Città di Castelnuovo di Garfagnana

Provincia di Lucca

Via Vallisneri, 1 – 55032 Castelnuovo di Garfagnana (LU)

Manuale di Gestione Documentale

Allegato 6 – Linee guida per la sicurezza delle postazioni di lavoro e delle infrastrutture telematiche dell'ente

(aggiornamento Giugno 2025)

Indice

Introduzione

Le presenti “Linee guida per la sicurezza delle postazioni di lavoro e delle infrastrutture telematiche dell’ente” costituiscono un documento tecnico descrittivo delle policy in uso presso i sistemi informatici del Comune di Castelnuovo di Garfagnana;

Scopo del documento è definire le modalità idonee a conseguire la massima sicurezza possibile sulla base della tecnologia, dell’organizzazione, delle dotazioni hardware e software effettivamente disponibili presso il Comune di Castelnuovo di Garfagnana alla data della sua approvazione.

Per tale ragione, il presente documento è necessariamente contingente e viene aggiornato di norma con cadenza annuale; può altresì essere aggiornato con maggiore frequenza in conseguenza di novità tecnologiche e/o organizzative e/o nella dotazione hardware/software dell’Ente.

Gli amministratori di sistema, individuati con appositi atti formali, assicurano il rispetto delle presenti Linee Guida.

Trattamento di dati relativi alla gestione delle Postazioni di Lavoro

L'utilizzo da parte dell'utente degli strumenti informatici assegnati comporta, di regola, la raccolta di informazioni sul loro uso, che possono essere direttamente o indirettamente associate all'utente, configurando un trattamento di dati personali ai sensi della normativa vigente. Tali informazioni possono essere oggetto di controlli incidentali da parte dell'Ente, anche per il tramite dell'amministratore di sistema e/o dell'Ufficio Sistemi Informativi, volti a garantire, in particolare, la sicurezza e tutela del patrimonio informativo dell'Ente. Gli interventi di controllo, possono permettere all'Ente di prendere indirettamente cognizione dell'attività svolta dall'utente mediante gli strumenti informatici. In via generale, i controlli previsti dall'Ente escludono finalità di monitoraggio diretto ed intenzionale dell'attività lavorativa dell'utente e sono svolti nel rispetto della normativa vigente in materia (art. 4 della Legge n. 300/1970 e s.m.i.; art. 114 del Codice in materia di protezione dei dati personali). Il rispetto della disciplina di settore costituisce infatti condizione di legittimità dei suddetti trattamenti.

In particolare le postazioni di lavoro fisse e portatili e gli strumenti di stampa costituiscono strumenti utilizzati dal dipendente per rendere la prestazione lavorativa, che impongono che sia data allo stesso "adeguata informazione sulle modalità d'uso degli strumenti e di effettuazione dei controlli, nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196" anche ai fini dell'utilizzabilità a tutti i fini connessi al rapporto di lavoro delle informazioni raccolte mediante gli strumenti stessi.

L'Ente esclude per impostazione tecnica predefinita la raccolta di dati e informazioni eccedenti a quelli strettamente necessari a garantire le finalità organizzative e di rispetto alle presenti linee guida. La presente assolve agli obblighi di informativa di cui al Punto 6.1 delle "Linee Guida del Garante per posta elettronica ed Internet" dell'Autorità Garante per la protezione dei dati.

