FARMACIE COMUNALI FERRARA

LINEE GUIDA
PER IL TRATTAMENTO SICURO DEI DATI PERSONALI E PER IL CORRETTO UTILIZZO DEGLI STRUMENTI DI LAVORO

Versione del documento

N°	Data	Descrizione	Emesso	Verificato	Approvato
1.0	13/12/2018	Prima emissione	13/12/2018	13/12/2018	13/12/2018
2.0	29/04/2025	Revisione	29/04/2025	29/04/2025	29/04/2025

SOMMARIO

INTRODUZIONE

L'uso improprio degli strumenti di lavoro che la Società mette a disposizione dei lavoratori per il trattamento dei dati personali, raccolti dalla società medesima per il lecito perseguimento delle proprie finalità istituzionali, oltre ad arrecare un danno in termini di maggiori costi e possibili perdite di continuità del servizio, può nuocere gravemente alla stessa da un punto di vista della reputazione e condurre a procedimenti legali con sanzioni di tipo amministrativo e penale.

Poiché la sicurezza dei dati personali non dipende solo da aspetti tecnici, ma anche, se non principalmente, da quelli organizzativi e comportamentali, tutti i lavoratori[1] devono considerarla una componente integrante dell'attività lavorativa quotidiana, al fine di prevenire il rischio di incidenti di sicurezza che possano compromettere l'integrità, la disponibilità o la riservatezza delle informazioni personali.

Il presente documento si pone pertanto quale obiettivo quello di adottare e diffondere una politica aziendale trasparente in cui siano esplicitati i limiti di utilizzo delle risorse assegnate ai lavoratori per lo svolgimento delle mansioni lavorative nonché regole comportamentali da osservare per trattare in modo sicuro le informazioni personali.

L'adozione di queste politiche viene fatta nell'intento di:

- provvedere ad un servizio continuativo nell'interesse dell'Azienda;
- salvaguardare la riservatezza delle informazioni e dei dati;
- tutelarsi da potenziali responsabilità legali;
- proteggere il buon nome e l'immagine dell'azienda;
- proteggere gli investimenti effettuati;
- evitare problemi di sicurezza informando e incentivando i comportamenti corretti;
- garantire la massima efficienza delle risorse informatiche e del loro utilizzo;
- contribuire al rispetto delle norme sul trattamento di dati personali.

FINALITÀ DEL DOCUMENTO

Questo documento ha quale finalità quella di fornire istruzioni sul corretto utilizzo degli strumenti di lavoro al fine di prevenire che l'uso improprio di tali strumenti possa esporre la società a incidenti di sicurezza tali da compromettere la riservatezza, l'integrità e la disponibilità dei dati personali.

DEFINIZIONI

1. "trattamento", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;
2. "dato personale", qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
3. "dati c.d. identificativi", i dati personali che permettono l'identificazione diretta dell'interessato (nome, cognome, codice fiscale, indirizzo e-mail...);
4. "dati c.d. sensibili", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od

[1] *Ai fini della corretta applicazione delle presenti linee guida, si intende per «lavoratore» una persona che, indipendentemente dalla tipologia contrattuale, svolge un'attività lavorativa nell'ambito dell'organizzazione aziendale, con o senza retribuzione, anche al solo fine di apprendere un mestiere, un'arte o una professione, esclusi gli addetti ai servizi domestici e familiari. Al lavoratore così definito è equiparato: il soggetto beneficiario delle iniziative di tirocini formativi e di orientamento; l'allievo degli istituti di istruzione ed universitari impegnati in tirocini curriculari, stage o periodi di alternanza scuola lavoro, e il lavoratore somministrato dipendente da società interinale.*

organizzazioni a carattere religioso, filosofico, politico o sindacale, i dati personali idonei a rivelare lo stato di salute e la vita sessuale, i dati genetici, i dati biometrici;

5. “titolare”, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
6. “c.d. incaricati”, le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
7. “interessato”, la persona fisica cui si riferiscono i dati personali;
8. “comunicazione”, il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
9. “diffusione”, il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
10. "Garante Privacy", l'autorità per la Protezione dei dati personali con compiti di vigilanza, indirizzo, informazione, promozione, consultazione e dotata di poteri ispettivi e sanzionatori.

