati o trattati su server o Strumenti, sono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso il Servizio CED dell'Ente, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente.
I controlli possono avvenire secondo le disposizioni previste al successivo punto 12 del presente Regolamento.

Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/16 "General Data Protection".

7 Utilizzo degli Strumenti elettronici (PC, notebook e altri strumenti con relativi software ed applicativi)

7.1 Il dipendente/collaboratore è consapevole che gli Strumenti elettronici (come ad es. il Personal Computer, fisso o portatile) ed i relativi programmi e/o applicazioni forniti sono strumenti di lavoro di proprietà del Comune di San Michele al Tagliamento e devono essere utilizzati esclusivamente per rendere la prestazione lavorativa (in relazione, ovviamente alle mansioni assegnate) e non per scopi personali, tanto meno per scopi illeciti.

7.2 Ognuno è responsabile dell'utilizzo delle dotazioni informatiche ricevute in assegnazione. Ogni utilizzo non inerente all'attività lavorativa è vietato in quanto può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Ciascun dipendente/collaboratore si deve quindi attenere alle seguenti regole di utilizzo degli Strumenti.

7.3 L'accesso agli Strumenti dell'Ente è protetto da password; per l'accesso devono essere utilizzati Username e password assegnate dal Servizio CED (cfr. 5). A tal proposito si rammenta che essi sono strettamente personali e l'utente è tenuto a conservarli nella massima segretezza.

7.4 Il Personal Computer, notebook, tablet ed ogni altro hardware deve essere custodito con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento e *segnalando tempestivamente al personale del Servizio CED ogni malfunzionamento e/o danneggiamento oppure un eventuale furto*.

7.5 Non è consentita l'attivazione della password d'accensione (BIOS), senza preventiva autorizzazione da parte dell'Amministratore di Sistema.

7.6 Non è consentito all'utente modificare le caratteristiche hardware e software impostate sugli Strumenti assegnati, salvo preventiva autorizzazione da parte del personale dell'Amministratore di Sistema.

7.7 L'utente è tenuto a scollegarsi dal sistema ("log out") oppure bloccarne l'accesso (anche utilizzando un programma "salvaschermo" o "screen saver", con ripristino sulla schermata di accesso e sblocco previa imputazione della propria password) ogni qualvolta sia costretto ad assentarsi per più di 5 minuti dal locale nel quale è ubicata la stazione di lavoro (PC) o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima (ovvero in mancanza di un collega che sorvegli tale stanza) o nel caso non riesca a chiudere a chiave la porta d'ingresso al locale. *Lasciare un PC 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*.

7.8 Le informazioni archiviate sul PC locale devono essere esclusivamente quelle necessarie all'attività lavorativa assegnata.

7.9 Costituisce buona regola la pulizia periodica degli archivi memorizzati sul proprio PC, con cancellazione dei file obsoleti o non più utili.

7.10 La gestione dei dati su PC è demandata all'utente utilizzatore che dovrà provvedere a memorizzare sulle condivisioni dell'Ente dati che possono essere utilizzati anche da altri utenti, evitando di mantenere l'esclusività su di essi. Non è consentita l'installazione di programmi diversi da quelli autorizzati dal Servizio CED.

7.11 Gli operatori del Servizio CED possono in qualunque momento procedere alla rimozione di ogni file o applicazione che riterranno essere pericolosi per la sicurezza del sistema (PC, rete locale e server dell'Ente), ovvero acquisiti o installati in violazione dei presenti articoli, nonché tutte le impostazioni eventualmente configurate che possano interferire con il corretto funzionamento dei servizi informatici dell'Ente.

7.12 È obbligatorio consentire l'installazione degli aggiornamenti di sistema (patch singole o cumulative) e del software antivirus che vengono proposti automaticamente, al primo momento disponibile, in modo tale da mantenere il PC sempre protetto.

7.13 Solo l'Amministratore di sistema ed i dipendenti del Servizio CED sono autorizzati ad installare nuovi programmi applicativi o aggiornare quelli esistenti;

7.14 È vietato utilizzare il PC per l'acquisizione, la duplicazione e/o la trasmissione illegale di opere protette da copyright ed inoltre non è consentito condividere file, cartelle, hard disk o porzioni di questi del proprio computer, per accedere a servizi su Internet non autorizzati di "peer to peer" al fine di scaricare materiale elettronico tutelato dalle normative sul diritto d'autore (software, file audio, film, etc.).

