MANUALE TECNICO-ORGANIZZATIVO PER L'UTILIZZO DELLE RISORSE ICT DEL COMUNE DI TAVAGNACCO

Rev_05 del 20/06/2022

Approvato con Deliberazione G.M. n. XX del XX.XX.2022

SOMMARIO

1. INTRODUZIONE

La crescente diffusione delle nuove tecnologie informatiche, il libero accesso alla rete *Internet* dai diversi dispositivi informatici e, in particolare, l'utilizzo massiccio e quasi esclusivo delle tecnologie *ICT* nell'attività lavorativa dell'Ente (secondo anche le Linee Guida del Codice dell'Amministrazione Digitale e gli obiettivi dell'Agenda Digitale Italiana) espongono l'Ente e gli Utenti a diverse forme responsabilità conseguenti alla violazione di specifiche disposizioni normative, creando un potenziale pregiudizio alle funzioni organizzative, così come alla sicurezza e all'immagine dell'Amministrazione.

Il presente Manuale intende fornire ai dipendenti e collaboratori, incaricati o utenti del Comune di Tavagnacco, 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 *personal computer*, *notebook*, *e-mail* ed altri strumenti con relativi *software* e applicativi (di seguito più semplicemente "Strumenti"), sono messi a disposizione dall'Ente per finalità istituzionali, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio dell'Ente. Gli Strumenti, nonché le relative reti dell'Ente a cui è possibile accedere tramite gli stessi, sono domicilio informatico del Comune di Tavagnacco. Al dipendente/collaboratore viene concesso l'uso degli Strumenti esclusivamente per lo svolgimento dell'attività lavorativa e non sono quindi consentiti scambi informativi/comunicazioni a carattere personale e/o non strettamente inerenti all'attività lavorativa stessa. È vietato il salvataggio sui *server* dell'Ente, ovvero sugli Strumenti, di documenti non inerenti all'attività lavorativa, quali a titolo esemplificativo documenti, fotografie, video, musica, pratiche personali, *sms*, *e-mail* personali, film.

Considerato che il presente Manuale costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione delle verifiche, 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 utilizzabili a tutti i fini connessi al rapporto di lavoro, sempre nel rispetto di quanto disposto dal Regolamento Europeo 679/2016 "*General Data Protection Regulation*".

Viene precisato, infine, 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.

1.1 Oggetto e finalità

La finalità principale è quella di promuovere tra tutto il personale dell'Ente un'adeguata cultura informatica, affinché l'utilizzo delle risorse informatiche e telematiche (risorse ICT) fornite dall'Ente - quali *PC* e *hardware* con i relativi *software*, la posta elettronica, *internet* e telefonia - sia conforme alle finalità dell'Ente e pienamente rispettoso della legge. Si vogliono fornire le necessarie indicazioni a tutto il personale, con l'obiettivo principale di evitare il verificarsi di qualsiasi abuso o uso non conforme.
L'Amministrazione, in particolare, intende ridurre i rischi relativi alle minacce di sicurezza informatica, preservando la disponibilità, integrità e riservatezza dei dati e la continuità dei servizi erogati, nonché garantire il rispetto della normativa in materia di utilizzo degli strumenti informatici.

1.2 Ambito di applicazione

Ai fini delle disposizioni per l'utilizzo delle risorse informatiche e telematiche, l'applicazione delle stesse è indirizzata ai seguenti soggetti (di seguito complessivamente denominati "utenti"), senza distinzione di ruolo e/o di livello e a prescindere dai rapporti contrattuali intrattenuti con gli stessi:

- tutti i dipendenti, senza distinzione di ruolo e/o di livello e indipendentemente dalla modalità di svolgimento dell'attività lavorativa (ad es. *smart working*, telelavoro);
- tutti i collaboratori e prestatori di lavoro autonomo, a prescindere dal rapporto contrattuale intrattenuto con l'amministrazione, in possesso di specifiche credenziali di autenticazione;
- in generale, chiunque sia autorizzato all'utilizzo delle dotazioni del Comune nello svolgimento delle proprie funzioni istituzionali (rientrano, tra gli altri, in tali categorie di figure anche gli assegnatari provvisori di credenziali quali stagisti, studenti, incaricati a svolgere servizi interni su affidamento da parte dell'Ente);
- gli ospiti dell'Ente e le figure che ricoprono incarichi politici.

1.3 Tutela del lavoratore

- Alla luce dell'art. 4, c. 1, L. 300/1970, la regolamentazione della materia indicata nell'art. 1 del presente Manuale, 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 rispetto del trattamento dei dati personali.
- 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. 679/2016.

2. PRINCIPI, MODALITÀ, DOVERI NELL'UTILIZZO

Le regole sono declinate su tre versanti: **tecnologico-procedurale**, **organizzativo** e **comportamentale**. Tutti gli interventi sono finalizzati a garantire la riservatezza, l'integrità e la disponibilità delle informazioni (dati) di cui l'Ente è Titolare.

In particolare:

- la confidenzialità o riservatezza riguarda la conoscibilità e la fruibilità delle informazioni ai soli soggetti autorizzati;
- l'integrità è relativa alla completezza e all'inalterabilità delle informazioni;
- la disponibilità concerne l'accessibilità e l'usabilità delle informazioni nel tempo da parte dei soggetti autorizzati.

2.1 Principi generali e di riservatezza nelle comunicazioni

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

- **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. 679/2016);
- **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 può avvenire all'insaputa o senza la piena

consapevolezza dei lavoratori, considerate anche le potenziali applicazioni di regola non adeguatamente conosciute dagli interessati;

- **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".

Il dipendente si attiene alle seguenti regole di trattamento:

- è vietato comunicare a soggetti non specificatamente autorizzati i dati personali comuni, particolari, giudiziari, sanitari o altri dati, elementi e informazioni dell'Ente dei quali il dipendente/collaboratore viene a conoscenza nell'esercizio delle proprie funzioni e delle mansioni all'interno dell'Ente. 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;
- 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, se non previa richiesta;
- 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, etc.) materiali che non siano inerenti alla pratica che si sta trattando in quel momento. Ciò vale soprattutto nel caso di lavoratori con mansioni di *front-office*. Il tutto è attuabile compatibilmente con le dotazioni assegnate e lo spazio a disposizione;
- è vietato gettare atti e/o appunti d'ufficio nella spazzatura, se non dopo averli debitamente parcellizzati tramite i sistemi distruggi-documenti o altro idoneo sistema;
- chiudere a chiave tutti i cassetti (se contenenti dati personali o particolari), gli armadi (se contenenti dai personali o particolari) e le porte, al termine dei propri orari di servizio;
- per le riunioni e per gli incontri con utenti, cittadini, clienti, fornitori, consulenti e collaboratori dell'Ente è preferibile, se presenti, utilizzare le eventuali sale dedicate;
- è vietato colloquiare con colleghi di attività d'ufficio, al telefono o di persona, in presenza di estranei;
- moderare il tono della voce ogni qualvolta si trattino argomenti inerenti dati personali;
- è vietato divulgare a familiari ed amici dettagli dell'attività svolta e della struttura informatica comunale.

3. SOLUZIONI TECNOLOGICO-PROCEDURALI

3.1 Gestione, assegnazione e revoca delle credenziali di accesso

3.1.1 Le credenziali di autenticazione per l'accesso alle risorse informatiche vengono assegnate dall'Amministratore di Sistema, previa formale richiesta del Responsabile dell'Area. Per ciascun nuovo utente dovrà essere specificato, all'atto della richiesta, il nome e cognome. Nel caso di collaboratori esterni la richiesta dovrà essere inoltrata direttamente dal Responsabile dell'Area con il quale il collaboratore si coordina nell'espletamento del proprio incarico secondo quanto indicato nel presente comma.

La richiesta di attivazione delle credenziali dovrà inoltre comprendere l'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 all'Ufficio Sistemi Informativi dal Responsabile di riferimento.

3.1.2 Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente, di solito costituito dalla prima lettera del nome punto e cognome dell'utente scritto in minuscolo tutto attaccato (ad es. "n.cognome"), altresì nominati *username*, nome utente o *user-id*, assegnato dall'Amministratore di Sistema, 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.

3.1.3 La *password* deve essere di adeguata robustezza: deve essere composta da almeno 8 caratteri, formata da lettere maiuscole e minuscole, numeri e caratteri speciali. Non deve contenere riferimenti agevolmente riconducibili all'utente (*username*, nomi o date relative alla persona o ad un familiare). Le *password* utilizzate per l'accesso ai diversi servizi devono essere diversificate, al fine di evitare la loro facile replicabilità.

3.1.4 È necessario procedere alla modifica della *password* a cura dell'utente al primo accesso e, successivamente, almeno ogni sei mesi (o quando richiesto dal sistema o *software* utilizzato). Nel caso in cui l'utente svolga mansioni che, in astratto, possano comportare il trattamento di dati personali particolari, è obbligatorio il cambio password almeno ogni due mesi.

