Manuale operativo per il corretto utilizzo dei dispositivi informatici, posta elettronica e trattamento degli archivi cartacei

Tabella di revisione

Rev. n.	Data emissione	Descrizione delle modifiche	Approvato del titolare del trattamento
0		Prima emissione	
1			
2			
3			
4			
5			

La riproduzione del presente documento è vietata senza la preventiva autorizzazione dell'ENTE PROVINCIA DI MANTOVA

Premessa

1. La progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai dispositivi (PC, notebook, tablet, smartphone, ecc), espone l'ente Provincia ai rischi di un coinvolgimento sia patrimoniale sia penale, creando problemi alla sicurezza e all'immagine dell'Ente stesso.
2. La Provincia adotta un manuale operativo volto a diffondere una maggiore consapevolezza circa l'utilizzo di tali risorse ed archivi ed evitare che vengano assunti comportamenti che possano innescare problemi o minacce alla sicurezza nel trattamento dei dati
3. La disciplina introdotta con il presente manuale operativo ha il fine di:
   - ✓ garantire il diritto del lavoratore/utente ad usare liberamente le tecnologie messe a disposizione (anche come strumento di crescita professionale) contemperando il diritto al pieno rispetto della propria riservatezza;
   - ✓ prevenire usi impropri degli strumenti dell'Ente messi a disposizione dei dipendenti durante l'orario di lavoro;
   - ✓ adeguare i comportamenti dei dipendenti alla normativa in materia di tutela dei dati personali nel rispetto del Regolamento EU 679/2016, di seguito GDPR, ed in particolare degli artt. 29, 32 che prescrivono al Titolare del trattamento di istruire gli Addetti al trattamento e applicare le misure di sicurezza necessarie alla tutela dei dati personali.

Definizioni

1. Al fine di poter operare nell'ambito del trattamento dei dati, occorre conoscere la terminologia e le definizioni introdotte dal GDPR, dal codice in materia di protezione dei dati personali adottato con decreto legislativo 30 giugno 2003, n. 196, "codice in materia di protezione dei dati personali" aggiornato dal decreto legislativo 10 agosto 2018, n. 101, e dal presente manuale operativo. Nello specifico, s'intende per:

a) "**trattamento**" qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, la strutturazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
b) "**dato personale**" qualunque informazione riguardante una persona fisica indentificata o identificabile; si considera identificabile la persona fisica che può essere riconosciuta, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
c) "**categorie particolari di dati**" i dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, dati biometrici atti a identificare in modo univoco una persona fisica, questa tipologia di dato è definito dall'Art. 9 del GDPR;
d) "**dati giudiziari**": informazioni in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale; questa tipologia di dato è definito dall'Art. 10 del GDPR;
e) "**dati che presentano rischi specifici**": si tratta di dati che, pur non essendo così delicati come quelli sensibili e giudiziari, presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati, ovvero alle modalità di trattamento o agli effetti che esso può determinare: in considerazione di tale fatto, il loro trattamento è ammesso nel rispetto delle misure e degli accorgimenti, prescritti dal Garante a garanzia dei soggetti interessati. In questa categoria di dati possono ricadere ad esempio le informazioni relative alla capacità di solvibilità del debito, dati biometrici, dati di geolocalizzazione, immagini riprese da impianti di videosorveglianza, ecc.

f) "**Titolare del trattamento**" la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

g) "**Responsabile per la protezione dei dati**" figura specializzata nel supporto al Titolare del trattamento prevista come obbligatoria negli enti pubblici;

h) **"Direzione"** il vertice della struttura organizzativa dell'Ente che, per quanto disciplinato dal presente regolamento, agisce tramite il Servizio Sistemi Informativi innovazione e sviluppo.

i) **"Soggetti addetti al trattamento di dati"** si intendono "le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile" in base alla definizione di cui all'art. 29 del GDPR.

l) "**Coordinatori degli addetti al trattamento e addetti al trattamento di primo livello"**
In base al sistema organizzativo adottato dalla Provincia di Mantova, il Dirigenti sono addetti al trattamento di primo livello e coordinatori degli addetti al trattamento dell'Area di competenza.