7.15 È vietato l'utilizzo di supporti di memoria (chiavette o HDD/SSD USB, CD, DVD o altri supporti di memoria rimovibili) per il salvataggio di dati trattati tramite gli Strumenti dell'Ente, salvo che il supporto utilizzato sia stato fornito dal Servizio CED. In tale caso, il supporto fornito può essere utilizzato esclusivamente per finalità lavorative.

7.16 È buona norma assicurarsi di non avviare accidentalmente il proprio PC fisso o portatile con una chiavetta USB inserita (oppure HDD/SSD USB, CD, DVD o altra memoria removibile). Infatti se tale supporto fosse infetto, il virus potrebbe trasferirsi nel sistema operativo del computer e di conseguenza espandersi in tutti file presenti nel disco locale e in quelli di rete accessibili.

7.17 In ogni caso i supporti rimovibili contenenti dati sensibili o giudiziari devono essere custoditi ed utilizzati in modo tale da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti: è necessario che vengano conservati in cassetti chiusi a chiave (durante il periodo di utilizzo) e formattati nel momento in cui cessa lo scopo per il quale i dati vi sono stati memorizzati. Infatti, una volta scomparsi i motivi per la conservazione di tali dati, i suddetti supporti non possono venire abbandonati, ma devono essere possibilmente cancellati in maniera completa oppure, se necessario o per impossibilità, perfino essere distrutti.

7.18 Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

7.19 È vietato inoltre scaricare file o contenuti da supporti magnetici e/o ottici, come quelli sopra menzionati, non aventi alcuna attinenza con la propria prestazione lavorativa.

7.20 È assolutamente vietato connettere al PC qualsiasi periferica non autorizzata preventivamente dall'Amministratore di Sistema.

7.21 È assolutamente vietato connettere alla rete locale qualsiasi dispositivo (PC esterni, router, switch, modem ed altri dispositivi di comunicazione/connessione) non autorizzato preventivamente dall'Amministratore di Sistema.

7.22 Non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici degli uffici dell'Ente;

7.23 Nel caso in cui l'utente dovesse notare comportamenti anomali del PC, l'utente stesso è tenuto a comunicarlo tempestivamente al Servizio CED.

I log relativi all'utilizzo di Strumenti, reperibili nella memoria degli Strumenti stessi ovvero sui server o sui router dell'Ente, nonché i file con essi trattati sono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso il Servizio CED dell'Ente, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente.
I controlli possono avvenire secondo le disposizioni previste al successivo punto 12 del presente Regolamento.
Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/16 "General Data Protection".

8 Utilizzo di Internet

Le regole di seguito specificate sono adottate anche ai sensi delle "Linee guida del Garante per posta elettronica e internet" pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007.
Ciascun dipendente /collaboratore si deve attenere alle seguenti regole di utilizzo della rete Internet e dei relativi servizi.

8.1 È ammessa solo la navigazione in siti considerati correlati con la prestazione lavorativa ed attinenti allo svolgimento delle sole mansioni assegnate. L'accesso è consentito tramite autenticazione (ovvero con le credenziali assegnate) dal proxy dell'Ente, con le sue policy di sicurezza debitamente implementate e aggiornate, ad es. i siti istituzionali, i siti degli Enti locali, di fornitori e partner dell'Ente.

8.2 È vietato compiere azioni che siano potenzialmente in grado di arrecare danno all'Ente, ad esempio, il download o l'upload di file audio e/o video, l'uso di servizi di rete con finalità ludiche o, comunque, estranee all'attività lavorativa.

8.3 È vietato a chiunque il download ed il successivo utilizzo di qualunque tipo di software gratuito (trial, freeware o shareware, nonché videogiochi) prelevato da siti Internet o allegato a riviste e libri, se non espressamente autorizzato dagli Amministratori di Sistema.

8.4 È vietato a chiunque il download da siti Internet e l'attivazione di applets di Java o di altri contenuti attivi, se non espressamente autorizzato dagli Amministratori di Sistema.

8.5 Non è consentito navigare in siti che accolgono contenuti contrari alle prescrizioni di Legge.

8.6 L'Ente si riserva di bloccare l'accesso a siti "a rischio" attraverso l'utilizzo di blacklist pubbliche in continuo aggiornamento e di predisporre filtri, basati su sistemi euristici di valutazione del livello di sicurezza dei siti web remoti, tali da prevenire operazioni potenzialmente pericolose o comportamenti impropri. In caso di blocco accidentale di siti di interesse dell'Ente, contattare il Servizio CED per uno sblocco selettivo.