3.1.5 Nel caso di cessazione del rapporto di lavoro con il dipendente/collaboratore, il Responsabile dell'Area di riferimento dovrà comunicare formalmente e preventivamente all'Ufficio Sistemi Informativi la data effettiva a partire dalla quale le credenziali saranno disabilitate. Qualora la cessazione del rapporto si riferisca al Responsabile dell'Area stessa, spetta al Segretario Comunale provvedere all'espletamento di tali attività.

3.1.6 Le credenziali d'accesso sono personali, segrete, non cedibili e non divulgabili. Ove tali codici d'accesso non siano stati attribuiti è vietato l'utilizzo di codici assegnati ad altri utenti.

3.1.7 Ogni utente deve conservare diligentemente tutte le credenziali d'accesso assegnate, in modo da consentire il loro facile e immediato recupero ed aggiornamento, garantendo nel contempo la riservatezza assoluta di tali informazioni. In caso di cessazione dal servizio, indipendentemente dalla motivazione (pensione, mobilità, trasferimento, dimissioni), l'utente che dispone di credenziali relative ad *account* attivati in nome e per conto dell'Ente, dovrà procedere per tempo al relativo passaggio di consegne.

3.2 Sicurezza dei sistemi di elaborazione e archiviazione dati centralizzati

Il sistema informativo di un Ente rappresenta un punto cardine nell'attività lavorativa dell'Amministrazione per l'erogazione dei servizi a cittadini e imprese. Il sistema informativo è a sua volta basato su un sistema informatico che, in caso di anomalie di funzionamento, potrebbe causare l'interruzione di molteplici servizi, provocando disservizio agli utenti e di conseguenza ai dipendenti dell'Amministrazione. Il Servizio Sistemi Informativi di un Ente deve essere considerato come infrastruttura critica tale per cui il suo corretto funzionamento rappresenta il requisito indispensabile per la regolare erogazione dei servizi. Il sistema informatico racchiude infatti gran parte del patrimonio di dati e informazioni di cui l'Ente è titolare, visto l'utilizzo massiccio e quasi esclusivo delle tecnologie ICT nell'attività lavorativa dell'Amministrazione. Una minaccia alla sicurezza del sistema informatico rappresenta una potenziale indisponibilità dei dati e delle informazioni in esso custoditi e dei servizi che tramite esso sono erogati. Risulta pertanto fondamentale provvedere ad

un'adeguata gestione, nonché alla sicurezza, sia fisica che logica, dei sistemi informatici che costituiscono l'infrastruttura del Servizio Sistemi Informativi dell'Ente. A questo proposito è indispensabile configurare i sistemi di elaborazione ed archiviazione dei dati centralizzati (*server*, NAS e simili), nonché i dispositivi individuali, conformemente agli standard di sicurezza e/o *best practice* (ad es. abilitare soltanto i servizi strettamente necessari, applicare sistematicamente le "*patch*") emessi da Enti ed Organizzazioni internazionali (ad es. I*nternational Standard Organization* - ISO, *National Institute of Standards and Technology* - NIST, *Sans Institute*). Laddove l'Ente si avvalga di propri fornitori dovrà prevedere nei contratti di appalto l'obbligo di rispettare i predetti standard di sicurezza e, inoltre, dovrà prevedere clausole di "responsabilità esterna" e di "amministrazione dei sistemi", in attuazione del Provvedimento Generale del Garante dei dati personali del 27.11.2008 (in materia di Amministratori di Sistema), come modificato con successivo Provvedimento Generale del 25.06.2009.

3.3 Sicurezza della rete

L'Amministratore di Rete/di Sistema configura la Rete Telematica dell'Ente per contribuire alla protezione dei sistemi informatici con strumenti e livelli di protezione (ad es. *firewall*, *IPS*, *application firewall*) adeguati in base al livello di classificazione assegnato ai dati ospitati nei suddetti sistemi (*server*, *NAS* e simili).

3.4 Distruzione dei dispositivi

Ogni dispositivo ed ogni memoria esterna affidati agli utenti (*computer*, *notebook*, *tablet*, *smartphone*, *memory card*, chiavi *USB*, *hard disk*, *dvd*, *cd-rom*, etc.), al termine del loro utilizzo dovranno essere restituiti all'Ente, che provvederà a distruggerli o a ricondizionarli seguendo le norme di legge in vigore al momento. In particolare, l'Ente provvederà a cancellare o a rendere inintelligibili i dati negli stessi memorizzati.

4. SOLUZIONI ORGANIZZATIVE

4.1 Autenticazione utente

Ciascun utente, da parte sua, per una corretta e sicura gestione delle proprie password, deve rispettare le seguenti regole:

4.1.1 le *password* sono assolutamente personali e non vanno mai comunicate ad altri;
4.1.2 occorre cambiare immediatamente una password, al momento del primo accesso al sistema informatico e non appena si abbia alcun dubbio che sia diventata poco "sicura";
4.1.3 le *password* devono rispettare criteri di complessità che possono adattarsi nel tempo a diverse situazioni;
4.1.4 le *password* non devono essere memorizzate su alcun tipo di supporto, quali, ad esempio, Post-It (sul monitor o sotto la tastiera) o agende (cartacee, posta elettronica, telefono cellulare);
4.1.5 le *password* devono essere sostituite almeno ogni 180 giorni, a prescindere dall'esistenza di un sistema automatico di richiesta di cambio password;
4.1.6 le *password* già utilizzate non devono essere riutilizzate a breve distanza di tempo (*password history*);

4.1.7 le *password* non devono contenere riferimenti esplicitamente riconducibili all'utente ed al suo *username*;

4.1.8 evitare di digitare la propria password in presenza di altri soggetti che possano vedere la tastiera, anche se collaboratori o dipendenti dell'Ente. In alcuni casi, sono implementati meccanismi che consentono all'utente un numero limitato di tentativi errati di inserimento della *password*, oltre ai quali il tentativo di accesso viene considerato un attacco al sistema e l'account viene bloccato per alcuni minuti;

4.1.9 le regole su elencate sono da considerarsi un punto di partenza, ma non vanno intese come principi cristallizzati nel tempo, valevoli per sempre, perciò occorre mantenersi sempre informati, per esempio, visitando periodicamente il sito dell'autorità "Garante per la protezione dei dati personali" in cui è presente una sezione https://www.garanteprivacy.it/temi/cybersecurity/password contenente una selezione di contenuti in costante aggiornamento, raccolti in un vademecum, "Suggerimenti per creare e gestire password a prova di privacy" https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4248578 con finalità divulgative, tenuto aggiornato in base in base agli sviluppi tecnologici e normativi.

4.2 Operazioni a protezione e gestione della postazione di lavoro

Di seguito vengono descritte le operazioni a carico dell'utente e il quadro di riferimento generale per l'esecuzione di operazioni a protezione della propria postazione di lavoro, nel rispetto della sicurezza e dell'integrità del patrimonio di dati e informazioni di cui l'Ente è Titolare.

4.2.1 *Login* e *Logout* - Il "*Login*" è l'operazione con la quale l'utente si connette al sistema informativo dell'Ente o ad una parte di esso, inserendo le proprie credenziali di autenticazione (nome utente e *password*), aprendo una sessione di lavoro. In molti casi è necessario effettuare più login, tanti quanti sono gli ambienti di lavoro (ad es. applicativi gestionali, *Intranet*), ognuno dei quali richiede un nome utente e una *password*.

4.2.2 Il "*Logout*" è l'operazione con cui viene chiusa la sessione di lavoro. Al termine della giornata lavorativa, tutte le applicazioni devono essere chiuse secondo le regole previste dall'applicazione stessa. La non corretta chiusura può provocare una perdita di dati o l'accesso agli stessi da parte di persone non autorizzate. Il "blocco del computer" è l'operazione con cui viene impedito l'accesso alla sessione di lavoro senza chiuderla. L'utilizzo dei dispositivi fisici e la gestione dei dati ivi contenuti devono svolgersi nel rispetto della sicurezza e dell'integrità del patrimonio dati dell'Ente.

4.2.3 L'utente deve quindi eseguire le operazioni seguenti:

- se ci si allontana dalla propria postazione, dovrà mettere in protezione il suo dispositivo affinché persone non autorizzate non abbiano accesso ai dati protetti; impostare sempre il salvaschermo con annessa richiesta di *password* al momento della riattivazione
- bloccare il proprio dispositivo prima delle pause e, in generale, ogni qualvolta abbia bisogno di allontanarsi dalla propria postazione;
- chiudere le sessioni di lavoro (*logout*) a fine giornata;
- spegnere il *PC* dopo il *logout* dalle suddette sessioni lavorative;
- controllare sempre che non vi siano persone non autorizzate che possano prendere visione delle schermate del proprio dispositivo;

- i documenti contenenti informazioni riservate devono essere chiusi a chiave in un cassetto o in un armadio. Si raccomanda a fine giornata di chiudere determinati uffici, se vi sono documenti contenenti dati sensibili o giudiziari;
- ricordarsi di estrarre dal fotocopiatore tutti i documenti; per la stampa di documenti riservati, si raccomanda di utilizzare una stampante non condivisa o una modalità di stampa ritardata;
- non comunicare a nessun soggetto non autorizzato le informazioni di cui si viene a conoscenza durante il rapporto di lavoro (ad es. dati sanitari, dati giudiziari);
- per quanto riguarda i colloqui con colleghi o utenti autorizzati, assicurarsi che non vi siano terzi; qualora i colloqui dovessero avere ad oggetto situazioni delicate, si raccomanda di svolgerli in luoghi isolati.