Istruzioni e raccomandazioni

1. I dispositivi informatici (personal computer fissi, portatili, tablet, smartphones, stampanti multifunzione: fotocopiatrice, scanner, fax; ecc..) ed i relativi programmi e/o applicazioni affidati al dipendente sono, strumenti di lavoro, il cui utilizzo ricade sotto la responsabilità del Titolare e che possono contenere dati riservati e informazioni personali di terzi.
2. Detti dispositivi vanno custoditi in modo appropriato evitando manomissioni, danneggiamenti o utilizzi, anche da parte di altre persone e possono essere utilizzati solo per fini professionali attinenti esclusivamente alle mansioni assegnate; vanno evitati usi per fini personali, al di fuori dei casi consentiti ed autorizzati espressamente dai propri responsabili, e utilizzi per scopi illeciti.
3. Debbono essere prontamente segnalati all'Ente il furto, il danneggiamento o lo smarrimento di tali strumenti.
4. Le impostazioni dei dispositivi informatici sono predisposte dagli addetti informatici sulla base di criteri e profili decisi dalla Direzione in funzione della qualifica del dipendente, delle mansioni cui questo è adibito, nonché dalle decisioni e della politica di utilizzo di tali strumenti stabilita dall'Ente stesso.
5. Tutti gli utenti, per il seguito **addetti,** sono tenuti ad attenersi scrupolosamente alle indicazioni sotto riportate.

Utilizzo non consentito dei dispositivi informatici

1. i telefoni ed i fax dell'Ente, non possono essere utilizzati per ricevere o effettuare comunicazioni private; si raccomanda, quindi, l'uso del telefono d'ufficio e del fax per le comunicazioni necessarie allo svolgimento del lavoro, salvo casi eccezionali di oggettiva urgenza e impossibilità ad utilizzare il proprio dispositivo mobile; il dipendente è tenuto a limitare la ricezione di telefonate personali sulle linee telefoniche dell'ufficio, a casi di oggettiva impossibilità alla ricezione su dispositivo mobile personale avendo cura di contenere la durata delle conversazioni al minimo indispensabile;
2. durante l'orario lavorativo, limitare alla gestione delle urgenze o per motivi strettamente eccezionali l'utilizzo di smartphone, tablet, ed altri device privati e in ogni caso mantenerli nella modalità silenziosa per rispetto dei colleghi.
3. gli addetti non devono violare o tentare di violare i sistemi di sicurezza informatici;
4. gli addetti non devono né cercare di ottenere accessi non autorizzati, né favorire analoghe attività da parte di altri utenti, interni o esterni; gli addetti non possono, deliberatamente e in modo non autorizzato, modificare o tentare di modificare dati contenuti nei Sistemi in Rete. Gli addetti non possono intercettare, tentare d'intercettare o accedere a dati in transito sulla rete dell'Ente, che non siano loro diretti;

5. gli addetti non possono mascherare la loro identità quando usano i sistemi della rete dell'Ente. Gli addetti non possono inoltre impersonare altri individui;
6. non è consentito installare programmi provenienti dall'esterno salvo espressa autorizzazione della Direzione; non è consentito scaricare file dalla rete o contenuti in supporti magnetici e/o ottici non aventi alcuna attinenza con la propria prestazione lavorativa;
7. non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici; non è consentita l'installazione sui PC a disposizione, di mezzi di comunicazione propri;
8. tutti i software caricati sul sistema operativo ed in particolare quelli necessari per la protezione dello stesso o della rete internet (quali antivirus o firewall) non possono essere disinstallati o in nessun modo manomessi dagli utenti (salvo quando questo sia richiesto dalla Direzione per compiere attività di manutenzione o aggiornamento);
9. non è consentito condividere file, cartelle, hard disk o porzioni di questi del proprio computer, per accedere a servizi non autorizzati al fine di scaricare materiale elettronico tutelato dalle normative sul Diritto d'Autore (software, file audio, film, etc.);
10. l'uso della Rete dell'Ente in violazione di norme del Codice Civile o Penale è proibito. Esempi di queste violazioni sono: distribuzione di materiale osceno; ricezione, registrazione, trasmissione o possesso d'immagini pornografiche violazione di copyright;
11. ogni utente è tenuto a segnalare con tempestività alla Direzione qualsiasi malfunzionamento degli strumenti informatici in uso;
12. non è consentito procedere autonomamente a tentativi di correzione di errori o malfunzionamenti, se non dietro esplicita autorizzazione della Direzione;
13. non si deve operare sulle connessioni elettriche o di rete, se non specificatamente autorizzati dalla Direzione. In nessun caso si deve operare sulle connessioni elettriche o di rete quando i dispositivi sono in tensione;
14. non è permesso modificare la configurazione del proprio posto di lavoro né dal punto di vista hardware, né dal punto di vista software, senza precedente autorizzazione della Direzione. In particolare non è permesso spostare dispositivi quali unità centrali, unità video o stampanti, scanner, telefoni o fax; non è possibile modificare la configurazione dei personal computer;
15. i dispositivi informatici "stand alone" o in rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo, essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità; l'Ente si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema ovvero acquisiti o installati in violazione delle presenti istruzioni.
16. non è consentito utilizzare stampanti con anche funzioni di copia, scansione e fax o qualsiasi altro strumento messo a disposizione dal Titolare, compresa la cancelleria, per scopi non attinenti all'espletamento delle proprie mansioni nell'Ente.
17. ogni comunicazione scritta (interna ed esterna), inviata o ricevuta attraverso strumenti informatici, scanner, fax, ecc. che riguardi o contenga impegni per l'Ente deve essere visionata e autorizzata dalla Direzione/Dirigente competente.