8.7 Nel caso in cui, per ragioni di servizio, si necessiti di una navigazione libera dai filtri del suddetto proxy, è necessario richiedere lo sblocco mediante una mail indirizzata al Servizio CED, ed in copia al Segretario Generale, nella quale siano indicati chiaramente: motivo della richiesta, utente e postazione da cui effettuare la navigazione libera, intervallo di tempo richiesto per completare l'attività. L'utente, nello svolgimento delle proprie attività, deve comunque tenere presente in modo particolare i punti **Errore. L'origine riferimento non è stata trovata.** e 12.2 del presente regolamento. Al termine dell'attività gli addetti del Servizio CED ripristineranno i filtri nella situazione iniziale.

8.8 È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo i casi direttamente autorizzati dal Segretario Generale e dal Servizio CED, con il rispetto delle normali procedure di acquisto.

8.9 È assolutamente vietato l'utilizzo di abbonamenti privati per effettuare la connessione a Internet tranne in casi del tutto eccezionali e previa autorizzazione degli Amministratori di Sistema e del Segretario Generale previo parere tecnico degli stessi Amministratori.

8.10 È assolutamente vietata la partecipazione e registrazione a siti web e forum per motivi non professionali, nonché ai Social Network, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books, anche utilizzando pseudonimi (o nicknames).

8.11 Per motivi tecnici e di buon funzionamento del sistema informatico è buona norma, salvo comprovata necessità, non accedere a risorse web che impegnino in modo rilevante banda, come a titolo esemplificativo: filmati (tratti da YouTube, siti di informazione, siti di streaming ecc) o web radio, in quanto possono limitare e/o compromettere l'uso della rete agli altri utenti.

Si informa che l'Ente, per il tramite del Servizio CED, non controlla con sistemi automatici i dati di navigazione del singolo Utente. Si informa tuttavia che al fine di garantire il servizio Internet e la sicurezza dei sistemi informativi, nonché per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio del Comune di San Michele al Tagliamento, l'Ente registra per 180 giorni i dati di navigazione su Internet (file di log riferiti al traffico web) di tutti gli utenti, memorizzando nello specifico i dati correlati all'Identificativo di utente (facente parte delle credenziali di autenticazione), all'indirizzo (URL) della pagina web visitata (comunque appartenente ad un sito Internet approvato nell'ambito del profilo dello stesso utente), all'indirizzo IP statico o dinamico della postazione (connessa alla LAN comunale) ed alla data/ora di visita della pagina.
Solo in casi eccezionali e di comprovata urgenza rispetto alle finalità sopra descritte, l'Ente può trattare i dati di navigazione aggregandoli per un singolo nome utente. In tali casi i controlli avverranno nelle forme indicate al successivo punto 12 del presente Regolamento.
Le informazioni così raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/16 "General Data Protection".

9 Utilizzo della posta elettronica

Le regole di seguito specificate sono adottate anche ai sensi delle "Linee guida del Garante per posta elettronica e internet" pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007. Si sottolinea che anche il servizio di posta elettronica è uno strumento di lavoro e pertanto non ne è consentito l'utilizzo per motivi non attinenti allo svolgimento delle mansioni assegnate.
Ciascun dipendente/collaboratore si deve inoltre attenere alle seguenti regole di utilizzo dell'indirizzo di Posta elettronica.

9.1 Ad ogni utente viene fornito un account e-mail dell'Ente nominativo, generalmente coerente con il modello *nome.cognome@comunesanmichele.it*. L'utilizzo dell'e-mail "nominale" deve essere limitato alle attività ed ai procedimenti amministrativi interni o esterni all'Ente e per le comunicazioni interne, ed è vietato ogni utilizzo di tipo esclusivamente privato. L'utente a cui è assegnata una casella di posta elettronica nominale è responsabile del corretto utilizzo della stessa.