4.3 Utilizzo della rete del Comune di Tavagnacco e *file system*

4.3.1 Per l'accesso alle risorse informatiche del Comune di Tavagnacco attraverso la rete locale, ciascun utente deve essere in possesso di credenziali di autenticazione secondo le sezioni 3.2 e 4.1.

4.3.2 È proibito accedere alla rete e ai sistemi informativi utilizzando credenziali di altre persone.

4.3.3 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 unità operativa o per diversi criteri o per obiettivi specifici di lavoro. 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 all'attività lavorativa, quali a titolo esemplificativo documenti, fotografie, video, musica, pratiche personali, *sms*, *e-mail* personali, film, etc. Ogni materiale personale rilevato dall'Amministratore di Sistema o dall'Ufficio Sistemi Informativi a seguito di interventi di sicurezza informatica ovvero di manutenzione/aggiornamento su server ed anche sugli Strumenti in uso sarà rimosso senza ulteriori avvisi, ferma restando ogni eventuale responsabilità personale in caso di danni causati. 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. A titolo di esempio e non esaustivo si citano: il disco C o altri dischi locali dei singoli PC, la cartella "Documenti" o "*Desktop*" dell'utente, 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.

4.3.4 Senza il consenso dell'Ufficio Sistemi Informativi o dell'Amministratore di Sistema, è vietato trasferire documenti elettronici dai sistemi informativi e Strumenti dell'Ente a *device* esterni (*hard disk*, chiavette *USB*, *CD*, *DVD* e altri supporti).

4.3.5 L'eventuale utilizzo di *repository* esterne per il salvataggio dati e/o l'invio dei documenti elettronici a terzi via posta elettronica devono essere autorizzati dall'Amministratore di Sistema.

4.3.6 Con regolare periodicità (almeno una volta al mese), ciascun utente provvede alla pulizia degli archivi (anche della posta elettronica), con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

4.3.7 Il Comune di Tavagnacco mette a disposizione dei propri utenti la possibilità di accedere alla posta elettronica anche remotamente.

4.3.8 L'Ufficio Sistema Informativi 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.

4.3.9 Ove non esistano specifiche diverse disposizioni, è vietato inserire codici di protezione all'accesso su singoli *file* (ad esempio di elaborati con sistemi di trattamento testi, fogli di calcolo).

I *log* relativi all'uso del *File System* e della *Intranet*, 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 l'Amministratore di Sistema, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio. I controlli possono avvenire secondo le disposizioni previste alla successiva sezione 9 del presente Manuale.

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 Regulation*".

4.4 Gestione delle richieste di accesso al contenuto di risorse *ICT*

L'Ente in caso di utenti deceduti, sospesi o cessati dal servizio, potrebbe avere la necessità di recuperare documenti importanti su risorse ICT, assegnate ai predetti Utenti, al fine di proseguire le attività in cui gli utenti medesimi erano coinvolti. In tali casi il Responsabile dell'Area/Servizio di afferenza dell'utente assegnatario delle risorse ICT potrà chiedere all'Amministratore di Sistema di avere accesso alle suddette risorse ICT per estrarre dalle risorse medesime le informazioni indispensabili per proseguire l'attività lavorativa.

4.5 Utilizzo di sistemi di *Cloud Computing*

In informatica con il termine inglese *cloud computing* (in italiano nuvola informatica) si indica un paradigma di erogazione di risorse informatiche (come l'archiviazione, l'elaborazione o la trasmissione di dati) caratterizzato dalla disponibilità *on demand* attraverso *Internet* a partire da un insieme di risorse preesistenti e configurabili.
Utilizzare un servizio di *cloud computing* per memorizzare dati personali, espone l'Ente a potenziali problemi di violazione della *privacy*. I Dati Personali vengono memorizzati nelle *server farm* di aziende che spesso risiedono in uno stato diverso da quello dell'Ente. Il *cloud provider*, in caso di comportamento scorretto o malevolo, potrebbe accedere ai dati personali per eseguire ricerche di mercato e profilazione degli utenti. Con i collegamenti *wireless* "liberi", il rischio sicurezza aumenta e si è maggiormente esposti ai casi di pirateria informatica a causa della minore sicurezza offerta dalle reti senza fili ad accesso libero. In presenza di atti illegali, come appropriazione indebita o illegale di dati personali, il danno potrebbe essere molto grave per l'Ente, con difficoltà di raggiungere soluzioni giuridiche e/o rimborsi se il fornitore risiede in uno stato diverso dal Paese dell'utente.
Per quanto indicato gli utenti dovranno rispettare le seguenti indicazioni:

- è vietato agli utenti l'utilizzo di sistemi *cloud* non espressamente approvati dall'Ente. Per essere approvati, i sistemi *cloud* devono rispondere ad almeno i seguenti requisiti:
- essere sistemi *cloud* esclusivi e non condivisi;
- essere sistemi *cloud* posizionati fisicamente nell'Unione Europea.

4.6 Smarrimento e furto delle risorse *ICT* – gestione *Data Breach*

Nei casi di smarrimento, furto accertato o grave manomissione dei dispositivi assegnati o del loro contenuto, gli utenti devono segnalare tempestivamente l'accaduto ai soggetti di seguito indicati:

a) Autorità Giudiziaria (sporgendo denuncia);
b) Titolare e Responsabile del trattamento dei dati;
c) Responsabile Sistemi Informativi e Amministratore di Sistema dell'Ente;
d) Provider di servizi di telecomunicazione (telefonia e internet).

Qualora il dipendente/collaboratore venga a conoscenza di una presunta violazione di sicurezza che comporta il trattamento illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso a dati personali trasmessi, conservati o comunque trattati, si dovrà agire come di seguito indicato.

FASE 1 - SEGNALAZIONE

La procedura *Data Breach* viene avviata quando si viene effettivamente a conoscenza del fatto che una sospetta, presunta o effettiva violazione dei dati personali si sia verificata. Di detto evento bisogna darne immediata comunicazione al proprio Responsabile (Posizione Organizzativa o Dirigente), il quale provvederà nel più breve tempo possibile a darne comunicazione a:

1. Responsabile Protezione Dati (*DPO*);
2. Responsabile Sistemi Informativi e Amministratore di Sistema dell'Ente;
3. Segretario Comunale (che avviserà Sindaco e/o Assessore competente e - se coinvolta - alla Società esterna che gestisce gli aspetti IT della risorsa violata, anche quale responsabile del trattamento ex art. 28 GDPR).

I soggetti da 1 a 3 sono definiti: "Gruppo *Data Breach*" e agiscono per conto del Titolare del Trattamento.

La comunicazione al Gruppo *Data Breach* relazionando quanto segue:

- denominazione della/e banca/banche dati oggetto di *data breach*;
- breve descrizione dei dati personali ivi trattati;
- quando si è verificata la violazione dei dati personali;
- dove e come è avvenuta la violazione dei dati (ad es., a seguito di virus informatico, attacco informatico, sottrazione o smarrimento di dispositivi o di supporti portatili).

FASE 2 - ISTRUTTORIA

Il "Gruppo *Data Breach*" assume nel più breve tempo possibile eventuali ulteriori informazioni sull'evento, qualora ritenute necessarie. Tale attività istruttoria può avvenire con:

a) richieste di informazioni a dipendenti e referenti del Servizio oggetto di potenziale Data Breach;
b) richieste di relazioni tecnico informatiche al Responsabile IT, al Responsabile esterno del trattamento art. 28, ad un tecnico informatico esterno e indipendente (con importo dedicato a bilancio);
c) acquisizioni di informazioni ed approfondimenti.

FASE 3 - RELAZIONE PRELIMINARE SU POTENZIALE *DATA BREACH*

Entro 36 ore dalla FASE 1 (termine indicativo, perché può dipendere dalla durata dell'istruttoria), il Gruppo *Data Breach* procede tempestivamente alla valutazione degli elementi acquisiti nella fase

istruttoria, redigendo una relazione (anche sottoforma di verbale di incontro) che contenga elementi essenziali quali:

- tipo di violazione (ad es. lettura, copia, alterazione, diffusione dei dati);
- dispositivo oggetto della violazione (PC, dispositivi portatili, etc);
- soggetti interessati dall'evento;
- gravità della violazione anche in relazione ai diritti e alle libertà eventualmente compromesse dell'interessato;
- misure di sicurezza tecniche ed organizzative applicate ai dati oggetto di violazione.

A tale fine, potrà essere utilizzato altresì il *tool* di valutazione messo a disposizione dal Garante o comunque in ossequio al provvedimento del Garante sulla notifica delle violazioni dei dati personali *(data breach*) di data 30 luglio 2019.