Utilizzo dei dispositivi mobili

1. L'utente è responsabile di dispositivi mobili (PC portatile, tablet, smartphone, ecc) assegnatigli e deve custodirli con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.
2. Agli stessi si applicano tutte le regole di utilizzo previste per i PC fissi o agli altri dispositivi informatici presenti nell'Ente.
3. I dispositivi mobili utilizzati all'esterno (convegni, fiere, visite, ecc.), in caso di allontanamento, devono essere custoditi in un luogo protetto. In particolare essi non devono mai essere lasciati incustoditi nell'autovettura, neppure all'interno del bagagliaio.
4. In caso di furto o smarrimento è obbligatorio comunicare tempestivamente l'accaduto alla Direzione, effettuare denuncia presso l'ufficio di pubblica sicurezza locale e consegnare copia della stessa all' Ente.

Gestione degli archivi, file, documenti e cartelle

1. Gli archivi, file, documenti e cartelle generati e/o gestiti dagli utenti devono essere memorizzati sui dispositivi di rete. La Direzione garantisce la sicurezza delle informazioni memorizzate sui dispositivi di rete eseguendo periodici backup degli archivi.
2. Non è consentita la copia di archivi dell'Ente di qualsiasi genere o specie né su dispositivi asportabili (CD,DVD, dischi o chiavi USB, tablet, smartphone e simili) né su dispositivi di memorizzazione esterni all'Ente (ad esempio in server accessibili mediante Internet, aree dati in Cloud tipo Dropbox, Google Drive, ecc.), né via posta elettronica su account non appartenenti al dominio dell'Ente, se non dietro esplicita autorizzazione della Direzione.

Utilizzo di Internet

1. La rete internet può e deve essere utilizzata dal dipendente a supporto dell'attività lavorativa nell'ambito delle mansioni ed autorizzazioni assegnategli dal proprio responsabile.

2. Al fine di ridurre il rischio di un utilizzo improprio della rete e allo stesso tempo di evitare, per quanto possibile, controlli che potrebbero comportare il trattamento di dati personali, l'Ente si riserva di adottare l'utilizzo di sistemi e filtri che possono prevenire determinate operazioni, reputate inconferenti con l'attività lavorativa, quali ad esempio l'upload o l'accesso a determinati siti e/o il download di file o software aventi particolari caratteristiche (quali ad esempio dimensionali o di tipologia di dato), con individuazione di categorie e liste di siti cui non è concesso l'accesso (black list), in quanto non attinenti l'attività lavorativa;

3. Di seguito sono riportati i principi che devono essere rispettati al fine di assicurare una navigazione internet sicura:
   a. non è permessa la creazione di siti e di pagine HTML in domini esterni, anche se gratuiti, senza autorizzazione della Direzione;
   b. non è consentito navigare in siti non attinenti allo svolgimento delle mansioni assegnate;
   c. a maggior ragione non è consentito navigare in siti che accolgono contenuti contrari alla morale e alle prescrizioni di Legge;
   d. non è, inoltre, consentito navigare in siti che possano rivelare una profilazione dell'individuo definita 'particolare' ai sensi del GDPR: quindi siti la cui navigazione palesi elementi attinenti alla fede religiosa, alle opinioni politiche e sindacali del dipendente o le sue abitudini sessuali;
   e. non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi direttamente autorizzati dal Titolare/Dirigente delegato, con il rispetto delle normali procedure di acquisto;
   f. non è consentito lo scarico di software gratuiti trial, freeware e shareware prelevati da siti Internet, se non espressamente autorizzato dalla Direzione;
   g. non è consentito lo scarico di materiale elettronico tutelato dalle normative sul Diritto d'Autore (software, file audio, film, etc.) attraverso Internet: web, ftp, servizi di condivisione, ecc.;
   h. non è consentita la memorizzazione di documenti di natura oltraggiosa e/o discriminatoria (a titolo esemplificativo e non esaustivo per sesso, lingua, religione, origine etnica, opinione e appartenenza sindacale e/o politica).
   i. è vietata ogni forma, anche a titolo personale, di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
   j. non è permessa la partecipazione, per motivi non professionali a Forum e giochi in rete pubblica, l'utilizzo di chat line, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (o nicknames). L'accesso a tali fonti di informazione, esclusivamente per motivi professionali, potrà avvenire solo previa autorizzazione scritta da parte della Direzione.