9.2 L'Ente può fornire al dipendente altresì delle *caselle di posta elettronica in condivisione*, associate a ciascun ufficio/servizio o gruppo di lavoro di appartenenza, il cui utilizzo è da preferire rispetto alle "e-mail nominali" qualora le comunicazioni siano di interesse collettivo: questo per evitare che degli utenti singoli mantengano l'esclusività su dati dell'Ente. Anche in questo caso, l'utente a cui è assegnata una o più caselle di posta elettronica di ufficio/servizio/gruppo di lavoro è responsabile del corretto utilizzo della stesse;

9.3 Non è consentito utilizzare web mail esterne, ovvero caselle di posta elettronica non appartenenti al dominio o ai domini comunali, salvo diversa ed esplicita autorizzazione del Segretario Generale;

9.4 L'iscrizione a dibattiti e forum on-line, a mailing-list o newsletter esterne con il proprio indirizzo dell'Ente personale è concessa esclusivamente per motivi professionali. Prima di iscriversi occorre verificare anticipatamente l'affidabilità del sito che offre il servizio.

9.5 Allo scopo di garantire sicurezza alla rete dell'Ente, evitare di aprire messaggi di posta in arrivo da mittenti di cui non si conosce l'identità o con contenuto sospetto o insolito (finti messaggi detti "bufale"), oppure contenenti nel testo del messaggio link a falsi indirizzi web (spesso riferiti a siti fraudolenti o infetti) o contenenti allegati di tipo *.exe, *.com, *.bat, *.sys, *.vbs, *.htm, *.scr, *.js e *.pif. È inoltre necessario porre molta attenzione alla credibilità del messaggio e del mittente per evitare casi di *phishing* o *frodi informatiche* (ad esempio possono ricevere false comunicazioni via e-mail aventi grafica, forma, autorevolezza e loghi ufficiali di enti noti, banche, intermediari finanziari, assicurazioni, ecc., chiedendo informazioni quali password, numeri di carta di credito, od altre informazioni riservate, attraverso moduli o link a pagine web debitamente camuffate). Anche in questi casi lo scopo dell'aggressore è spacciarsi per una persona o una entità giuridica apparentemente sicura (anche tramite espedienti psicologici e tecniche di "social engineering") per indurre l'utente destinatario a fidarsi e comunicargli conseguentemente delle informazioni riservate. In qualunque situazione di incertezza contattare gli Amministratori di Sistema o il Servizio CED per una valutazione dei singoli casi.

9.6 Non é consentito diffondere messaggi del tipo "catena di S. Antonio" o di tipologia simile anche se il contenuto sembra meritevole di attenzione; in particolare gli appelli di solidarietà, di guadagni facili ed i messaggi che informano dell'esistenza di nuovi virus (sono tutti inganni aventi spesso scopi molto simili a quelli dei virus, cioè utilizzare indebitamente le risorse informatiche). In generale è vietato l'invio di messaggi pubblicitari di prodotti di qualsiasi tipo.

9.7 Non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

9.8 Nel caso fosse necessario inviare allegati "pesanti" (fino a 10 MB) è opportuno ricorrere prima alla compressione dei file originali in un archivio di formato .zip o equivalenti. Nel caso di allegati particolarmente voluminosi è necessario rivolgersi al Servizio CED.

9.9 La posta elettronica diretta all'esterno della rete informatica comunale può essere intercettata da estranei, e dunque, non deve essere usata per inviare informazioni, dati o documenti di lavoro "strettamente riservati" senza alcun accorgimento (si veda il punto successivo);

9.10 Nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati personali o dati personali sensibili, è obbligatorio che questi allegati vengano preventivamente resi inintelligibili attraverso crittazione con apposito software (archiviazione e compressione con password). La password di crittazione deve essere comunicata al destinatario attraverso un canale diverso dalla mail (ad esempio per lettera o per telefono) e mai assieme ai dati criptati. Tutte le informazioni dell'Ente, i dati personali e/o sensibili di competenza dell'Ente possono essere inviati soltanto a destinatari - persone o Enti – qualificati e competenti.

9.11 *Non è consentito l'invio automatico di e-mail all'indirizzo e-mail privato* (attivando per esempio un "inoltro" automatico delle e-mail entranti), anche durante i periodi di assenza (es. ferie, malattia, infortunio ecc.). In questa ultima ipotesi, è raccomandabile utilizzare un messaggio "Out of Office" facendo menzione di chi, all'interno dell'Ente, assumerà le mansioni durante l'assenza, oppure indicando un indirizzo e-mail alternativo preferibilmente di ufficio/servizio/gruppo di lavoro, tipo *nomeufficio@comunesanmichele.it*. Rivolgersi al Servizio CED per tale eventualità.