In tale documento il Gruppo *Data Breach* dichiara motivatamente se l'evento segnalato costituisce un'effettiva violazione di dati personali, tale da integrare gli estremi dell'art. 33 e ss. GDPR. Nello specifico verrà deciso motivatamente:

a. Se necessario notificare o meno al Garante privacy l'evento di data breach (art. 33 par. 1 GDPR) in caso positivo, dare mandato di eseguire la notificazione nelle forme previste dall'Autorità Garante per la Protezione dei dati personali
b. Se necessario comunicare o meno agli interessati l'evento di data breach (art. 34 par 1) in caso positivo, dare mandato di eseguire la comunicazione nelle forme ritenute più opportune
c. Le misure tecnologiche e organizzative assunte o da assumere per contenere la violazione dei dati e prevenire simili violazioni in futuro.

FASE 4 CONCLUSIONE

Verranno protocollate e, al termine delle operazioni, archiviate:

- la relazione preliminare su potenziale *data breach*;
- l'eventuale notifica di *data breach* ai sensi dell'art. 33 par 1 GDPR;
- l'eventuale comunicazione agli interessati ai sensi dell'art. 34 par. 1 GDPR.

Verrà infine compilato e sottoscritto un "registro *data breach*" su cui viene annotata ogni attività svolta nel contesto di questa procedura.

5. SOLUZIONI COMPORTAMENTALI

5.1 Uso delle risorse informatiche e fruizione del *wi-fi*

Tutti gli utenti devono utilizzare le risorse *ICT*, fornite dall'Ente, in maniera diligente, in modo appropriato, efficiente, rispettoso e per motivi lavorativi. Gli Utenti devono utilizzare le risorse *ICT* solamente per fini professionali (in relazione alle mansioni assegnate) e per conto dell'Ente, evitando l'uso per attività non pertinenti (ad esempio esecuzione di programmi di intrattenimento, giochi *online).* Al fine di scongiurare i rischi derivanti dall'effetto "*bridge*" (ponte) tra la rete Intranet aziendale ed altre reti, gli utenti devono evitare di accedere dall'esterno della rete Intranet ai servizi di posta elettronica istituzionali e/o al servizio web dell'Ente e contemporaneamente ad altri siti Internet potenzialmente pericolosi. Particolare cautela deve essere posta, inoltre, nell'utilizzo di reti wi-fi gratuite per accedere alla rete Intranet e ai servizi di posta elettronica istituzionale, dal momento che

nell'accedere a tali servizi devono essere inserite le credenziali e che queste ultime potrebbero essere facilmente carpite da malintenzionati/*hacker*.

Gli utenti sono tenuti inoltre a:

- sottoporre a scansione antivirus preventiva gli eventuali supporti mobili in dotazione ed espressamente autorizzati (*pen-drive* USB, CD ROM/DVD, *hard disk* esterni, etc.) prima di utilizzare le risorse negli stessi contenuti;
- non trasportare le postazioni di lavoro "fisse" al di fuori delle sedi dell'Ente, salvo specifica autorizzazione.

5.2 Utilizzo degli strumenti elettronici

5.2.1 Il dipendente e collaboratore è consapevole che gli Strumenti forniti sono di proprietà del Comune di Tavagnacco e devono essere utilizzati esclusivamente per rendere la prestazione lavorativa. 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 e collaboratore si deve quindi attenere alle seguenti regole di utilizzo degli Strumenti. L'accesso agli Strumenti dell'Ente è protetto da *password*; per l'accesso devono essere utilizzati *username* e *password* assegnate dall'Amministratore di Sistema (sez. 3). A tal proposito si rammenta che essi sono strettamente personali e l'utente è tenuto a conservarli nella massima segretezza.

5.2.2 *PC*, *notebook*, *tablet*, *smartphone* ed ogni altro *hardware* devono essere custoditi con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento e segnalando tempestivamente al personale dell'Ufficio Sistemi Informativi ogni malfunzionamento e/o danneggiamento. Non è consentita l'attivazione della *password* d'accensione (*BIOS*), senza preventiva autorizzazione da parte dell'Amministratore di Sistema.

5.2.3 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.

5.2.4 L'installazione di *software* sui posti-lavoro informatizzati può avvenire solamente a fronte di autorizzazione scritta del Responsabile dell'Unità Operativa, previo nulla osta da parte del Responsabile Sistemi Informativi e Amministratore di Sistema dell'Ente: tutti gli estremi delle licenze d'uso dei *software* installati, devono essere comunicati all'amministratore si sistema dell'ente.

5.2.5 I sistemi devono essere sempre custoditi: l'utente è tenuto a disattivare il sistema, o bloccarne l'accesso, ogni qualvolta sia costretto ad assentarsi dal locale nel quale è ubicato o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima: 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.

5.2.6 I sistemi assegnati dovranno essere disattivati e spenti al termine dell'orario di servizio, fatte salve le necessità previste dalle attività di lavoro agile debitamente autorizzate.

5.2.7 I posti-lavoro informatizzati non possono essere resi inaccessibili localmente con sistemi di tipo fisico (*hardware*), al fine di permetterne la costante accessibilità da parte dell'assistenza tecnica e la loro pronta configurabilità e riallocazione fisica, per esigenze organizzative.

5.2.8 Costituisce buona regola la pulizia periodica (almeno mensile) degli archivi memorizzati sui sistemi in uso (*web-mail*, etc.), con cancellazione dei file obsoleti o non più utili.

5.2.9 La gestione dei dati su *PC* è demandata all'utente utilizzatore che dovrà provvedere a memorizzarli sulle condivisioni dell'Ente, in modo che i dati possano essere utilizzati anche da altri utenti, evitando sempre l'esclusività su di essi. Non è consentita l'installazione di programmi diversi da quelli autorizzati dall'Ufficio Sistemi Informativi.

5.2.10 Gli operatori dell'Ufficio Sistemi Informativi possono in qualunque momento procedere alla rimozione di ogni *file* o applicazione che riterranno essere pericolosi per la sicurezza dei *PC*, della rete locale e dei server dell'Ente, nonché tutte le impostazioni eventualmente configurate che possano interferire con il corretto funzionamento dei servizi informatici dell'Ente.

5.2.11 È vietato utilizzare il *PC* per l'acquisizione, la duplicazione e/o la trasmissione illegale di opere protette da *copyright*.

5.2.12 È vietato l'utilizzo di supporti di memoria magneto-ottici (chiavi *USB*, *CD*, *DVD* o altri supporti) per il salvataggio di dati trattati tramite gli Strumenti dell'Ente, salvo che il supporto utilizzato sia stato fornito/autorizzato dall'Ufficio Sistema Informativo Comunale. In tale caso, il supporto fornito può essere utilizzato esclusivamente per finalità istituzionali dell'Ente.

5.2.13 I sistemi messi a disposizione di utenti non sottoposti alle presenti prescrizioni (ad es. Biblioteca), non possono accedere alla rete del Sistema Informativo Comunale. Saranno pertanto instradati su apposite distinte reti virtuali ed avranno accesso solamente alle risorse elaborative locali ed alla rete *internet*.

5.2.14 La firma digitale viene, di norma, assegnata ai funzionari e loro sostituti aventi potere di firma.

5.2.15 I sistemi *anti-virus* installati a protezione delle stazioni di lavoro assegnate, non possono essere disattivati, se non a cura dell'Amministratore di Sistema per specifiche motivazioni.

5.2.16 È obbligatorio consentire l'installazione degli aggiornamenti di sistema che vengono proposti automaticamente, al primo momento disponibile, in modo tale da mantenere il *PC* sempre protetto.

5.2.17 Nel caso in cui l'utente dovesse notare comportamenti anomali del *PC*, lo stesso è obbligato a comunicarlo tempestivamente all'Ufficio Sistemi Informativi ovvero all' Amministratore di Sistema.

5.2.18 L'archivio anagrafico è consultabile telematicamente da parte degli utenti autorizzati, in ossequio alla normativa vigente, mediante i sistemi tecnologici disponibili e con i profili di limitazione correlati alle esigenze del servizio.

I *log* di accesso relativi all'utilizzo di Strumenti, reperibili nella memoria degli Strumenti stessi ovvero sui Server o sui router, nonché i *file* con essi trattati, sono registrati e possono essere oggetto di controllo da parte del Titolare del trattamento, attraverso l'Amministratore di Sistema, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio.

I controlli possono avvenire secondo le disposizioni previste alla successiva sezione 9 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 Regulation*".

5.3 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.

5.3.1 È ammessa solo la navigazione in siti considerati correlati con la prestazione lavorativa. L'accesso è consentito tramite apposite *policy* di sicurezza debitamente implementate e aggiornate, ad esempio per i siti istituzionali, i siti degli Enti locali, di fornitori e partner dell'Ente. Il Comune di Tavagnacco si avvale di un sistema di *content filtering*. Qualora l'accesso necessario ad un determinato link venga impedito da tale sistema, il Responsabile dell'Unità Operativa ne chiede lo sblocco in forma scritta tramite *e-mail* all'Ufficio Sistemi Informativi che provvederà a valutare la richiesta e se ritenuta lecita ne abiliterà l'accesso.

5.3.2 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 (se non pertinenti all'attività svolta), l'uso di servizi di rete con finalità ludiche o, comunque, estranee all'attività lavorativa.