Utilizzo della posta elettronica dell'Ente

1. La posta elettronica, sia interna che esterna, è un mezzo di comunicazione che il Titolare mette a disposizione del dipendente esclusivamente per consentirgli lo svolgimento della propria attività lavorativa, pertanto:
   a. si raccomanda di evitare di utilizzare tali strumenti per motivi non attinenti allo svolgimento delle mansioni assegnate, salvo casi eccezionali di comprovata urgenza e necessità;
   b. non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria (a titolo esemplificativo e non esaustivo per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica);
   c. la posta elettronica diretta all'esterno della rete informatica dell'Ente non deve essere usata per inviare informazioni, dati o documenti di lavoro "Strettamente Riservati";
   d. non è consentito l'utilizzo dell'indirizzo di posta elettronica dell'Ente per la partecipazione a dibattiti, forum o mail-list; che non siano strettamente inerenti all'attività dell'Ente;
   e. non è consentito utilizzare caselle di posta elettronica private per corrispondenza inerente le attività dell'Ente;
   f. è necessario configurare un sistema di risponditore automatico da attivare in caso di prolungata assenza che avvisi il mittente dell'assenza. Si raccomanda di:
      i. inserire un indirizzo mail dell'Ente di un collega che il mittente può contattare in caso di urgenza;
      ii. adottare un testo del tipo "Sarò assente fino al _____ p.v. Per urgenze è possibile inviare una mail all'indirizzo_____ ".

Gestione delle credenziali e password

1. L'accesso ai dispositivi informatici, ai programmi applicativi e alle varie funzionalità messe a disposizione degli utenti per lo svolgimento dell'attività, avviene previa autenticazione, che consiste nella verifica dell'identità del dipendente attraverso l'uso di un codice identificativo e di una parola chiave (password).
2. Le credenziali di autenticazione sono assolutamente personali e non cedibili, per nessuna ragione.
3. E' necessario rispettare l'ambito di competenza (i dati cui poter accedere) ed il profilo di autorizzazione (tipi di trattamento consentito) indicate nella propria nomina ad addetto al trattamento dei dati personali.
4. Elaborare le password seguendo le istruzioni di seguito riportate:
   a. al primo accesso ad un sistema e/o ad una banca dati, l'incaricato ha la responsabilità di cambiare la password assegnatagli dalla Direzione. Tale password deve essere al minimo lunga 8 caratteri, includere sia lettere, sia cifre e una maiuscola;
   b. la password per l'accesso alla rete dell'Ente scade ogni 6 mesi e va obbligatoriamente cambiata;
   c. la password per l'accesso a sistemi e/o banche dati deve essere modificata dall'incaricato almeno ogni 6 mesi, se non altrimenti specificato;
   d. la password non deve contenere elementi che possano in qualche modo essere legati all'incaricato come, ad esempio il suo nome o cognome, quello di sua moglie/marito, del cane, date di nascita, numeri di telefono etc. e non deve contenere le parole "provincia" e "mantova";
   e. la password non deve essere comunicata a nessuno, lo scopo principale del suo utilizzo è assicurare che nessun altro possa accedere alle risorse o sostituirsi all'addetto al trattamento individuato;
   f. l'addetto al trattamento dei dati personali ha la responsabilità di custodire con diligenza la propria password; in nessuna circostanza il dipendente è autorizzato a condividere le proprie credenziali di autenticazione con altri addetti o terze persone;
   g. l'incaricato dovrà informare la Direzione nel caso in cui abbia fondati motivi di ritenere che possa essere compromessa la riservatezza della password, o comunque che ne sia stato fatto un utilizzo indebito cambiandola immediatamente;
   h. l'incaricato può nominare un "fiduciario" che in caso di assenza (temporanea o prolungata) possa accedere ai suoi dispositivi informatici, inclusi i messaggi di posta elettronica in entrata e in uscita, al fine di garantire l'ordinaria operatività dell'Ente o per ragioni di sicurezza. L'addetto al trattamento dei dati sarà prontamente informato dell'avvenuto accesso il prima possibile; sarà fornita adeguata spiegazione e redatto apposito verbale. La password verrà resettata e

l'incaricato invitato a formularne una nuova; i codici identificativi e le password degli addetti saranno disattivate in caso di cessazione del loro rapporto di lavoro.