9.12 In caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, qualora non fosse possibile attivare la funzione di inoltro automatico su altre caselle dell'Ente e si debba conoscere il contenuto dei messaggi di posta elettronica, l'utente assegnatario di una *casella di posta nominativa* ha la facoltà di delegare un altro dipendente (fiduciario) tramite la consegna delle proprie credenziali di accesso, oppure di richiedere il "reset" della password da parte del Servizio CED, per verificare il contenuto di messaggi e per inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Sarà compito del Dirigente responsabile assicurarsi che sia redatto un verbale attestante quanto avvenuto e che sia informato il lavoratore interessato alla prima occasione utile;

9.13 La diffusione massiva di messaggi di posta elettronica deve essere effettuata esclusivamente per motivi inerenti il servizio, possibilmente su autorizzazione del Dirigente responsabile competente. Per evitare che le eventuali risposte siano inoltrate a tutti, generando traffico eccessivo ed indesiderato, i destinatari dovranno essere messi in copia nascosta (Bcc o Ccn) se la tipologia del messaggio lo consente.

9.14 È vietato inviare posta elettronica in nome e per conto di un altro utente, salvo sua espressa autorizzazione;

9.15 La casella di posta elettronica personale deve essere mantenuta in ordine, cancellando messaggi e documenti la cui conservazione non è più necessaria. Anche la conservazione di messaggi con allegati pesanti è da evitare per quanto possibile, preferendo, in alternativa, il salvataggio dell'allegato sulle condivisioni dell'Ente.

9.16 I messaggi in entrata vengono sistematicamente analizzati alla ricerca di virus e malware o per l'individuazione di spam. I messaggi che dovessero contenere virus o rappresentare spam vengono comunque opportunamente segnalati e trasmessi dal sistema al destinatario mediante uno specifico messaggio.

Si informa che le comunicazioni anche elettroniche ed i documenti elettronici allegati possono avere rilevanza procedimentale e pertanto devono essere conservate per la durata prevista dalla normativa vigente.
Si informa altresì che l'Ente, per il tramite del Servizio CED, non controlla sistematicamente il flusso di comunicazioni mail né è dotato di sistemi per la lettura o analisi sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail.
Tuttavia, in caso di assenza improvvisa o prolungata del dipendente ovvero per imprescindibili esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio del Comune di San Michele al Tagliamento ovvero per motivi di sicurezza del sistema informatico, l'Ente per il tramite del Servizio CED può, secondo le procedure indicate successivo punto 12 del presente Regolamento, accedere alla casella nominale di posta elettronica assegnata al dipendente, prendendo visione dei messaggi, salvando o cancellando file.
Si informa che, in caso di cessazione del rapporto lavorativo del dipendente, la casella nominale di posta elettronica dell'Ente ad esso assegnata verrà disattivata entro una settimana. Il Dirigente responsabile può eventualmente richiedere formalmente una proroga di tale disattivazione e, solo per esigenze strettamente organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente, può eventualmente richiedere al Servizio CED il "reset" della password delle credenziali per consegnarle ad un soggetto incaricato dall'Ente per il trattamento in sola consultazione dei dati e delle informazioni pervenute, trasmettendone il contenuto ad altri dipendenti (se il messaggio ha contenuto lavorativo) ovvero cancellandolo (se il messaggio non ha contenuto lavorativo).
Le informazioni eventualmente raccolte sono altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, compresa la verifica del rispetto del presente Regolamento, che costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli ai sensi del Regolamento Europeo 679/16 "General Data Protection".

10 Utilizzo dei telefoni, fax, fotocopiatrici, scanner e stampanti dell'Ente

Il dipendente è consapevole che gli Strumenti di stampa, così come anche il telefono dell'Ente, sono di proprietà del Comune di San Michele al Tagliamento e sono resi disponibili all'utente per rendere la prestazione lavorativa. Pertanto ne viene concesso l'uso esclusivamente per tale fine.

10.1 Il telefono dell'Ente affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa e non sono quindi consentite comunicazioni a carattere personale e/o non strettamente inerenti l'attività lavorativa stessa. La ricezione o l'effettuazione di comunicazioni a carattere personale è consentito solo nel caso di comprovata necessità ed urgenza.