5.3.3 È vietato a chiunque il *download* di qualunque tipo di *software* gratuito (*freeware*) o *shareware* prelevato da siti Internet, diverso da quelli autorizzati dall'Amministratore di Sistema.

5.3.4 L'Ente si riserva di bloccare l'accesso a siti "a rischio" anche di *default,* con l'uso del *content filtering*, attraverso l'utilizzo di *black-list* 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 nel caso in cui, per ragioni di servizio, si necessiti di una navigazione libera dai filtri, è necessario richiedere lo sblocco mediante una e-mail indirizzata all'Ufficio Sistemi Informativi, 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. Al termine dell'attività l'Amministratore di Sistema o gli addetti dell'Ufficio Sistemi Informativi ripristineranno i filtri nella situazione iniziale. È 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 dall'Ufficio Sistemi Informativi.

5.3.5 È assolutamente vietato l'utilizzo di abbonamenti privati per effettuare la connessione a Internet tranne in casi del tutto eccezionali e previa autorizzazione dell'Amministratore di Sistema.

5.3.6 È assolutamente vietata la partecipazione a forum non professionali, ai *Social Network*, l'utilizzo di *chat line* (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in *guest book* anche utilizzando pseudonimi (o *nick-name*).

5.3.7 È consentito l'uso di strumenti di messaggistica istantanea, per permettere un'efficace e comoda comunicazione tra i colleghi, mediante i soli strumenti autorizzati dall'Ufficio Sistemi Informativi. Tali strumenti hanno lo scopo di migliorare la collaborazione tra utenti aggiungendo un ulteriore canale comunicativo rispetto agli spostamenti fisici, alle chiamate telefoniche ed *e-mail*. È consentito un utilizzo legato esclusivamente a scopi professionali.

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

5.3.9 È autorizzato l'accesso ed uso, sia durante l'orario di servizio che al di fuori dello stesso, a tutti i *social network* nei quali è iscritta la Squadra Comunale di Protezione Civile del Comune di Tavagnacco da parte del Responsabile Comunale della Squadra, dal Coordinatore della medesima, dal personale incaricato, di quello dell'Ufficio Sistemi Informativi e da parte dei Volontari di *PC* Digitali individuati dal Sindaco, nonché dal Consigliere Delegato al Servizio di Protezione Civile.

5.3.10 In ossequio alla Direttiva n. 02/09 della Presidenza del Consiglio dei Ministri – Dipartimento della Funzione Pubblica – è consentito ai dipendenti l'uso della rete internet aziendale per assolvere incombenze amministrative e burocratiche senza allontanarsi dal luogo di lavoro (ad es. per effettuare adempimento on-line nei confronti di pubbliche amministrazioni e di concessionari di servizi pubblici ecc., ovvero per tenere rapporti con istituti bancari e assicurativi). Tale modalità, purché contenuta nei tempi strettamente necessari allo svolgimento delle transazioni, ha, inoltre, il vantaggio di contribuire a ridurre gli spostamenti delle persone e degli oneri logistici e di personale per l'amministrazione che eroga il servizio, favorendo, altresì, la dematerializzazione dei processi produttivi.

5.3.11 Il dipendente può altresì, previa preventiva autorizzazione dell'Responsabile di Area, supportare il cittadino che ne faccia richiesta, e che non abbia a disposizione la tecnologia necessaria e neppure la competenza informatica di base, ad accedere attraverso le credenziali che fornirà, ai servizi pubblici/privati richiesti (ad es. Inps, Inail, Enel, Rai) per procedere allo svolgimento di operazioni a lui necessarie e richieste.

Si informa che l'Ente, per il tramite dell'Amministratore di Sistema, non effettua la memorizzazione sistematica delle pagine *web* visualizzate dal singolo dipendente/collaboratore, né controlla con sistemi automatici i dati di navigazione dello stesso.

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, l'Ente registra per 90 giorni i dati di navigazione (file di *log* riferiti al traffico *web*) con modalità inizialmente volte a precludere l'immediata e diretta identificazione di utenti, mediante opportune aggregazioni.

Solo in casi eccezionali e di comprovata urgenza rispetto alle finalità sopra descritte, l'Ente potrà trattare i dati di navigazione riferendoli specificatamente ad un singolo nome utente. In tali casi i controlli avverranno nelle forme indicate alla successiva sezione 9 del presente Manuale.

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 Regulation*".

5.4 Utilizzo dei telefoni, smartphone e degli strumenti di stampa dell'Ente

Il dipendente è consapevole che gli strumenti di stampa, così come anche la telefonia dell'Ente, sono di proprietà del Comune di Tavagnacco e sono resi disponibili all'utente per rendere la prestazione lavorativa. Pertanto ne viene concesso l'uso esclusivamente per tale fine.

5.4.1 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 all'attività lavorativa stessa. La ricezione o l'effettuazione di comunicazioni a carattere personale è consentita solo nel caso di comprovata necessità ed urgenza, per il limitato tempo strettamente necessario alla comunicazione stringata, specifica ed essenziale (ad. es. comunicare a casa un ritardo dovuto a questioni lavorative, problematiche sanitarie urgenti o riguardanti figli minori).

5.4.2 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, 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 (prgf. 5.3) e si applicano le medesime regole previste per i dispositivi informatici (prgf. 5.2).

5.4.3 Al fine di garantire un corretto utilizzo dei servizi di telefonia (*VoIP*, *mobile*, etc.) l'Ente predispone, ove tecnicamente possibile, adeguate configurazioni dei sistemi che consentano l'effettuazione o meno delle diverse tipologie di chiamata (es. chiamate su telefonini, internazionali, etc.).

5.4.4 Per motivi di sicurezza del sistema telefonico, per motivi tecnici e/o manutentivi e programmazione dei costi (comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa) in merito all'accesso ai dati trattati dall'utente - è facoltà dell'Ufficio Patrimonio e/o Informatica, tramite l'Amministratore del Sistema, accedere direttamente, nel rispetto della normativa sulla protezione dei dati, a tutti gli strumenti di telecomunicazione aziendali.

5.4.5 Sugli *smartphone* ed i *tablet* dell'Ente è vietata l'installazione e l'utilizzo di applicazioni (o altresì denominate "*app*" nel contesto degli smartphone) diverse da quelle autorizzate dall'Ufficio Sistemi Informativi.

5.4.6 Nei periodi di assenza, ogni operatore avrà cura di deviare la propria linea telefonica fissa su altra terminazione, regolarmente presidiata, dell'ufficio/servizio di appartenenza.

5.4.7 È vietato l'utilizzo improprio delle fotocopiatrici dell'Ente; in particolare, è vietato l'utilizzo delle fotocopiatrici per fini personali.

5.4.8 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;
- evitare di stampare la corrispondenza digitale già registrata nel Protocollo Informatico, strumento conforme alle regole del CAD (Codice Amministrazione Digitale) anche per quanto inerente alla conservazione sostitutiva.

5.4.9 Le stampanti e le fotocopiatrici di scrivania devono essere spente ogni sera prima di lasciare gli uffici o in caso di inutilizzo prolungato.

5.4.10 Nel caso in cui si rendesse necessaria la stampa di informazioni riservate, il dipendente/collaboratore dovrà presidiare il dispositivo di stampa per evitare la possibile perdita o divulgazione di tali informazioni e persone terze non autorizzate.

5.4.11 Tutti i documenti acquisiti tramite scanner/fotocopiatore, devono essere immediatamente rimossi, o cancellati, dalla relativa cartella condivisa, nello stretto tempo necessario al raggiungimento della propria postazione di lavoro a cura dell'utente che ha operato la scansione. Tutti i file che rimarranno depositati nella cartella condivisa, esaurite le loro finalità, verranno cancellati dal personale coinvolto nel loro trattamento.

5.4.12 L'utilizzo del *fax* deve intendersi come sistema di comunicazione residuale, limitatamente nei confronti di entità privatistiche, essendo obbligatorio l'utilizzo della comunicazione digitale nei rapporti tra Pubbliche Amministrazioni.

5.5 Utilizzo delle memorie esterne

Agli Utenti può essere assegnata una memoria esterna (quali *pendrive* USB, *hard disk* esterno, *memory card*, etc.) su cui copiare temporaneamente dei dati per un facile trasporto, o altri usi (ad es. macchine fotografiche con *memory card*). Questi dispositivi devono essere gestiti con le stesse accortezze di cui alla sez. 5.2 del presente Manuale e devono essere utilizzati esclusivamente dalle persone a cui sono state affidate e, in nessun caso, devono essere consegnate a terzi.

5.6 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. Ciascun dipendente/collaboratore si deve attenere alle seguenti regole di utilizzo dell'indirizzo di posta elettronica, come di seguito specificato.

5.6.1 Ad ogni utente viene fornito un account *e-mail* dell'Ente nominativo, generalmente coerente con il modello n.cognome@comune.tavagnacco.ud.it oppure nome.cognome@comune.tavagnacco.ud.it e l'utilizzo dell'*e-mail* deve essere limitato prevalentemente a scopi dell'Ente evitando ogni eccesso nell'utilizzo. L'utente a cui è assegnata una casella di posta elettronica è responsabile del corretto utilizzo della stessa.