Custodia dispositivi informatici

1. I dispositivi informatici non possono essere lasciati incustoditi:

   a. In caso di allontanamento anche temporaneo dalla postazione di lavoro o comunque dal dispositivo informatico è necessario non lasciare il sistema aperto con la propria password.
   b. Al fine di evitare che persone estranee effettuino accessi non permessi l'addetto deve eseguire il "Log out" della sessione di lavoro o in alternativa attivare funzioni che, trascorso un breve periodo di tempo predeterminato in cui il dispositivo resta inutilizzato, non consentano più l'accesso al dispositivo se non con inserimento di password.
   c. In particolare i supporti di memorizzazione rimovibili devono essere custoditi ed utilizzati in modo tale da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti: è bene adottare archiviazioni in modo che vengano conservati in cassetti chiusi a chiave, durante il loro utilizzo, e successivamente formattati, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi;
   d. Una volta cessate le ragioni per la conservazione dei dati, i supporti di memorizzazione rimovibili non possono venire abbandonati. Si devono quindi cancellare i dati, se possibile, o distruggere il supporto, se necessario.

Protezione dispositivi informatici

1. L'Ente adotta adeguati ed aggiornati strumenti e metodologie per la protezione dei dispositivi: segmentazione della rete, firewall, antispam, antiphising, endpoint protection (antivirus), web filtering, per i file scaricati da internet, aggiornamenti automatici di sicurezza dei sistemi operativi, backup periodici ecc.
2. L' addetto è, comunque, tenuto ad adottare i seguenti comportamenti per prevenire danni ai sistemi, o ridurne il rischio, dall'esecuzione di software "malevolo":
   a. utilizzare soltanto programmi provenienti da fonti fidate. Copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma deve essere sottoposto alla scansione prima di essere installato. Non utilizzare programmi non autorizzati;
   b. evitare la trasmissione di file eseguibili (.COM, .EXE, .OVL, .OVR) e di sistema (.SYS) tra computer in rete;
   c. impostare in modalità di "sola lettura" le memorie di massa dei dispositivi rimovibili (dischi, chiavette ecc) quando i dispositivi stessi lo permettono. Questa modalità tutela il sistema informativo provinciale dall'accesso e dall'utilizzo da parte di software dannoso;
   d. non trasferire documenti, file, archivi relativi a dati dell'Ente su dispositivi non dell'Ente per essere trattati od utilizzati esternamente alla rete dell'Ente e riportati nella stessa;
   e. non aprire e non diffondere messaggi email di provenienza dubbia o con mittenti sconosciuti o con oggetto non pertinente alle proprie attività con evidenti errori ortografici o contenenti allegati o link poco chiari o dubbi, cancellandoli tempestivamente;
   f. nel caso di apertura di messaggi di tale tipo almeno non aprire gli eventuali allegati o non accedere ai link presenti e provvedere a eliminarli tempestivamente;
   g. in ogni caso, nel dubbio che ci sia in corso un'attività anomala o malevola sul proprio dispositivo **spegnere lo stesso e/o staccare il cavo di rete, ed allertare immediatamente la Direzione** La tempestività nell'azione di bonifica è essenziale per limitare eventuali danni arrecati al dispositvo ed ad altri dispositivi o apparati della rete dell'Ente.

Riservatezza e cautela nella tenuta e comunicazione dei dati

1. Tutte le informazioni dell'Ente possono essere utilizzate e fatte circolare esclusivamente all'interno dell'Ente, tranne nei casi diversi esplicitamente previsti per legge. Anche informazioni di normale quotidianità relative all'Ente o ritenute non riservate nell'ambito delle ordinarie attività fra addetti, assumono diversa importanza, e quindi richiedono una maggiore tutela, se comunicate all'esterno a soggetti terzi. La salvaguardia delle informazioni e dei dati oltre ad essere un requisito fondamentale per la sicurezza del patrimonio informativo dell'Ente, è anche un espresso obbligo di legge nei confronti di qualsiasi soggetto definito "interessato" in particolare se relative a persone fisiche e se attengono a dati sensibili.
2. L'addetto al trattamento dei dati osserva ogni cautela nel trasferire all'esterno qualsiasi informazione in relazione al contenuto e all'attendibilità dell'interlocutore, nel rispetto delle presente manuale operativo .
3. Ogni utente ha accesso unicamente ai dati per i quali è stato autorizzato in relazione allo svolgimento delle mansioni assegnate. Questo si riferisce in generale a tutte le informazioni trattate dal Sistema Informativo dell'Ente, ed in particolare ai dati personali, per i quali l'Ente assicura l'osservanza della normativa di legge in materia.
4. Nessuna informazione deve essere comunicata e diffusa all'esterno dell'Ente, se non esiste una precisa motivazione per farlo. Autorizzazioni generali di comunicazione ad esterni vengono comunicate insieme alle altre informazioni necessarie per svolgere la propria attività. In casi diversi deve essere richiesta l'autorizzazione al proprio responsabile.
5. Nessun utente è autorizzato a rispondere a richieste telefoniche o interviste che chiedano notizie dirette o indirette riguardanti il Sistema Informativo. L'unica risposta ammessa in questi casi deve essere la seguente: "Non sono autorizzato a rilasciare questo tipo di informazioni. Dovete rivolgervi direttamente alla Direzione".
6. Nessun utente è autorizzato a trasmettere alcuna informazione, documento, file o archivio in risposta ad una richiesta proveniente da fonte non accertata e se non espressamente autorizzato dal responsabile del trattatamento dello stesso.
7. In caso di richieste inoltrate da soggetti esterni (telefonicamente, per mail, per posta o altri mezzi); è necessario, che il richiedente sia identificato ai sensi di legge e nelle modalità previste dal regolamento per l'accesso agli atti, alle informazioni e ai documenti amministrativi e che siano specificate le motivazioni delle richieste, salvo i casi di esercizio dell'accesso civico generalizzato nei limiti consentiti dall'ordinamento .