Nomenclatura

Ai fini del presente regolamento s'intende per:

a. **accesso alla rete dati**: qualsiasi tentativo di accesso alla rete dati dell'ente proveniente sia dalle sedi interne che dall'esterno mediante qualsiasi sistema di connessione;
b. **amministratore di sistema:** figura professionale interna o esterna all'ente dedicata alla gestione e alla manutenzione di hardware e software con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali. Gli amministratori di sistema sono designati nominativamente e l'elenco dei soggetti nominati è conservato presso l'Ufficio Sistema Informativi o altro ufficio dell'ente che si occupa di Privacy.
c. **apparati attivi**: apparecchiature hardware collegate alla rete dati che ne permettono il funzionamento;
d. **backup**: procedura per la duplicazione dei dati su un supporto esterno o distinto da quello sul quale sono memorizzati, in modo da garantirne una copia di riserva;
e. **cartelle condivise**: spazi di memorizzazione messi a disposizione degli utenti sui sistemi centralizzati;
f. **ente**: Comune di Castelnuovo di Garfagnana;
g. **firewall**: apparato di rete hardware o software che filtra tutto il traffico entrante e uscente, da e verso una rete o un computer, applicando regole che contribuiscono alla sicurezza della rete stessa.
h. **indirizzamento**: attività di assegnazione di indirizzi logici ad apparati attivi e ad attrezzature informatiche connesse alla rete dati;
i. **postazione di lavoro:** dispositivo (personal computer, notebook, thin/fat client, ecc.) che consente l'accesso al proprio ambiente di lavoro informatico;
j. **protocollo**: insieme di regole che definisce il formato dei messaggi scambiati tra due entità e che consente loro di comunicare nonché di comprendere la comunicazione;
k. **restore o ripristino**: procedura per il recupero dei dati precedentemente salvati (backup) su un supporto esterno o distinto da quello sul quale sono normalmente memorizzati, in modo da recuperare informazioni perse o corrotte;
l. **rete dati**: insieme dell'infrastruttura passiva (cavi, prese, ecc.) e degli apparati attivi (switch, router, ecc.) necessari alla interconnessione di apparati informatici;
m. **servizi centralizzati**: insieme dei servizi e delle applicazioni software forniti agli utenti attraverso i sistemi centralizzati;
n. **sistemi centralizzati**: server fisici e/o virtuali che forniscono servizi attraverso la rete dati;
o. **utente:** persona fisica autorizzata ad accedere alle banche dati ed ai servizi informatici dell'ente;

Credenziali di autenticazione

Regole generali

Tutti i dipendenti dell'ente sono dotati di credenziali di accesso al dominio, agli applicativi dell'ente ed alle caselle di posta personali o di ufficio con le indicazioni riportate nei paragrafi successivi.

Le credenziali di autenticazione al dominio Active Directory adottate dal Comune di Castelnuovo di Garfagnana consistono in:

- un identificativo alfanumerico dell'utente tipicamente costruito nel modo seguente: <iniziale nome>.<cognome> salvo casi di omonimia. In quest'ultimo caso si utilizza per entrambi il nome completo. Se questo non fosse sufficiente verrà aggiunto un numero progressivo al nome;
- una password associata a detto identificativo creata rispettando i requisiti riportati nel paragrafo successivo.

Nel caso di collaboratori che debbano avere accesso alle risorse informatiche dell'ente, verranno create credenziali di accesso generiche che fanno riferimento all'Ufficio presso il quale il soggetto svolgerà la sua attività, seguito da un progressivo numerico e/o dall'anno di riferimento (es: ced001)

Le credenziali di autenticazione ai Sistemi Informativi / Programmi adottate dall'ente devono rispettare le seguenti indicazioni:

- ove il sistema/ambiente applicativo consenta l'accesso con protocollo LDAP, le credenziali e le password coincidono con quelle del dominio;
- ove il sistema/ambiente applicativo non permetta di effettuare l'accesso tramite credenziali di dominio, ne verranno create altre con la stessa tipologia sia per il nome utente sia per la complessità della password (ove possibile);
- la password di dominio deve essere modificata al primo accesso ed ha una validità di 3 mesi;
- gli utenti sono in grado, in tutti i Sistemi Informativi e nel Dominio di autenticazione in uso presso l'ente, di modificare autonomamente la propria password;
- l'Ufficio Sistemi Informativi provvederà alla creazione delle credenziali di autenticazione ed alla profilazione degli utenti sui diversi Sistemi Informativi in uso, in funzione delle indicazioni ricevute dai dirigenti dei Servizi di competenza.