5.6.2 L'Ente fornisce, altresì, delle caselle di posta elettronica associate a ciascuna unità organizzativa, ufficio o gruppo di lavoro (coerenti con il modello ufficio@comune.tavagnacco.ud.it) il cui utilizzo è da preferire rispetto alle *e-mail* nominative qualora le comunicazioni siano di interesse collettivo: questo per evitare che degli utenti singoli mantengano l'esclusività su dati dell'Ente. Il Responsabile dell'Unità Operativa di riferimento individua almeno un operatore, per ciascuna di tali caselle, da abilitare alla loro gestione; operatori che saranno abilitati dal Sistema Informativo Comunale, tramite Insiel Spa, ad accedere a tale casella, con le stesse credenziali utilizzate per l'accesso alla *e-mail* personale fornita dall'Ente tramite Insiel Spa. Ogni casella di posta elettronica deve essere configurata in modo che, in calce ad ogni messaggio, siano sempre riportate le generalità del mittente, il ruolo, il servizio/ufficio e l'Amministrazione di appartenenza, i recapiti telefonici fissi e cellulari (di servizio), *fax* ed *e- mail*.

5.6.3 L'accesso alla casella generale dell'Ufficio è consentito, attraverso l'uso delle proprie credenziali che permettono già l'accesso alla propria casella *e-mail*, al personale

autorizzato dal responsabile dell'Unità Operativa e comunicato preventivamente all'Ufficio Sistemi Informativi che provvederà ad attivare la relativa abilitazione. In caso di variazioni, il responsabile dell'Unità Operativa è obbligato a darne comunicazione immediata all'Ufficio Sistemi Informativi che provvederà in merito.

5.6.4 La casella di Posta Elettronica Certificata istituzionale dell'Ente è integrata nel Protocollo Informatico del Comune di Tavagnacco.

5.6.5 L'iscrizione 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.

5.6.6 Allo scopo di garantire sicurezza alla rete dell'Ente, è assolutamente vietato aprire messaggi di posta in arrivo da mittenti di cui non si conosce l'identità, oppure si sospetta della genuinità della stessa, o con contenuto sospetto o insolito, oppure che contengano allegati di tipo *.exe, *.com, *.vbs, *.htm, *.scr, *.bat, *.js , *.pif ed altre estensioni. È necessario porre molta attenzione, inoltre, alla credibilità del messaggio e del mittente per evitare casi di *phishing* o frodi informatiche. In qualunque situazione di incertezza è fatto obbligo di contattare l'Amministratore di Sistema o l'Ufficio Sistemi Informativi per una valutazione dei singoli casi.

5.6.7 Non è 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 e i messaggi che informano dell'esistenza di nuovi virus. In generale è vietato l'invio di messaggi pubblicitari di prodotti di qualsiasi tipo.

5.6.8 Nel caso fosse necessario inviare allegati "pesanti" è opportuno ricorrere prima alla compressione dei file originali in un archivio di formato .*zip* o equivalenti. Nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati personali o dati personali particolari, è obbligatorio che questi allegati vengano preventivamente resi inintelligibili attraverso crittazione con apposito *software*. La password deve essere sufficientemente complessa ed essere composta da almeno 14 caratteri. La modalità di trasferimento del materiale, qualora non sia possibile via posta elettronica, avverrà con strumenti di scambio, secondo consiglio da parte del personale dei Sistemi Informativi. Tutte le informazioni dell'Ente, i dati personali e/o particolari di competenza dell'Ente possono essere inviati soltanto a destinatari – persone o Enti – qualificati e competenti.

5.6.9 Non è consentito, di norma, 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 (ad es. ferie, malattia, infortunio). In questa ultima ipotesi, sull'account *e-mail* dell'Ente nominativo, dovrà essere inserito un messaggio di cortesia "*Out of Office*", facendo menzione di chi o quale struttura, all'interno dell'Ente, assumerà le mansioni durante l'assenza ed indicando almeno un indirizzo e-mail alternativo di tipo collettivo, tipo ufficio@comune.tavagnacco.ud.it. L'invio automatico di *e-mail* all'indirizzo *e-mail* privato (attivando per esempio un "inoltro" automatico delle e-mail entranti) è consentito esclusivamente sulle caselle *e-mail* fornite agli Amministratori dell'Ente (Assessori e Consiglieri Comunali), con attivazione da richiedere all'Ufficio Sistemi Informativi.

5.6.10 La casella di posta elettronica personale deve essere mantenuta in ordine, cancellando messaggi e documenti la cui conservazione non è più necessaria. La conservazione di messaggi con allegati è da evitare per quanto possibile, provvedendo al tempestivo salvataggio dell'allegato sulle condivisioni dell'Ente.

5.6.11 La diffusione massiva di messaggi di posta elettronica deve essere effettuata esclusivamente per motivi inerenti al servizio, possibilmente su autorizzazione del

Responsabile dell'Unità Operativa 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.

5.6.12 È vietato inviare posta elettronica in nome e per conto di un altro utente.

5.6.13 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 e-mail (ad es. via lettera o telefono) e mai assieme ai dati criptati. Tutte le informazioni, i dati personali e/o sensibili di competenza le possono essere inviati soltanto a destinatari, persone o Enti qualificati e competenti.

5.6.14 In caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, qualora non fosse possibile attivare la funzione *autoreply* o l'inoltro automatico su altre caselle e si debba conoscere il contenuto dei messaggi di posta elettronica, il titolare della casella di posta ha la facoltà di delegare un altro dipendente (fiduciario) 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 Responsabile assicurarsi che sia redatto un verbale attestante quanto avvenuto e che si sia informato il lavoratore interessato alla prima occasione utile.

5.6.15 È concesso in via eccezionale l'accesso alla propria casella di posta elettronica privata per il solo tempo necessario alla sua consultazione, ferma restando ogni e qualsivoglia responsabilità in capo al dipendente circa le ricadute che tale atto potrebbe cagionare al sistema informativo comunale secondo i principi già espressi nel presente Manuale.

5.6.16 Qualora per intrattenere rapporti con gli utenti, aziende etc. sia utilizzata in fase interlocutoria la propria *e-mail* personale fornita dall'Ente, dovrà essere specificato a chiare lettere che l'invio della corrispondenza ufficiale indirizzata all'Ente ed oggetto di protocollazione dovrà essere trasmessa solo ed esclusivamente all'indirizzo: tavagnacco@postemailcertificata.it, senza doppi passaggi.

Si informa che, ai sensi della Normativa sull'Archiviazione e Conservazione degli Atti Amministrativi, dell'articolo 2214 del Codice Civile e dell'articolo 22 del DPR 600/73, per ottemperare legittime istanze di accesso agli atti ai sensi della L. 241/90 o accesso civico generalizzato (D. Lgs 33/13) l'Ente deve conservare per dieci anni sui propri server di posta elettronica tutti i messaggi di posta elettronica aventi rilevanza istruttoria o inerenti all'attività procedimentale e contrattuale.

Si informa altresì che l'Ente, per il tramite dell'Amministratore di Sistema, 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, l'Ente per il tramite dell'Amministratore di Sistema può, secondo le procedure indicate successiva sezione 9 del presente Manuale, accedere all'*account* di posta elettronica, prendendo visione dei messaggi, salvando o cancellando file.

Si informa che, in caso di cessazione del rapporto lavorativo, la *e-mail* affidata all'incaricato verrà sospesa per un periodo massimo di 3 mesi e successivamente disattivata. Nel periodo

di sospensione l'account rimarrà attivo e visibile ad un soggetto incaricato dall'Ente solo in ricezione, che tratterà i dati e le informazioni pervenute per esigenze organizzative e produttive (ad esempio per non perdere comunicazioni relative a procedimenti in essere, a richieste inerenti l'ufficio o l'ente, istanze, dichiarazioni ecc.), per la sicurezza del lavoro e per la tutela del patrimonio, trasmettendone il contenuto ad altri dipendenti (se il messaggio ha contenuto lavorativo) ovvero cancellandolo (se il messaggio non ha contenuto lavorativo). Il soggetto incaricato non risponderà mai usando l'*account* sospeso e il sistema in ogni caso genererà una risposta automatica al mittente, invitandolo a rinviare il messaggio ad altro indirizzo *e-mail*.

A richiesta scritta del dipendente, verrà messo a sua disposizione l'*account* sospeso per permettere l'estrazione di eventuali contenuti che, nonostante l'espresso ed esplicito divieto di uso dello strumento per finalità diverse da quelle lavorative, dovessero essere presenti.

In ogni caso si informa che il contenuto della *mailbox* oggetto di sospensione potrà essere trattato dall'Ente, per il tramite dell'Amministratore di sistema, per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio. Le informazioni così raccolte saranno 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 Regulation*".

5.7 Partecipazione ai Social Media

5.7.1 L'utilizzo a fini promozionali dei *social media* (ad es. Facebook, Telegram), dei *blog*, dei *forum* anche professionali 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.

5.7.2 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 *partner*, oltre che gli stessi utenti utilizzatori dei *social media*. Maggiori dettagli sono contenuti nel "Disciplinare per l'utilizzo dei profili dei social network del Comune di Tavagnacco".

