Città di Portogruaro

Città Metropolitana di Venezia

LINEE GUIDA
PER L'UTILIZZO DEI
SISTEMI INFORMATICI
DEL COMUNE DI PORTOGRUARO

Approvato con deliberazione G.C. n. 169 in data 24.11.2021

Indice

PREMESSA

Le presenti Linee Guida intendono fornire ai dipendenti e collaboratori, denominati anche incaricati o utenti, del Comune di Portogruaro 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 precisa 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

Le presenti Linee Guida sono redatte:

- 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 n. 2016/679 sulla protezione dei dati personali (d'ora in avanti Reg. 679/2016 o GDPR);
- ai sensi delle "Linee guida del Garante per posta elettronica e Internet" in Gazzetta Ufficiale n. 58 del 10 marzo 2007;

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.

2. Principi generali e di riservatezza nelle comunicazioni

2.1. I principi che sono a fondamento delle presenti Linee Guida sono gli stessi espressi nel GDPR Reg 679/2016 e, precisamente:

a. il principio di necessità;
b. il principio di correttezza;
c. i trattamenti devono essere effettuati per finalità determinate, esplicite e legittime.

2.2. Il dipendente deve attenersi alle seguenti regole di trattamento:

a. È vietato comunicare a soggetti 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.
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.

3. Tutela del lavoratore

3.1. Alla luce dell'art. 4, comma 1, L. n. 300/1970, la regolamentazione della materia indicata nel punto n. 1 delle presenti Linee Guida 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 i servizi informatici 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

Le presenti Linee Guida si applicano 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 lo stesso intrattenuto.

5. Gestione, assegnazione e revoca delle credenziali di accesso

5.1. Le credenziali di autenticazione per l'accesso alle risorse informatiche vengono assegnate dal personale dell'Ufficio Servizi Informatici, previa formale richiesta del Dirigente nell'ambito del quale verrà inserito ed andrà ad operare il nuovo utente.
5.2. Le credenziali di autenticazioni consistono in un codice per l'identificazione dell'utente (altresì nominati username, nome utente o user id), assegnato dall'Ufficio Servizi Informatici, 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.
5.3. La password deve essere di adeguata robustezza e rispettare i requisiti di complessità.
In particolare le password di accesso ai servizi di rete devono:

a) essere costituite da almeno 8 caratteri;
b) contenere un set di caratteri il più possibile esteso (oltre ai caratteri dell'alfabeto, quelli numerici e quelli speciali ad esempio |!"£$%&/()=?^*+[ç@#°§_-:.;,<>\];
c) non essere banali: cioè reperibili in dizionari on-line, non facilmente associabili alla persona, non essere ripetizione della login o una permutazione ciclica della login, né una stringa di caratteri contigui della tastiera.
d) contenere caratteri maiuscoli e/o minuscoli;
e) essere cambiate dall'operatore subito all'atto della prima assegnazione, evitando il riutilizzo di chiavi già adottate nei 12 mesi precedenti.
E' vietato, altresì, riutilizzare la propria password di accesso ai servizi di rete comunale per la registrazione in altri siti web.

6. Utilizzo della rete del Comune di Portogruaro

6.1. Per l'accesso alle risorse informatiche del Comune di Portogruaro attraverso la rete locale, ciascun utente deve essere in possesso di credenziali di autenticazione secondo quanto specificato all'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 sui 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.
6.4. Il Comune di Portogruaro mette a disposizione di alcuni 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. Per l'eventuale utilizzo di tale modalità l'utente, sul dispositivo da dove si collega, deve aver installato funzionante ed aggiornato adeguato sistema antivirus. Deve, altresì', digitale la password d'accesso ad ogni collegamento evitando la memorizzazione della stessa da parte del sistema.
6.5. L'Ufficio Servizi Informatici 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.