Linee guida per l'utilizzo dei profili social network

1. L'avvento e la crescente diffusione dei servizi di social network segnalano un cambiamento radicale nell'accessibilità pubblica a dati ed informazioni, secondo modalità e misure sinora sconosciute..
2. Assimilando i mezzi di diffusione del pensiero dei social network (Facebook, Twitter, Linkedin, WhatsApp, Blog, Chat ed altro), alle dichiarazioni rese dall'addetto a mezzo degli strumenti tradizionali di comunicazione pubblica (giornali, radio, televisione), si ricorda che il diritto di manifestazione del pensiero e di critica in costanza del rapporto di lavoro soggiace a determinati limiti, esplicitazioni dei doveri di fedeltà, di riservatezza ed adesione ai valori dell'Ente, a cui l'addetto è tenuto a uniformarsi:
   a. Continenza verbale;
   b. Continenza sostanziale: verità dei fatti e del ruolo ricoperto all'interno dell'Ente;
   c. Divulgazione di qualsiasi tipo di dato o informazione relativo e attinente l'attività dell'addetto all'interno dell'Ente.
3. Allorchè il "profilo privacy" scelto e adottato dall'incaricato consente la visualizzazione dei suoi "post", commenti, video e foto, anche ad una cerchia di utenti aperta e sostanzialmente indeterminabile, l'incaricato soggiace a valutazioni ed ad azioni di responsabilità disciplinare quando integri una lesione del rapporto fiduciario che lega l'incaricato all'Ente, con evidenti profili di violazione della riservatezza e danno dell'immagine, alla continuità e alla regolarità dell'attività.