5.7.3 Il presente articolo deve essere osservato dal dipendente/collaboratore 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.

5.7.4 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*.

5.7.5 La condivisione dei contenuti nei *social media* deve sempre rispettare e garantire la segretezza sulle informazioni considerate dall'Ente riservate ed in genere, a titolo esemplificativo e non esaustivo, sulle informazioni inerenti attività, dati contabili, finanziari, progetti, procedimenti svolti o in svolgimento presso gli uffici. Inoltre, ogni comunicazione e divulgazione di contenuti dovrà essere effettuata nel pieno rispetto dei diritti di proprietà industriale e dei diritti d'autore, sia di terzi sia dell'Ente. Il dipendente/collaboratore non potrà quindi inserire nelle proprie comunicazioni il nominativo e il logo dell'Ente, né potrà pubblicare disegni, modelli od altro connesso ai

citati diritti. Ogni deroga a quanto sopra disposto potrà peraltro avvenire solo previa specifica autorizzazione della Direzione.

5.7.6 Il dipendente/collaboratore deve garantire la tutela della riservatezza e dignità delle persone; di conseguenza, non potrà comunicare o diffondere dati personali (quali ad es. dati anagrafici, immagini, video, suoni e voci di colleghi e in genere di collaboratori), se non con il preventivo personale consenso di questi, e comunque non potrà postare nei *social media* immagini, video, suoni e voci registrati all'interno dei luoghi di lavoro, se non con il preventivo consenso del Responsabile d'ufficio.

5.7.7 Qualora il dipendente/collaboratore intenda usare *social network*, *blog*, *forum* su questioni anche indirettamente professionali (ad es. post su prodotti, servizi, fornitori, partner), egli esprimerà unicamente le proprie opinioni personali; pertanto, ove necessario od opportuno per la possibile connessione con l'Ente, in particolare in forum professionali, il dipendente/collaboratore dovrà precisare che le opinioni espresse sono esclusivamente personali e non riconducibili all'Ente.

5.8 Modifiche delle risorse ICT

Per quanto riguarda le modifiche si devono distinguere:

a) modifiche *hardware* dei dispositivi informatici dell'Ente: gli Utenti non devono intervenire sui dispositivi, togliendo, sostituendo od installando componenti *hardware* (masterizzatori *CD/DVD*, schede *LAN*, etc.) senza eccezione alcuna;
b) modifiche *software*: gli utenti non devono modificare i parametri di configurazione dei dispositivi assegnati, salvo che ciò avvenga su precisa autorizzazione dell'Amministratore di Sistema. Sono fatte salve le personalizzazioni a livello utente che non abbiano conseguenze impattanti sulla funzionalità dei dispositivi stessi. Gli Utenti, inoltre, non devono alterare la configurazione originaria del dispositivo ricevuto in uso (ad es. disinstallando, eseguendo o installando applicazioni che interferiscano sul funzionamento del dispositivo medesimo) senza autorizzazione dell'Amministratore di Sistema.

6 6. ASSISTENZA AGLI UTENTI E MANUTENZIONI

6.4 Interventi di assistenza

L'Ufficio Sistemi Informativi e l'Amministratore 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*.

6.4.1 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, l'Amministratore di Sistema ed il personale dell'Ufficio Sistemi Informativi sono autorizzati ad effettuare gli interventi senza il consenso dell'utente cui la risorsa è assegnata.

6.4.2 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.

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

6.5 Protezione Anti-Virus

I virus (o più in generale qualsiasi *software* malevolo) possono essere trasmessi tramite scambio di file via *internet*, via *e-mail*, scambio di supporti removibili, *file-sharing*, *chat*, etc.

L'Ente impone su tutte le postazioni di lavoro (fisse e mobili) l'utilizzo di un sistema *antivirus* correttamente installato, attivato e continuamente aggiornato automaticamente con frequenza almeno quotidiana.

L'utente, da parte sua, deve impegnarsi a controllare il corretto funzionamento e aggiornamento del sistema antivirus installato sul proprio computer e, in particolare, deve rispettare le regole seguenti:

- comunicare all'Amministratore di Sistema ogni anomalia o malfunzionamento del sistema antivirus;
- comunicare all' Amministratore di Sistema eventuali segnalazioni di presenza di virus o file sospetti.

Inoltre, all'utente:

- è vietato accedere alla rete aziendale senza servizio antivirus attivo e aggiornato sulla propria postazione;
- è vietato ostacolare l'azione dell'antivirus aziendale;
- è vietato disattivare l'antivirus senza l'autorizzazione espressa dell'Amministratore di Sistema, anche e soprattutto nel caso sia richiesto per l'installazione di *software* sul *computer*.

6.6 Ricezione istanze esercizio diritti ex art. 15 e seguenti GDPR

6.6.1 L'interessato può esercitare in qualunque momento i diritti previsti agli artt. 15 e seguenti del GDPR, ovvero il diritto di accesso, il diritto di rettifica, il diritto all'oblio, il diritto di limitazione e il diritto alla portabilità.

6.6.2 Qualora il dipendente/collaboratore riceva una specifica istanza di esercizio da parte dell'interessato dovrà tempestivamente informare il proprio responsabile/referente mettendo successivamente a disposizione dell'istante l'apposito modulo per esercitare i diritti (reperibile all'interno del sito web istituzionale o presso gli uffici amministrativi).

7 CONSERVAZIONE DEI DATI

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

Costituiscono eccezioni esigenze tecniche o di sicurezza o l'indispensabilità dei dati rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria o l'obbligo di custodire e di consegnare i dati per ottemperare ad una specifica richiesta dell'Autorità Giudiziaria o della Polizia Giudiziaria.

In questi casi il trattamento dei dati personali è limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati. Inoltre è consentito il prolungamento dei tempi di conservazione limitatamente al soddisfacimento delle esigenze sopra-esplicitate.
L'Ente si impegna ad applicare le misure di sicurezza nel trattamento e nella conservazione di tale tipologia di dati alla luce di quanto stabilito dal Legislatore.

8 PUBBLICAZIONE CONTENUTI SU SITO WEB ISTITUZIONALE

Nella pubblicazione di dati, atti e informazioni sul sito web istituzionale (Albo Pretorio, Amministrazione Trasparente, etc.) ai sensi della normativa sulla trasparenza o sulla pubblicità degli atti, gli incaricati sono informati:

- che è sempre vietata la pubblicazione di dati sanitari o particolari;
- che la pubblicazione di dati personali identificativi è lecita solo se prevista da norma di legge o regolamento;
- che se anche una norma prevede la pubblicazione di un atto, ciò non autorizza a pubblicare una copia identica all'originale detenuto dall'ufficio perché prevale il principio di minimizzazione e necessità previsto dal GDPR.

Il Titolare, pertanto, fornisce agli addetti le seguenti indicazioni per la corretta pubblicazione di atti:

1) per i provvedimenti collegiali e monocratici ed ogni altro atto oggetto di pubblicazione all'Albo Pretorio si raccomanda di creare una Copia per la Pubblicazione, seguendo le istruzioni qui riportate:

- per atti che, in riferimento a persone fisiche, non contengono direttamente o indirettamente informazioni idonee a rivelare lo stato di salute, la vita sessuale, l'origine razziale od etnica, le condizioni religiose, filosofiche le opinioni politiche, condizioni socio economiche, stato lavorativo, la minore età, lo stato di morosità o ritardo di pagamenti, informazioni su procedimenti sanzionatori o limitativi di diritti, il fatto di non aver superato una prova selettiva o altra informazione di cui – se fossi tu al posto di quel cittadino – non saresti contento di vedere *online*, si consiglia di lasciare leggibili solo dati personali identificativi indispensabili (cioè nome cognome e solo eventualmente in caso di rischio omonimia la data di nascita) oscurando dati eccedenti quali Codice Fiscale, titolo di studio, impiego, indirizzo di residenza, data e luogo di nascita, dati finanziari, IBAN, punteggio analitico in caso di concorsi e altre informazioni sulla persona);
- qualora invece l'atto contenga le informazioni sensibili sopra descritte, è necessario togliere sempre ogni riferimento identificativo delle persone fisiche, adottando tecniche di oscuramento dei dati nella Copia per la Pubblicazione oppure riportando i dati identificativi e ogni altra informazione identificativa in un allegato, da tenere distinto dalla determina o dall'atto (cui si potrà fare riferimento) che poi non sarà soggetto a pubblicazione.

2) Per le pubblicazioni in Amministrazione Trasparente si invita ad effettuare le pubblicazioni limitandosi a quelle previste dal D. Lgs 33/13 come esplicitate nell'allegato 1 alla delibera ANAC n. 1310/2016, attenendosi a quanto sopra descritto per le pubblicazioni all'Albo *online*. Si raccomanda in ogni caso di omettere o oscurare sempre:

a) copia di documenti di identità, immagine della grafia delle sottoscrizioni di atti, Codice Fiscale, titolo di studio, impiego, indirizzo di residenza, data e luogo di nascita, dati finanziari, IBAN, punteggio analitico in caso di concorsi e altre informazioni sulla persona fisica;

b) le ditte individuali sono considerate persone fisiche ai fini privacy, quindi, vale quanto detto sopra per le persone fisiche, salvi gli obblighi di pubblicazione degli atti nelle procedure di gara;
c) i dati bancari non vanno mai indicati nel testo dell'atto ma vanno riportati in un allegato da tenere distinto dalla determina (cui quest'ultima potrà fare riferimento) che poi non sarà soggetto a pubblicazione.