7. Utilizzo degli Strumenti elettronici

(PC, notebook e altri strumenti con relativi software e applicativi)

7.1. Il dipendente/collaboratore è consapevole che gli Strumenti forniti sono di proprietà del Comune di Portogruaro e devono essere utilizzati esclusivamente per la prestazione lavorativa.
7.2. Il Personal Computer, notebook, tablet ed ogni altro hardware deve essere custodito con cura da parte degli assegnatari evitando ogni possibile forma di danneggiamento.
7.3. 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.
7.4. La gestione dei dati su PC è demandata all'utente utilizzatore. Non è consentita l'installazione di programmi diversi da quelli autorizzati dall'Ufficio Servizi Informatici.
7.5. 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.
7.6. È vietato utilizzare il PC per l'acquisizione, la duplicazione e/o la trasmissione illegale di opere protette da copyright.
7.7. È assolutamente vietato connettere al PC qualsiasi periferica non autorizzata preventivamente dall'Amministratore di Sistema.
7.8. È assolutamente vietato connettere alla rete locale qualsiasi dispositivo (PC esterni, router, switch, modem, etc.) non autorizzato preventivamente dall'Amministratore di Sistema.

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.
8.2. È vietato a chiunque il download di qualunque tipo di software gratuito (freeware) o shareware prelevato da siti Internet, se non espressamente autorizzato dall'Amministratore di Sistema.
8.3. L'Ente si riserva di bloccare l'accesso a siti "a rischio" attraverso l'utilizzo di blacklist pubbliche in continuo aggiornamento.
8.4. Nel caso in cui, per ragioni di servizio, si necessiti di una navigazione libera dai filtri firewall e/o proxy, è

necessario richiedere lo sblocco mediante una mail indirizzata all'Ufficio Servizi Informatici
8.5. 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 Responsabile di Area e dall'Ufficio Servizi Informatici, con il rispetto delle normali procedure di acquisto.
8.6. È consentito l'uso di strumenti di messaggistica istantanea, per permettere una efficace e comoda comunicazione tra i colleghi, mediante i soli strumenti autorizzati dall'Ufficio Servizi Informatici.
8.7. 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 Internet disponibile.

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.
Ciascun dipendente/collaboratore si deve 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@comune.portogruaro.ve.it . L'utilizzo dell'e-mail deve essere limitato esclusivamente a scopi dell'Ente.
9.2. 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.
9.3. Nel caso fosse necessario inviare allegati "pesanti" è opportuno ricorrere prima alla compressione dei file originali in un archivio di formato .zip o equivalenti.
9.4. In caso di assenza improvvisa o prolungata e per improrogabili necessità legate all'attività lavorativa, qualora non fosse possibile attivare la funzione autoreply 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.

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

Il dipendente è consapevole che gli Strumenti di stampa e scansione, così come anche il telefono/cellulare dell'Ente, sono di proprietà del Comune di Portogruaro e sono resi disponibili all'utente per rendere la prestazione lavorativa.

11. Controlli sugli Strumenti

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.
12.1. ***Controlli per la tutela del patrimonio dell'Ente, nonché per la sicurezza e la salvaguardia del sistema informatico.***

Qualora per le finalità qui sopra descritte risulti necessario l'accesso agli Strumenti e alle risorse informatiche e relative informazioni descritte il Responsabile del trattamento dei dati personali per il tramite dell'Ufficio Servizi Informatici, si atterrà al processo descritto qui di seguito:

a. 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 delle presenti Linee Guida.
b. Qualora il rischio di compromissione del sistema informativo dell'Ente sia imminente e grave il Responsabile del Trattamento, per il tramite dell'Amministratore di Sistema, può intervenire senza indugio sullo strumento da cui proviene la potenziale minaccia.

12 . Conservazione dei dati

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 ed al traffico telematico (log di sistema, firewall e server proxy), la cui conservazione non sia necessaria, saranno cancellati dopo 12 mesi, salvo esigenze tecniche o di sicurezza.
13.2. L'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.

13. Obblighi

È fatto obbligo a tutti i dipendenti/collaboratori/utenti di osservare le disposizioni portate a conoscenza con le presenti Linee Guida.

14. Entrata in vigore del Regolamento e pubblicità

15.1. Con l'entrata in vigore del presente Regolamento tutte le norme e le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.

15.2. Copia del Regolamento, oltre ad essere affisso nella bacheche dell'Ente, è pubblicato nel sito Web.