Controlli dell'Ente

1. Il Titolare, per mezzo dei soggetti preposti, fermo restando il divieto di monitoraggi sistematici e costanti, deve effettuare periodicamente controlli ed ispezioni, anche a garanzia della sicurezza e riservatezza dei dati personali oggetto di trattamento sempre nel rispetto dell'articolo 4 della Legge n. 300 del 20 maggio 1970.
2. L'Ente, quale datore di lavoro, si riserva la facoltà di accedere in qualsiasi momento, nel rispetto della normativa sulla privacy e del presente manuale operativo, a tutti gli strumenti informatici, telematici e telefonici dell'Ente assegnati in dotazione ai singoli utenti per l'espletamento delle proprie mansioni lavorative, ai documenti e ai dati personali e alle altre informazioni ivi contenute.
3. L'Ente si astiene da qualsiasi finalità di controllo sistematico dell'attività lavorativa attraverso forme di controllo prolungate, continuative, intenzionalmente ad elevata frequenza. Nell'esercizio dei controlli e delle verifiche il personale preposto deve garantire la massima riservatezza dei dati conosciuti, anche incidentalmente, in occasione della verifica, pena l'applicazione di sanzioni disciplinari in base alla gravità dell'accaduto. Le informazioni derivanti dai controlli potranno quindi essere rese disponibili solo ed esclusivamente a soggetti interni o esterni all'Ente per cui la comunicazione sia necessaria in relazione alle finalità perseguite con l'accesso, nel rispetto dei principi di correttezza, necessità, pertinenza e non eccedenza previsti dalla legge.
4. I controlli potranno essere collettivi (es. rete dell'Ente, funzionamento della posta elettronica) oppure su singoli dispositivi o postazioni o utenti e avverranno, più spesso, in caso di anomalie o abusi (spot o reiterati).
5. Oltre a ciò l'Ente si riserva di effettuare specifici controlli sui software e/o applicazioni caricati sui dispositvi informatici dell'Ente utilizzati dagli addetti, al fine di verificarne la regolarità sotto il profilo delle autorizzazioni e delle licenze, nonché, in generale, la conformità degli stessi alla normativa vigente e di effettuare specifici controlli ad hoc nel caso di segnalazioni di attività che hanno causato danno o che ledono diritti di terzi o che comunque sono illegittime.
6. I controlli potranno avere luogo con o senza preavviso. Il preavviso potrà essere collettivo od individuale, e sarà comunicato all'utente nel rispetto del principio delle libertà fondamentali di lavoratori, come esplicitato ai punti successivi.
7. Nei casi in cui sia necessario restringere l'ambito della verifica, l'Ente si riserva di poter protrarre l'indagine fino all'individuazione puntuale del singolo utente, secondo il principio di "Graduazione dei controlli" enunciato al punto 6.1 del provvedimento del Garante: " linee guida del Garante per posta elettronica e internet" – (Gazzetta Ufficiale n. 58 del 10 marzo 2007):
8. In caso di anomalie, il personale preposto del servizio sistemi informativi effettuerà controlli che si concluderanno con avvisi e richiami generalizzati diretti a tutti i soggetti dell'area o del settore o altra unità organizzativa in cui si è rilevato l'utilizzo anomalo degli strumenti aziendali, con l'invito ad attenersi scrupolosamente al compiti assegnati e alle istruzioni.
9. Ulteriori controlli aventi base individuale potranno avvenire:
   a. in caso di ulteriori anomalie o abusi successivi all'avviso precedente;
   b. anche fin dall'inizio, nel caso in cui, sulla base degli elementi conoscitivi disponibili, il Titolare abbia ragionevole motivo di sospettare che l'utilizzo degli strumenti dell'Ente da parte del singolo individuo, in assenza di immediati specifici controlli possa arrecare un pregiudizio anche solo potenziale alla stessa (controlli aventi scopo cd. "difensivo") e/o determinare eventi che le finalità stesse del controllo mirano a prevenire od a contrastare.
10. Il Titolare si riserva la possibilità di inoltrare avvisi individuali (per email o telefono). Tali avvisi possono essere sospesi o ritardati qualora la tempestività comporti un pericolo di elusione anche parziale, da parte dell'utente, degli accertamenti o provvedimenti dell'Ente, in termini di alterazione, distruzione od occultamento delle informazioni che i controlli sono diretti a raccogliere e/o a consentire, oppure causino un rischio di aggravamento del danno o la compromissione della difesa o dell'accertamento di diritti, responsabilità giudiziali o attività istituzionali dell'Ente. In questi casi l'informazione potrà/dovrà essere data a posteriori.
11. Gli avvisi preventivi possono altresì essere omessi per i controlli difensivi o richiesti da Pubbliche Autorità (Polizia Postale, Autorità Giudiziaria, ecc.) o in caso di incidenti che necessitino di interventi immediati ed urgenti secondo la valutazione del personale preposto alla loro gestione.

Gestione documenti cartacei contenenti dati personali

1. Per il trattamento dei documenti cartacei è necessario rispettare sempre le indicazioni del Titolare o del Dirigente Responsabile e coordinatore degli addetti al trattamento dei dati, con riferimento agli archivi a cui poter accedere e ai documenti che è possibile trattare: l'ambito di trattamento dei dati personali è quello indicato nel provvedimento di individuazione del dipendente in qualità di addetto al trattamento .
2. Una volta presi in carico, gli atti e i documenti, contenenti dati personali, non devono essere lasciati senza controllo per un tempo indefinito, ma occorre provvedere e vigilare per un opportuno controllo e un'adeguata custodia, per poi restituirli al termine delle operazioni affidate.
3. In caso di affidamento di atti e documenti contenenti dati sensibili o giudiziari, il controllo e la custodia devono avvenire in modo tale che ai dati non accedano persone prive di autorizzazione. A tale fine, è quindi necessario dotarsi di cassetti con serratura, o di altri accorgimenti aventi funzione equivalente, nei quali riporre i documenti contenenti dati sensibili o giudiziari prima di assentarsi dal posto di lavoro, anche temporaneamente.
4. In caso di distruzione di documenti contenenti dati personali, specie se di natura particolare e giudiziaria si dovrà avere cura di rendere non intelleggibili i documenti eliminati, anche attraverso l'uso di specifica strumentazione tecnica per distruggerli.
5. Si invitano gli addetti al trattamento dei dati personali a fare particolare attenzione alle operazioni di riproduzione di copia immagine di documenti, avendo cura a non lasciare incustodite le copie nelle macchine fotocopiatrici o in altri dispositivi di trasmissione in uso.
6. Assicurare l'accesso agli archivi contenenti dati particolari e giudiziari alle sole persone autorizzate da specifico e scritto profilo di autorizzazione, ricordando loro di non abbandonare mai tali documenti e di riconsegnarli non appena terminato l'incarico che ne ha determinato il trattamento.