Si consiglia di inserire nella richiesta di curriculum ovvero nelle altre dichiarazioni oggetto di pubblicazione (incompatibilità/inconferibilità, dichiarazione cariche incarichi, etc.) la seguente dicitura o analoga:

"*Si informa che il Curriculum Vitae / dichiarazione XXX richiestoLe con la presente nota è soggetto alla pubblicazione online obbligatoria nella sezione "Amministrazione Trasparente" del sito web istituzionale, ai sensi del D.lgs 33/13. Si invita pertanto a rimuovere preventivamente ogni dato non necessario alla mera identificazione (es. numeri di telefono privati, Codice Fiscale, indirizzo di residenza ecc.) e, in caso di Curriculum, ogni altra informazione ritenuta eccedente rispetto la finalità di comprovare competenze ed esperienze relative all'incarico. Consapevole di quanto sopra, il partecipante autorizza l'ente alla pubblicazione del Curriculum inviato. Si rammenta che il Curriculum rimarrà pubblicato per i tre anni successivi alla cessazione dell'incarico e che, durante tale periodo, non è possibile richiedere l'integrazione o l'aggiornamento del Curriculum fornito*."

9 CONTROLLI

L'Ente, in qualità di Titolare dei dati trattati dagli Utenti nonché Titolare degli Strumenti Informatici e dei dati ivi contenuti e/o trattati, si riserva la facoltà di effettuare i controlli che ritiene opportuni per le seguenti finalità:

- tutelare la sicurezza e preservare l'integrità degli strumenti informatici e dei dati;
- evitare la commissione di illeciti o per esigenze di carattere difensivo anche preventivo;
- verificare la funzionalità del sistema e degli strumenti informatici.

Si precisa, in ogni caso, che l'Ente non adotta "apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori" (ex art. 4, c.1, L. 300/1970), tra cui sono certamente comprese le strumentazioni *hardware* e *software* mirate al controllo dell'utente. In applicazione del principio di necessità di cui all'art. 3 del D. Lgs 196/03 e ssmmii, l'Ente promuove ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri e, comunque, a "minimizzare" l'uso di dati riferibili agli Utenti e allo scopo ha adottato idonei strumenti, organizzativi e fisici, volti a prevenire trattamenti illeciti sui dati trattati con strumenti informatici. L'Ente informa di non adottare sistemi che determinano interferenza ingiustificata sui diritti e sulle libertà fondamentali dei lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata. In particolare, eventuali sistemi atti a monitorare possibili violazioni di legge o comportamenti anomali da parte degli utenti operano nel rispetto del principio di pertinenza e non eccedenza, con esclusione di registrazioni o verifiche con modalità sistematiche. Qualora nell'ambito di tali verifiche si dovesse rilevare un evento dannoso, una situazione di pericolo o qualche altra modalità non conforme all'attività lavorativa (ad es. scarico di file pirata, navigazioni da cui sia derivato il *download* di *virus* informatici) si effettuerà un avvertimento in forma generalizzata, con l'invito ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.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 è tenuto a vigilare sul rispetto delle direttive contenute nel presente Manuale (art. 6.1 Provv.

Garante, ad integrazione dell'Informativa ex art. 13 Reg. 679/16). L'Amministratore di Sistema provvederà quindi alla verifica delle eventuali anomalie riscontrate sul sistema informativo comunale provvedendo in merito, nei limiti consentiti dalle norme legali e contrattuali. 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. Le verifiche devono essere effettuate nel rispetto del Regolamento UE 2016/679 e del presente Manuale 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 Manuale 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.

Si evidenzia che l'uso degli Strumenti Informatici dell'Ente può lasciare traccia delle informazioni sul relativo uso. Tali informazioni, che possono contenere dati personali eventualmente anche particolari dell'utente, possono essere oggetto di accesso da parte dell'Amministratore di Sistema per motivazioni esclusivamente volte a garantire la sicurezza immediata e l'inviolabilità dei sistemi informativi comunali. Lo stesso Amministratore di Sistema eventualmente si farà carico di comunicare, se ritenuto prioritario, al Segretario Comunale, le difformità riscontrate.

9.1 Controlli per la tutela del patrimonio, nonché per la sicurezza e per la salvaguardia del sistema informatico

Qualora per le finalità qui sopra descritte risulti necessario l'accesso agli Strumenti e alle risorse informatiche, l'Amministratore di Sistema si atterrà al processo descritto qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo):

- 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;
- se il comportamento anomalo persiste, per almeno i successivi 7 giorni, l'Ente potrà autorizzare il personale addetto al controllo, con possibilità di rilevare file 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 del numero IP, dell'utente e con l'identificazione del soggetto che non si attiene alle istruzioni impartite;
- qualora il rischio di compromissione del sistema informativo sia imminente e grave a tal punto da non permettere l'attesa dei tempi necessari per i passaggi procedimentali descritti ai punti qui sopra, l'Amministratore di Sistema potrà intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia.

9.2 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 file o informazioni lavorative di cui si è ragionevolmente certi che siano disponibili su risorse informatiche di un dipendente/collaboratore (quali file salvati, posta elettronica,

chat, *SMS*, etc.) che non sia reperibile, in quanto ad esempio assente, temporaneamente irreperibile ovvero cessato.
Qualora risulti necessario l'accesso alle risorse informatiche, l'Amministratore di Sistema si atterrà alla procedura descritta qui di seguito (se e in quanto compatibile con lo Strumento oggetto di controllo):

- redazione di un atto da parte Responsabile di Area che comprovi le necessità produttive e di organizzazione che richiedano l'accesso allo Strumento;
- 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 del dipendente/collaboratore interessato, con avviso che al primo accesso alla risorsa, lo stesso dovrà inserire nuove credenziali;
- redazione di un verbale che riassuma i passaggi precedenti;
- in ogni caso l'accesso ai documenti presenti nella risorsa è limitato a quanto strettamente indispensabile alle finalità produttive e di organizzazione del lavoro;
- 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 Regulation*".

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 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 Regulation*".

10 VIOLAZIONI E SANZIONI DISCIPLINARI

È fatto obbligo a tutti i dipendenti/collaboratori/utenti di osservare le disposizioni portate a conoscenza con il presente Manuale. Qualsiasi utilizzo non conforme alle disposizioni del presente Manuale e/o alle leggi vigenti è ad esclusiva responsabilità dell'utente. Nonostante l'Amministrazione Comunale non intenda monitorare l'utilizzo degli Strumenti e della rete da parte dell'utente di postazione, si riserva il diritto di monitorare e verificare, nel pieno rispetto della normativa vigente in tema di *privacy*, l'attuazione delle disposizioni del presente documento. L'eventuale violazione delle norme e/o delle buone regole di comportamento può comportare l'applicazione in capo ai contravventori di sanzioni di tipo civile, penale e/o disciplinare.

11 NORME FINALI

La sicurezza dei dati e delle informazioni è legata anche alla qualità della sicurezza fisica. È preciso dovere di ciascuno, secondo le proprie funzioni e le relative responsabilità, fare in modo che vengano utilizzati scrupolosamente tutti gli accorgimenti atti ad evitare indebite intrusioni negli edifici comunali (ad es. manutenzione e controllo dell'impianto di allarme, chiusura a chiave dei contenitori e dei luoghi ove vengono conservati dati e attrezzature, posizionamento di estintori). È considerata negligenza, e trattata nei modi previsti dalla normativa vigente, anche la mancata segnalazione di eventuali anomalie casualmente riscontrate da parte di chiunque ne venga a conoscenza.

12 ENTRATA IN VIGORE

Il presente Manuale sarà operativo ed efficace per tutti gli interessati a partire dall'esecutività della deliberazione della Giunta Comunale di approvazione.

13 PUBBLICAZIONE E MESSA A DISPOSIZIONE

Copia del presente Manuale sarà trasmesso per opportuna conoscenza al Segretario Comunale ed agli Amministratori, ai Responsabili del Servizio di Prevenzione e Protezione e al Rappresentante dei Lavoratori per la Sicurezza, a tutto il personale comunale e suoi collaboratori, e pubblicato sul sito Istituzionale dell'Ente.

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni e modifiche al presente Regolamento tramite comunicazione all'Amministratore di Sistema.

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: STEFANO SORAMEL
CODICE FISCALE: SRMSFN68E08L483V
DATA FIRMA: 07/11/2022 15:32:55
IMPRONTA: 950635C5C2E8C330CD7084C055B79BBE9E90E85A7D5D5D150E3D57AFDB052C62
9E90E85A7D5D5D150E3D57AFDB052C62CA13E4281208095CE974F0A721D17F83
CA13E4281208095CE974F0A721D17F83C97BA5158A183048A079BAA0E050F210
C97BA5158A183048A079BAA0E050F210A9B3ED8DDE6A50A425E99FBE402A784B