Password

La password deve rispettare i seguenti criteri di lunghezza, complessità e segretezza:

1. la password deve essere lunga almeno 8 caratteri;

2. la password deve essere contenere almeno 3 dei seguenti quattro gruppi di caratteri:
    a. lettere maiuscole (A-Z),
    b. lettere minuscole (a-z),
    c. numeri (0-9),
    d. caratteri speciali (punteggiatura e altri caratteri presenti sulla tastiera);

3. la password non deve essere basata su informazioni riconducibili all'ambito personale (nome, cognome, date legate a eventi propri o dei propri familiari, hobby, interessi culturali e così via);

4. la password non deve essere formata da sequenze di caratteri facilmente individuabili (per esempio "qwertyui" o "12345678") o da forme verbali individuabili con un preciso senso logico (per esempio, espressioni gergali o dialettali comunemente usate).

Modifica della password

Le password di accesso al dominio dell'ente nascono già 'scadute' e devono essere modificate a cura dell'utente, al primo accesso.

Le password di accesso al dominio dell'Comune di Castelnuovo di Garfagnana e, di conseguenza, di tutti quei sistemi/ambienti applicativi che possono essere collegati a quel meccanismo di autenticazione, scadono ogni tre mesi. E' inibito l'utilizzo di una password uguale ad una delle ultime otto già utilizzate.

Per gli applicativi che non hanno a disposizione meccanismi di verifica della scadenza della password, gli utenti sono tenuti a modificarla ogni 3 (tre) mesi in modo autonomo.

Attivazione delle credenziali di autenticazione

Le nuove credenziali di autenticazione vengono create in due situazioni:

- assunzione nuovo dipendente;
- incarico a collaboratore che deve accedere ai sistemi informativi dell'ente.

Nel primo caso l'informazione della nuova assunzione deve essere inviata dall'Ufficio Personale all'Ufficio Sistemi Informativi almeno 4 giorni prima della presa di servizio del nuovo dipendente, riportando: Nome, Cognome, Codice Fiscale, Data di assunzione e Servizio presso il quale il nuovo dipendente verrà assegnato.

Nel secondo caso la richiesta di creazione di nuove credenziali deve pervenire dal funzionario responsabile del Servizio presso il quale il collaboratore svolgerà la propria attività sempre con 4 giorni di preavviso rispetto all'inizio del rapporto di collaborazione.

Il titolare di credenziali di autenticazione assume il nome di "utente".

Disattivazione credenziali di autenticazione

La disattivazione delle credenziali di autenticazione di un utente avviene in caso di:

- cessazione del rapporto di lavoro con il dipendente;
- cessazione del rapporto con il collaboratore.

Nel primo caso l'Ufficio Personale comunica all'Ufficio Sistemi Informativi la cessazione del rapporto di lavoro (pensionamento, trasferimento, …) con almeno 4 giorni di anticipo

indicando la data di fine rapporto. Le credenziali di autenticazione verranno disabilitate dal primo giorno successivo al termine del rapporto di lavoro. Sulla casella di posta personale dovrà essere impostato, dal primo giorno successivo al termine del rapporto di lavoro, un risponditore automatico con indicazione di una casella di posta alternativa a cui inoltrare i messaggi. La casella di posta verrà definitivamente cessata tre mesi dopo il termine del rapporto di lavoro.

Nel secondo caso la comunicazione deve essere fatta dal funzionario competente per il rapporto di collaborazione e deve essere fatta almeno 4 giorni prima del termine di tale rapporto. Le credenziali di autenticazione verranno disabilitate dal primo giorno successivo al termine del rapporto di collaborazione.