10.2 Qualora venisse assegnato un cellulare dell'Ente all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Ai cellulari e smartphone dell'Ente si applicano le medesime regole sopra previste per gli altri dispositivi informatici (cfr. 7 "Utilizzo di personal computer"), per quanto riguarda il mantenimento di un adeguato livello di sicurezza informatica. In particolare si raccomanda il rispetto delle regole per una corretta navigazione in Internet (cfr. 8), se consentita.

10.3 Per gli smartphone dell'Ente è vietata l'installazione e l'utilizzo di applicazioni (o altresì denominate "App" nel contesto degli smartphone) diverse da quelle autorizzate dal Servizio CED.

10.4 È vietato l'utilizzo delle fotocopiatrici dell'Ente per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile di Ufficio/Servizio.

10.5 Per quanto concerne l'uso delle stampanti gli utenti sono tenuti a:

- Stampare documenti solo se strettamente necessari per lo svolgimento delle proprie funzioni operative;
- Prediligere le stampanti di rete condivise, rispetto a quelle locali/personali, per ridurre l'utilizzo di materiali di consumo (toner ed altri consumabili);
- Prediligere la stampa in bianco/nero e fronte/retro al fine di ridurre i costi, se possibile.

10.6 Le stampanti e le fotocopiatrici dell'Ente devono essere spente ogni sera prima di lasciare gli uffici o in caso di inutilizzo prolungato.

10.7 Nel caso 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.

11 Assistenza agli utenti e manutenzioni

11.1 Il Servizio CED e gli Amministratori di Sistema possono accedere ai dispositivi informatici dell'Ente sia direttamente, sia mediante software di accesso remoto, per i seguenti scopi:

- verifica e risoluzione di problemi sistemistici ed applicativi, su segnalazione dell'utente finale;
- verifica del corretto funzionamento dei singoli dispositivi in caso di problemi rilevati nella rete;
- richieste di aggiornamento software e manutenzione preventiva hardware e software (aggiornamento con cadenza almeno settimanale delle impronte digitali di malware nei software antivirus installati nelle postazioni, installazione delle patch di aggiornamento dei sistemi operativi e dei programmi utilizzati per il trattamento dei dati personali con cadenza annuale, che tuttavia diviene semestrale in caso di trattamenti di dati sensibili o giudiziari).

11.2 Gli interventi tecnici posso avvenire previo consenso dell'utente, quando l'intervento stesso richiede l'accesso ad aree personali dell'utente stesso. Qualora l'intervento tecnico in loco o in remoto non necessiti di accedere mediante credenziali utente, gli Amministratori di sistema sono autorizzati ad effettuare gli interventi senza il consenso dell'utente cui la risorsa è assegnata.

11.3 L'accesso in teleassistenza sui PC della rete dell'Ente richiesto da terzi (fornitori e/o altri) deve essere autorizzato dall'Amministratore di Sistema, per le verifiche delle modalità di intervento per il primo accesso. Le richieste successive, se effettuate con la medesima modalità, possono essere gestite autonomamente dall'utente finale.

11.4 Durante gli interventi in teleassistenza da parte di operatori terzi, l'utente richiedente o gli Amministratori di Sistema devono presenziare la sessione remota, in modo tale da verificare ed impedire eventuali comportamenti non conformi al presente regolamento.

12 Controlli sugli Strumenti (art. 6.1 Provv. Garante, ad integrazione dell'Informativa ex art. 13 Reg. 679/16)

12.1 Poiché in caso di violazioni contrattuali e giuridiche, sia l'Ente, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'Ente verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico. Il datore di lavoro, infatti, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori (art. 4, comma2), di sistemi che consentono indirettamente il controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori. Resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all'introduzione o alla modifica di sistemi automatizzati per la raccolta e l'utilizzazione dei dati, nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori. I controlli devono essere effettuati nel rispetto dell'art. **Errore. L'origine riferimento non è stata trovata.** del presente Regolamento e dei seguenti principi:

- **Proporzionalità:** il controllo e l'estensione dello stesso dovrà rivestire, in ogni caso, un carattere adeguato, pertinente e non eccessivo rispetto alla/alle finalità perseguite, ma resterà sempre entro i limiti minimi;
- **Trasparenza:** l'adozione del presente Regolamento ha l'obiettivo di informare gli utenti sui diritti ed i doveri di entrambe le parti;
- **Pertinenza e non eccedenza:** ovvero evitando un'interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, così come la possibilità di controlli prolungati, costanti o indiscriminati.