Cessazione dal servizio o interruzione del rapporto di lavoro per qualsiasi causa

1. In caso di cessazione dal servizio o interruzione del rapporto di lavoro per qualunque causa il Titolare provvederà ad attuare le seguenti operazioni al fine di garantire il rispetto del principio di correttezza dei trattamenti e di tutela della dignità della persona:
   a. sarà consentito all'interessato di partecipare alla ricognizione (e, se del caso, alla consegna) di documenti o di oggetti collocati all'interno degli uffici, soprattutto in caso di assegnazione di spazi e postazioni ad uso di un singolo e per un periodo significativo di tempo;
   b. alla cessazione del rapporto di lavoro, l'interessato dovrà restituire alla Direzione tutti i dispositivi informatici dell'Ente affidati dall'Ente, per questo motivo si raccomanda di eliminare preventivamente ed esclusivamente i contenuti "personali" eventualmente presenti sui dispositivi e dall'account di posta elettronica dell'Ente;
   c. l'account di posta elettronica (ove direttamente riconducibile all'interessato) verrà disattivato e per un periodo di 6 mesi la Direzione provvederà ad attivare un sistema di risponditore automatico allo scopo di avvisare eventuali mittenti che il lavoratore/utente non è più in forza all'ente e quindi nel caso verrà fornito un indirizzo alternativo (interno all'ente) al quale inviare eventuali comunicazioni;
   d. i dati esterni e il contenuto della corrispondenza relativa all'account di posta elettronica disattivato, riconducibile all'Utente saranno conservati:
      i. per 12 mesi dalla cessazione del rapporto/disattivazione dell'account, limitatamente al perseguimento di finalità organizzative, produttive e di sicurezza,
      ii. per un periodo massimo di 10 anni, dalla cessazione del rapporto/disattivazione dell'account, per l'esclusiva finalità di tutela dei diritti del Titolare in sede giudiziaria, nei limiti di cui all'art. 160-*bis* del D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018.
   e. la Direzione provvederà alla formattazione completa dei device restituiti, avendo cura di eliminare eventuali copie dei contenuti presenti nei back-up dell'Ente;
   f. i dati dell'interessato saranno conservati per il tempo necessario a garantire il rispetto degli obblighi legislativi.

Applicabilità del manuale operativo e responsabilità degli utenti

1. Il presente manuale oparativo si rivolge a tutto il personale dipendente e ad ogni altro soggetto che opera per l'ente sotto qualsiasi forma contrattuale che lo collega all'Ente, lo abilita ad utilizzarne i sistemi informatici e all'accesso autorizzato alle risorse informatiche dell'Ente.
2. Il nuovo manuale operativo si applica a tutti gli utenti senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori a prescindere dal rapporto contrattuale istaurato con la Provincia (lavoratori somministrati, collaboratore a progetto, in stage, ecc.).
3. Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente e collaboratore (professionista) in possesso di specifiche credenziali di autenticazione.
4. Il mancato rispetto o la violazione delle regole contenute nel presente manuale operativo è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.
5. Tutti gli addetti possono proporre, quando ritenuto necessario, integrazioni al presente manuale, indicando gli ambiti di integrazione, i profili di sicurezza ritenuti a rischio e gli approfondimenti tecnici realizzati in collaborazione con il servizio sistemi informativi.
6. Le proposte verranno esaminate dal Titolare del trattamento.

Formazione sulla protezione dei dati personali

1. Il Titolare del trattamento è tenuto ad erogare specifica formazione in materia di Privacy (Artt. 29, 32 del GDPR). In particolare relativamente a:
   a. profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle rispettive attività e conseguenti responsabilità in caso di utilizzo dei dati improprio, abusivo e difforme alle leggi e alle direttive operative impartite al personale;
   b. rischi che incombono sui dati;
   c. misure disponibili per prevenire eventi dannosi;
   d. modalità per un costante aggiornamento sulle misure di sicurezza adottate dal titolare.

Informativa agli utenti *ex* art. 13 Regolamento UE n. 2016/679

1. Il presente manuale operativo, nella parte in cui contiene le regole per l'utilizzo dei beni e degli strumenti informatici dell'Ente in relazione ai trattamenti di dati personali svolti dal Titolare e finalizzati all' effettuazione di controlli leciti sui dispositivi in uso agli utenti (come definiti nell'apposito paragrafo), vale quale informativa *ex* art. 13 del Regolamento UE n. 2016/679

Entrata in vigore del manuale operativo

1. Il nuovo manuale operativo entrerà in vigore a partire dalla data di esecutività del decreto di adozione.
2. Con l'entrata in vigore del presente manuale tutte le disposizioni in precedenza adottate in materia, in qualsiasi forma comunicate, devono intendersi abrogate e sostituite dalle presenti.