Ripristino della password

Il ripristino della password di accesso al dominio e alla posta elettronica viene effettuato esclusivamente:

- su richiesta del dipendente titolare delle credenziali di accesso;
- su richiesta formale dell'autorità giudiziaria o di polizia;
- con le diverse modalità eventualmente previste da un disciplinare interno - redatto, adottato e pubblicizzato tra i dipendenti con le modalità indicate dalle Linee guida del Garante della privacy, per posta elettronica ed internet.

In tutti i casi sopra indicati l'Amministratore di sistema provvederà a generare una password temporanea che l'utente dovrà provvedere obbligatoriamente a personalizzare, con i criteri esposti nei paragrafi precedenti, al primo accesso.

Profilazione degli utenti

L'Ente dispone di diversi sistemi informativi di fornitori diversi, che ammettono profili di utenti diversificati.

I file di lavoro sono ospitati su un server dell'Ente organizzati in cartelle. Le abilitazioni di accesso ad ogni cartella fanno riferimento ad uno o più gruppi di utenti che hanno abilitazioni di lettura e/o scrittura sui file e sulle sottocartelle contenute.

Creazione di un nuovo profilo utente

Il responsabile dell'Ufficio presso il quale entra in servizio il nuovo dipendente, comunica all'amministratore di sistema le autorizzazioni che è necessario fornire per l'accesso ai diversi sistemi informativi ed indica su quali cartelle di lavoro deve essere abilitato ad operare.

Modifica di un profilo utente

In caso di trasferimento di un dipendente, il Responsabile dell'Ufficio presso il quale prestava servizio comunica all'amministratore di sistema la necessità di eliminare le autorizzazioni ai sistemi informativi ed alle cartelle condivise di un determinato ufficio. Il responsabile dell'Ufficio presso il quale si trasferisce il dipendente, comunica all'amministratore di sistema le autorizzazioni che è necessario fornire per l'accesso ai diversi sistemi informativi ed indica su quali cartelle di lavoro deve essere abilitato ad operare.

Disabilitazione di un profilo utente

Quando un dipendente cessa il rapporto di lavoro con l'ente, l'Ufficio Personale comunica l'evento all'amministratore di sistema così da provvedere al blocco delle credenziali di autenticazione e la sospensione dell'utente da tutti i sistemi informativi presso i quali era stato registrato.

Caselle di posta elettronica

Regole generali per l'utilizzo delle caselle di posta elettronica

Ciascun dipendente è dotato di una casella di posta elettronica personale costituita dal nome e cognome separati da un punto e dal nome del dominio dell'ente (es: utente Mario Rossi → email mario.rossi@ente.it). In fase di creazione della casella, al dipendente viene fornito un 'token' o 'password temporanea' con il quale dovrà effettuare il primo accesso e l'impostazione della propria password personale. In caso di smarrimento della password, andrà fatta una richiesta all'amministratore di sistema che provvederà a generare un nuovo token di accesso.

L'accesso alla casella di posta elettronica ed ai relativi messaggi avviene tramite apposito sito web e/o tramite apposito client di posta. Il protocollo usato per l'utilizzo delle caselle di posta dell'ente è IMAP.

Lo spazio inizialmente a disposizione delle caselle di posta personali è di 3Gb. L'utente è tenuto a cancellare autonomamente i messaggi di spam, pubblicitari o comunque la cui conservazione non è necessaria.

Nel caso lo spazio a disposizione non fosse più sufficiente, l'utente potrà fare una richiesta di ampliamento all'Ufficio Sistemi Informativi. La richiesta dovrà essere preventivamente approvata dal Responsabile del Servizio del richiedente.

Tutti quei messaggi che contengono allegati che vengono poi salvati su cartelle condivise o altri supporti, devono essere cancellati al fine di contenere lo spazio occupato dalla casella di posta.

Prima di periodi prolungati di assenza (ferie, aspettative, …) l'utente deve impostare tramite l'apposita interfaccia sul web, un messaggio automatico di risposta ai messaggi in arrivo, indicando eventualmente nel corpo del messaggio una mail alternativa di ufficio a cui trasmettere messaggi urgenti relativi all'attività lavorativa. L'utente dovrà impostare la data di inizio e se possibile di fine per la risposta automatica.