12.2 L'uso degli Strumenti Informatici dell'Ente può lasciare traccia delle informazioni sul relativo uso, come analiticamente spiegato nei riquadri di cui ai punti 6 – 7 – 8 – 9 del presente Regolamento. Tali informazioni, che possono contenere dati personali eventualmente anche sensibili dell'Utente, possono essere oggetto di controlli da parte dell'Ente, per il tramite dell'Amministratore di Sistema, volti a garantire esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente, nonché per la sicurezza e la salvaguardia del sistema informatico, per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento / sostituzione / implementazione di programmi, manutenzione hardware, etc.). Gli interventi di controllo sono di due tipi (di seguito descritti al punto 12.3 e 12.4) e possono permettere all'Ente di prendere indirettamente cognizione dell'attività svolta con gli strumenti.

12.3 **Controlli per la tutela del patrimonio dell'Ente, nonché per la sicurezza e la salvaguardia del sistema informatico. Controlli per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, ecc.).**
Qualora per le finalità qui sopra descritte risulti necessario l'accesso agli Strumenti e alle risorse informatiche e relative informazioni descritte ai punti 6 – 7 – 8 – 9 il Responsabile del trattamento dei dati personali per il tramite del Servizio CED, si atterrà al processo descritto qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo):

i. Avviso generico a tutti i dipendenti della presenza di comportamenti anomali che possono mettere a rischio la sicurezza del sistema informativo e richiamo all'esigenza di attenersi al rispetto del presente Regolamento;
ii. Successivamente, dopo almeno 7 giorni, se il comportamento anomalo persiste, l'Ente potrà autorizzare il personale addetto al controllo, potendo così accedere alle informazioni descritte ai punti 6 – 7 – 8 – 9 con possibilità di rilevare files trattati, siti web visitati, software installati, documenti scaricati, statistiche sull'uso di risorse ecc. nel corso dell'attività lavorativa. Tale attività potrà essere effettuata in forma anonima ovvero tramite controllo dell'indirizzo IP, dell'Utente e con l'identificazione del soggetto che non si attiene alle istruzioni impartite;
iii. Qualora il rischio di compromissione del sistema informativo dell'Ente sia imminente e grave a tal punto da non permettere l'attesa dei tempi necessari per i passaggi procedimentali descritti ai punti 1 e 2, il Responsabile del Trattamento, unitamente all'amministratore di sistema, può intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia.

12.4 **Controlli per esigenze produttive e di organizzazione.**

Per esigenze produttive e di organizzazione si intendono – fra le altre – l'urgente ed improrogabile necessità di accedere a files o informazioni lavorative di cui si è ragionevolmente certi che siano disponibili su risorse informatiche di un Utente (quali file salvati, posta elettronica, chat, SMS, ecc) che non sia reperibile, in quanto ad esempio assente, temporaneamente irreperibile ovvero cessato.

Qualora risulti necessario l'accesso alle risorse informatiche e relative informazioni descritte ai punti 6 – 7 – 8 – 9 il Responsabile del trattamento dei dati personali, per il tramite del Servizio CED, si atterrà alla procedura descritta qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo):

i. Redazione di un atto da parte del Segretario generale e/o Dirigente del Settore che comprovi le necessità produttive e di organizzazione che richiedano l'accesso allo Strumento;
ii. Incarico all'Amministratore di sistema di accedere alla risorsa con credenziali di Amministratore ovvero tramite l'azzeramento e la contestuale creazione di nuove credenziali di autenticazione dell'Utente interessato, con avviso che al primo accesso alla risorsa, lo stesso dovrà inserire nuove credenziali;
iii. Redazione di un verbale che riassuma i passaggi precedenti;
iv. In ogni caso l'accesso ai documenti presenti nella risorsa è limitato a quanto strettamente indispensabile alle finalità produttive e di organizzazione del lavoro;
v. Qualora indirettamente si riscontrino file o informazioni anche personali, esse potranno essere altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, considerato che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo 679/16 "General Data Protection".