Le caselle di posta personali devono essere utilizzate esclusivamente per attività lavorativa. L'ente, previo avviso all'interessato, ha facoltà in caso di prolungata assenza o in caso di urgenza nel reperimento di un messaggio che è noto essere stato trasmesso ad una casella personale, di resettare la password della casella di posta personale per potervi accedere, dandone comunicazione all'interessato.

Software

Software di base installato sulle postazioni di lavoro dell'Ente

Su tutte le postazioni di lavoro dell'ente è installato un set minimo di software che consente di mettere in sicurezza il PC e di svolgere la normale attività lavorativa.

L'Ente utilizza come software di Office Automation quelli presenti nella suite MS Office / Libre Office nelle loro diverse versioni. Per le altre tipologie di software l'ente utilizza preferenzialmente software Open Source.

Il software viene generalmente installato nella ultima versione disponibile salvo alcuni casi (es: Java) per problemi di compatibilità con alcune applicazioni.

Le applicazioni installate normalmente sono le seguenti

- 7zip, WINZIP, WINRAR: software per la compressione/decompressione dei file
- Adobe Reader: lettore di file PDF;
- Antivirus: software antivirus per la sicurezza della PdL;
- Google Chrome: software per la navigazione web;
- Firefox: software per la navigazione web;
- Dike e/o Arubasign: software per la verifica e firma digitale dei file;
- ID protect: software per la gestione delle smart card di autenticazione/firma;
- Java: ambiente per l'avvio di applicazioni;
- Microsoft Office e/o Libre Office: software di Office Automation;

Software specifico installato sulle postazioni di lavoro

Su alcune postazioni di lavoro è necessario installare software specifico che può essere di tipo client - server o stand alone eventualmente con licenze di utilizzo concorrenti.

- **Software Client - Server**. Le licenze dei software *client - server* sono di norma conservate dall'amministratore di sistema, che provvede a installare il software direttamente sulla postazione di lavoro o a incaricare le relative ditte per effettuare tale attività (es: Software client SICI della ApKappa), presso l'Ufficio Sistemi Informativi dell'ente.
- **Software specifico con licenze concorrenti**. Le licenze dei software con licenze concorrenti sono conservate di norma presso presso l'Ufficio Sistemi Informativi dell'ente (es: PrimusWIN). La licenza centrale viene installata su uno dei server a disposizione e l'amministratore di sistema provvede all'installazione del prodotto fornendo tutti i dati necessari per il raggiungimento della licenza sul server.
- **Software specifico con licenze stand alone**. Queste licenze (es: SketchUp, AutoCAD, …) sono conservate presso l'Ufficio Sistemi Informativi dell'ente.

L'amministratore di sistema provvede all'installazione del software sulle postazioni di lavoro.

Software in cloud

Per i software che saranno resi disponibili in cloud, dovrà essere resa obbligatoria, ove possibile, l'autenticazione a due fattori.

Internet

Regole generali

La connessione alla rete internet dal pc è ammessa esclusivamente per motivi attinenti allo svolgimento dell'attività lavorativa.

L'utilizzo per scopi personali è permesso con moderazione e con gli accorgimenti di cui al presente documento.

In particolare, si vieta l'utilizzo dei social network, se non espressamente autorizzati o necessari per l'attività istituzionale.

L'Ente potrà adottare idonee misure tecniche preventive volte a ridurre navigazioni verso siti non correlati all'attività lavorativa attraverso filtri e black list.