Tutti i controlli sopra descritti avvengono nel rispetto del principio di necessità e non eccedenza rispetto alle finalità descritte nel presente Regolamento. Dell'attività sopra descritta viene redatto verbale, sottoscritto dal Responsabile del Trattamento e dall'Amministratore di Sistema che ha svolto l'attività.
In caso di nuovo accesso da parte dell'utente allo Strumento informatico oggetto di controllo, lo stesso dovrà avvenire previo rilascio di nuove credenziali (salvo diverse esigenze tecniche).
Qualora indirettamente si riscontrino file o informazioni anche personali, esse potranno essere altresì utilizzabili a tutti i fini connessi al rapporto di lavoro, considerato che il presente Regolamento costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo 679/16 "General Data Protection".

13 Conservazione dei dati di accesso e di traffico telematico

13.1 In riferimento agli articoli 5 e 6 del Reg. 679/16 e in applicazione ai principi di diritto di accesso, legittimità, proporzionalità, sicurezza ed accuratezza e conservazione dei dati, le informazioni relative all'accesso ad Internet e dal traffico telematico (log di sistema e del server proxy), la cui conservazione non sia necessaria, saranno cancellati entro i termini indicati nel presente Regolamento, salvo esigenze tecniche o di sicurezza; o per l'indispensabilità dei dati rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria o, infine, all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

13.2 La Ente si impegna ad assumere le misure di sicurezza nel trattamento e nella conservazione di tale tipologia di dati alla luce di quanto stabilito dal Legislatore.

14 Partecipazioni a Social Media

14.1 L'utilizzo a fini promozionali di Facebook, Twitter, Linkedin, dei blog e dei forum, anche professionali (ed altri siti o "social media") è gestito ed organizzato esclusivamente dall'Ente attraverso specifiche direttive ed istruzioni operative al personale a ciò espressamente addetto, rimanendo escluse iniziative individuali da parte dei singoli utenti o collaboratori.

14.2 Fermo restando il diritto della persona alla libertà di espressione, l'Ente ritiene comunque opportuno indicare agli utenti alcune regole comportamentali, al fine di tutelare tanto la propria immagine ed il patrimonio dell'Ente, anche immateriale, quanto i propri collaboratori, i propri clienti e fornitori, gli altri enti collegati, oltre che gli stessi utenti utilizzatori dei social media, fermo restando che è vietata la partecipazione agli stessi social media durante l'orario di lavoro.

14.3 Il presente articolo deve essere osservato dal dipendente sia che utilizzi dispositivi messi a disposizione dall'Ente , sia che utilizzi propri dispositivi, sia che partecipi ai social media a titolo personale, sia che lo faccia per finalità professionali, come dipendente dell'Ente.

14.4 La condivisione dei contenuti nei social media deve sempre rispettare e garantire la segretezza sulle informazioni dell'Ente, nel rispetto del segreto d'ufficio, segreto professionale e privacy.

15 Formazione degli utenti e dipendenti sulle misure di sicurezza tecniche ed organizzative

Il Titolare del trattamento dovrà occuparsi di fornire strumenti idonei a tutti gli utenti e dipendenti per la formazione sui vari argomenti inerenti il Regolamento Europeo 679/16 per la protezione dei dati personali, ed in particolare relativamente a:

- Profili della disciplina sulla protezione dei dati personali, più rilevanti in rapporto alle correlate attività, e conseguenti responsabilità che ne derivano;
- Rischi che incombono sui dati;
- Misure di sicurezza disponibili per prevenire eventi dannosi;
- Modalità per aggiornarsi sulle misure minime di sicurezza adottate dal Titolare del trattamento.

16 Sanzioni disciplinari

16.1 È fatto obbligo a tutti i dipendenti/collaboratori/utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento.

Elenco firmatari

ATTO SOTTOSCRITTO DIGITALMENTE AI SENSI DEL D.P.R. 445/2000 E DEL D.LGS. 82/2005 E SUCCESSIVE MODIFICHE E INTEGRAZIONI

Questo documento è stato firmato da:

NOME: Tamara Plozzer
CODICE FISCALE: IT:PLZTMR73H70E473H
DATA FIRMA: 15/10/2019 09:56:13
IMPRONTA: 3564316536353839613161373237323039393536393538343030613462356533261333461626633

NOME: Pasqualino Codognotto
CODICE FISCALE: TINIT-CDGPQL59C25I040H
DATA FIRMA: 15/10/2019 10:42:00
IMPRONTA: 653163623562323337623466643131393964353565653263653965636335313939616139303163 63