È altresì vietato:

1. L'accesso a siti internet che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico, rilevante ai fini della realizzazione di una fattispecie di reato o che siano in qualche modo discriminatori sulla base della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.
2. Scaricare software (anche gratuito) prelevato da siti Internet;
3. Effettuare ogni genere di transazione finanziaria privata ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi autorizzati per l'espletamento di attività d'ufficio (prenotazione treni per missioni di lavoro, …).
4. Registrare account a siti i cui contenuti non siano legati all'attività lavorativa.
5. Partecipare a forum non professionali, utilizzare chat line e bacheche elettroniche, partecipare a gruppi di discussione o lasciare commenti ad articoli o iscriversi a mailing list spendendo il marchio o la denominazione dell'Ente, salvo specifica autorizzazione.
6. Memorizzare documenti informatici di natura oltraggiosa, diffamatoria e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
7. Promuovere utile o guadagno personale attraverso l'uso di Internet o della posta elettronica dell'Ente.
8. Accedere dall'esterno alla rete locale, salvo autorizzazione specifica.
9. Creare siti web personali sui sistemi dell'Ente.
10. Accedere ad alcuni siti internet mediante azioni inibenti dei filtri, sabotando o comunque superando o tentando di superare o disabilitando i sistemi adottati dall'ente per bloccare accessi non conformi all'attività lavorativa.
11. Utilizzare l'accesso a internet in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore (es. legge 22 aprile 1941, n. 633 e successive modificazioni, d.lgs. 6 maggio 1999, n. 169 e legge 18 agosto 2000, n. 248) e, in particolare, scaricare materiale soggetto a copyright (testi, immagini, musica, filmati, file in genere) se non espressamente autorizzato.

Si raccomanda di evitare di inviare username e password o altre informazioni personali su siti che utilizzano protocolli non sicuri il cui indirizzo inizia con http://. Si possono invece ritenere sicuri i siti che utilizzino il protocollo https (https://…) previa verifica, tramite le funzioni che il browser mette a disposizione, della qualità del certificato fornito dal sito.

Backup

Postazioni individuali

Il backup dei dati presenti sui PC degli utenti NON è garantito. I documenti di lavoro devono essere salvati nelle cartelle condivise sul server, soggette a politiche di backup.

Politiche di backup dei server fisici e/o virtuali

Le cartelle condivise presenti sul file server sono protette mediante il meccanismo delle shadow copy che crea delle 'fotografie' con cadenza almeno quotidiana secondo le politiche definite dall'amministratore di sistema.

L'ente utilizza il software di Backup per effettuare i salvataggi delle macchine fisiche e virtuali su supporti in locale e, ove possibile, con una copia non riscrivibile in un sito remoto.

Le politiche di retention prevedono il mantenimento di revisioni quotidiane fino ad almeno 6 giorni precedenti, oltre a due backup delle due settimane precedenti e ad un punto di ripristino del mese precedente.

Politiche di backup della posta elettronica

La posta elettronica è fornita da un ISP esterno all'interno dell'accordo quadro denominato "Sistema Cloud Toscana" (SCT) ospitato presso il Tuscany Internet eXchange (TIX) di Regione Toscana. Sulle postazioni di lavoro le caselle elettronica vengono accedute tramite client di posta in modalità IMAP. Periodicamente le email vengono eliminate o scaricate in archivi locali sul server. I backup delle caselle di posta fa parte del contratto di servizio con il fornitore individuato da Regione Toscana.

Politiche di ripristino dei file o dati danneggiati

In caso di eliminazione o danneggiamento dei dati, gli stessi saranno ripristinati utilizzando in prima battuta le shadow copy per quanto riguarda i file presenti nelle cartelle condivise del file server ovvero dai backup notturni dei diversi server fisici e virtuali, dietro richiesta esplicita e tracciabile degli interessati.

Uso dell’Intelligenza Artificiale (IA)

Regole generali

Gli strumenti di Intelligenza Artificiale stanno diventando sempre più strumenti di supporto all’attività lavorativa.

L’Unione Europea con Regolamento UE 1689/2024, si è dotata di una normativa specificatamente destinata agli strumenti di Intelligenza Artificiale. Anche AgID sta per pubblicare delle Linee Guida per l’utilizzo di strumenti di Intelligenza Artificiale nella PA.

La presente Policy si applica a tutti i dipendenti e collaboratori e ha lo scopo di stabilire linee guida per l'uso dell'IA generativa all'interno dell’ente con l'obiettivo di garantire:

- la **protezione dei dati personali**, prevedendo per impostazione predefinita in fase di acquisto/progettazione/utilizzo di strumenti AI, misure tecniche ed organizzative funzionali ad assicurare i principi e le disposizioni in materia di protezione dei dati personali (Regolamento UE 2016/679 e Codice in materia di protezione dei dati personali – D.lgs. n. 196/2003, come mod. dal d.lgs. n. 101/2018 e s.m.i., nonché le linee guida ed i chiarimenti in materia);
- la **sicurezza delle informazioni**, necessaria ad assicurare la riservatezza e/o confidenzialità alle informazioni dell’organizzazione, in attuazione delle discipline di settore vigenti.

Linee Guida per l'utilizzo dell'IA Generativa

Nell’utilizzo degli strumenti di IA generativa devono essere applicate le istruzioni operative formalizzate nelle presenti Linee Guida.

È necessario utilizzare prompt generici e non specifici per evitare la divulgazione di informazioni di dati riservati o confidenziali.

1. **Protezione dei Dati Personali**

   Allo scopo di assicurare il rispetto dei principi e delle disposizioni in materia di protezione dei dati personali è fatto divieto agli utenti di inserire negli strumenti di IA generativa:

   a. nomi, cognomi, indirizzi, numeri di telefono, numeri di previdenza sociale, informazioni finanziarie o qualsiasi altro dato personale che possa identificare, direttamente o indirettamente, una persona fisica (interessato).
   b. informazioni personali particolarmente sensibili (categorie particolari di dati personali ai sensi dell’art. 9 del Regolamento, come dati relativi allo stato di salute), dati giudiziari (relativi a reati o condanne penali di cui all’art. 10 del Regolamento) o altre informazioni particolarmente riservate (informazioni finanziarie, dati di pagamento).

2. **Protezione delle informazioni dell’ente**

Allo scopo di assicurare la protezione delle informazioni riservate dell'ente è fatto divieto agli utenti di inserire negli strumenti di IA generativa:

a. informazioni riservate dell'ente, relative ad attività interne dell'organizzazione, utenti, collaboratori, fornitori o qualsiasi altro tipo di informazione che potrebbe essere considerata di tipo confidenziale o a carattere riservato.

3. **Conformità alla normativa**

Allo scopo di assicurare la conformità normativa vigente, comprese le discipline di settore, ogni utente prima di utilizzare strumenti di IA generativa è tenuto a:

a. assicurarsi che l'utilizzo di volta in volta necessario alle attività di lavoro sia conforme alla disciplina in materia di protezione dei dati personali, nonché alle Policy e politiche interne all'organizzazione in materia di sicurezza delle informazioni;
b. rispettare le linee guida stabilite dal fornitore dell'IA nei Termini di servizio,

4. **Formazione e consapevolezza**

Per assicurare la **consapevolezza e sensibilità** degli utenti, a fronte degli specifici rischi connessi all'utilizzo di nuove tecnologie, in particolare degli strumenti di IA generativa, l'organizzazione promuove specifiche sessioni formative frontali o asincrone (vedi portale Syllabus).

Gli utenti coinvolti nell'utilizzo di strumenti di IA generativa devono:

a. partecipare alle **sessioni di formazione** organizzate dall'Ente per approfondire l'uso sicuro e responsabile degli strumenti di IA generativa;
b. utilizzare gli strumenti resi disponibili online per la formazione a distanza e asincrona come ad esempio 'Syllabus' secondo le indicazioni ricevute dai propri Responsabili
c. mantenere un alto livello di consapevolezza riguardo ai rischi associati all'uso dell'IA generativa e alle misure di protezione da adottare;