REGOLE GENERALI PER IL TRATTAMENTO DEI DATI PERSONALI

Il trattamento dei dati personali deve avvenire nel rigoroso rispetto dei principi previsti dal Capo II del Regolamento (UE) 2016/679. In particolare, ogni lavoratore deve:

- trattare i dati personali in modo lecito, corretto e trasparenza nei confronti dell’interessato (**principio di liceità, correttezza e trasparenza**);
- se incaricato, raccogliere i dati personali per finalità determinate, esplicite e legittime, attenendosi a quanto indicate nelle relative informative privacy prodotte dalla Società, e successivamente trattarli in modo che non sia incompatibile con tali finalità (**principio di limitazione della finalità**);
- trattare i dati personali in modo adeguato, pertinente e limitato a quanto necessario rispetto alle finalità per le quali sono stati raccolti (**principio di minimizzazione dei dati personali**);
- trattare i dati personali in modo esatto e, se necessario, aggiornarli (principio di esattezza);
- conservare i dati personali per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (**principio di limitazione della conservazione**);
- trattare i dati personali in maniera tale da garantire la loro sicurezza, adottando ogni accorgimento utile a prevenire trattamenti non autorizzati o illeciti o la loro perdita, distruzione o danno accidentale (**principio di integrità e riservatezza**);

REGOLE GENERALI PER L’UTILIZZO DEGLI STRUMENTI DI LAVORO

Gli strumenti di lavoro che la Società mette a disposizione dei lavoratori, ivi inclusi dispositivi informatici, account di posta elettronica, applicativi gestionali, software, dispositivi mobili e ogni altro supporto elettronico o cartaceo utilizzato per il trattamento di dati personali, devono essere impiegati **esclusivamente per finalità connesse all’attività aziendale**.
Tale utilizzo deve essere limitato all’espletamento delle **mansioni affidate al singolo lavoratore**, nel rispetto delle istruzioni ricevute, delle procedure interne e della normativa vigente in materia di protezione dei dati personali.
È fatto **divieto di utilizzare tali strumenti per fini personali o estranei all’attività lavorativa**, anche in via occasionale o saltuaria, nonché per finalità non conformi agli scopi aziendali o che possano comportare rischi per la sicurezza e la riservatezza dei dati trattati.
Il lavoratore è tenuto a **custodire con diligenza gli strumenti assegnati**. Ogni utilizzo non conforme potrà costituire violazione delle disposizioni aziendali e normativa applicabile, con le conseguenze disciplinari e giuridiche previste.

CIRCOLAZIONE INTERNA E COMUNICAZIONE DEI DATI

Circolazione dei dati personali

La circolazione interna dei dati personali è ammessa esclusivamente nei confronti del personale espressamente autorizzato al trattamento, ai sensi dell'art. 29 del Regolamento (UE) 2016/679 e/o dell'art. 2-*quaterdecies* del d.lgs. 196/2003, come modificato dal d.lgs. 101/2018.
L'accesso ai dati personali da parte dei lavoratori è **limitato ai soli casi in cui tale accesso sia necessario per lo svolgimento delle mansioni attribuite** e rientri nell'ambito delle finalità aziendali, con riferimento al rispettivo ruolo e alle istruzioni ricevute.
È **vietata la circolazione dei dati personali tra soggetti non autorizzati o che non siano formalmente designati al trattamento**. Ogni accesso o condivisione di dati tra uffici, servizi o persone prive di autorizzazione è da considerarsi illecito e potenzialmente sanzionabile.
Ogni richiesta di accesso a dati personali da parte di un lavoratore deve essere **riconducibile alle funzioni proprie del ruolo ricoperto**. Solo in tali casi la richiesta può essere soddisfatta direttamente, senza formalità, nella misura strettamente necessaria al perseguimento degli interessi aziendali.
Qualora, invece, la richiesta sia finalizzata a un **utilizzo ulteriore e/o diverso** rispetto allo scopo originario del trattamento, sarà necessario presentare **richiesta scritta e motivata**, che sarà valutata dal responsabile competente.
I soggetti che accedono, trattano, comunicano o semplicemente vengono a conoscenza di dati personali sono tenuti al **rispetto del segreto d'ufficio** e, nei casi previsti, al **segreto professionale**, tenendo anche conto di quanto previsto dall'art. 9 del Codice di condotta aziendale.

→ Art. 9 -Obbligo di riservatezza e protezione dati - informazioni confidenziali - social network

Il Personale non può acquisire, raccogliere, utilizzare, processare, trasmettere o rivelare informazioni personali su dipendenti, collaboratori o terzi in modi non conformi alla politica dell'Azienda in materia di privacy o a tutte le altre leggi o regolamenti applicabili. Le informazioni personali includono, a titolo esemplificativo ma non esaustivo, nome, identità sessuale, indirizzo, Codice Fiscale o altri codici rilasciati dalle autorità, numero di telefono, indirizzo e-mail e altre informazioni simili. Altre informazioni confidenziali sono salario, stato di salute e dati contenuti nel file personale di ciascun membro del Personale.
Le informazioni non pubbliche, confidenziali e aziendali, incluse informazioni che si riferiscono ad affari presenti o futuri, a fornitori, venditori, concorrenti e/o clienti ("informazioni confidenziali") costituiscono un bene prezioso per l'Azienda. "Segreti" e "know how" commerciali fanno parte delle informazioni confidenziali, che includono tuttavia una serie più ampia di informazioni. Le informazioni confidenziali comprendono, ma non solo:

- software, sistemi, database, documentazioni e tutti i dati in essi contenuti;
- informazioni su attività finanziarie (inclusi investimenti, profitti, politica di prezzo, costi e contabilità);
- marketing, pubblicità, programmi e strategie di vendita;
- fusioni, acquisizioni o disinvestimenti;
- informazioni sul personale (inclusi compensi, procedure di assunzione e di formazione);
- piani strategici dell'Azienda

A prescindere dall'aver stipulato o meno un accordo formale di riservatezza con l'Azienda, il Personale è tenuto a proteggere la riservatezza di tutte le informazioni da considerarsi tali e che siano state ricevute dall'Azienda e/o dai suoi fornitori, venditori, clienti, concorrenti o che si riferiscano a essi. Il Personale non può rivelare (neanche ai familiari) o utilizzare informazioni confidenziali per scopi diversi da quelli strettamente necessari per garantire l'espletamento del loro lavoro all'interno dell'Azienda. Allo stesso modo, il Personale non può cercare di ottenere, di venire a conoscenza o di utilizzare le informazioni confidenziali che non siano utili al fine di eseguire il proprio lavoro in azienda. Tale obbligo dura per tutto il periodo di impiego in azienda e anche al termine di esso.
Il Personale è tenuto a non discutere di questioni confidenziali quando si trova in presenza o a portata di voce di persone non autorizzate, come ad esempio in ascensori (anche in azienda), ristoranti, taxi, aerei o altre aree accessibili al pubblico. Telefoni cellulari e altri mezzi di comunicazione devono essere utilizzati con attenzione.
Il Personale non può divulgare attraverso i social network informazioni riservate, come le circolari aziendali, la corrispondenza interna, informazioni di terze parti di cui è a conoscenza (ad esempio partner, istituzioni, utenti, stakeholder, etc...) o informazioni su attività lavorative, servizi, progetti e documenti di cui è a conoscenza per ragioni d'ufficio.
Fermi restando il corretto esercizio delle libertà sindacali e del diritto di critica, non è consentita la trasmissione e diffusione di messaggi minatori ovvero ingiuriosi, commenti e dichiarazioni pubbliche offensive nei confronti

dell'Azienda, riferiti alle attività istituzionali svolte e più in generale al suo operato, che per forma e/o i contenuto possano comunque nuocere all'Azienda ledendone l'immagine o il prestigio o compromettendone l'efficienza.
Il Personale deve rispettare la privacy dei colleghi e, ad eccezione di eventi pubblici che si svolgono presso la sede di lavoro, non può divulgare foto, video, o altro materiale multimediale che riprenda locali aziendali e personale senza l'esplicita autorizzazione delle strutture e delle persone coinvolte.
E' fatto divieto al Personale di utilizzare il logo o l'immagine dell'Azienda su account personali.
La modalità d'uso privato di social networking non è consentita quando il dipendente è in servizio durante l'orario di lavoro.

Ogni uso illecito o non conforme dei dati personali è **esclusiva responsabilità della persona che ne è causa**, anche sotto il profilo disciplinare, civile e penale, ai sensi del d.lgs. 196/2003 e del Regolamento (UE) 2016/679.

Comunicazione e divulgazione dei dati personali

La **comunicazione di dati personali** deve avvenire nel **rispetto del principio del "need to know"**, in forza del quale le informazioni personali possono essere condivise solo con soggetti che, in ragione delle proprie mansioni, **abbiano effettiva necessità di conoscerle** per svolgere le attività aziendali di loro competenza.
Tale limitazione si applica anche tra persone autorizzate al trattamento: **il solo fatto di essere incaricati o autorizzati non legittima l'accesso o la condivisione di dati se non strettamente necessario** per lo svolgimento delle proprie mansioni. Si applica altresì il principio di **minimizzazione**, che impone di limitare l'accesso, l'uso e la comunicazione dei dati al **minimo indispensabile** rispetto alla finalità perseguita.
La **comunicazione verso l'esterno** dei dati personali è consentita **esclusivamente**:

- **nei limiti delle finalità previste** dall'informativa sul trattamento dei dati personali;
- **previa nomina del destinatario quale responsabile del trattamento**, ai sensi dell'art. 28 del Regolamento (UE) 2016/679, oppure
- **in esecuzione di obblighi di legge o ordini dell'autorità**, ove applicabile.

Prima di procedere alla comunicazione dei dati, anche quando legittima, è necessario:

- **verificare con certezza l'identità del soggetto richiedente** e la **qualifica/titolo legittimante** la richiesta;
- **accertarsi dell'esattezza e dell'aggiornamento dei dati** oggetto di comunicazione;
- **registrare, ove previsto, l'operazione di comunicazione** secondo le procedure aziendali.

Non è consentito fornire dati personali per via telefonica, nemmeno nei confronti di amministrazioni pubbliche o autorità giudiziarie, se non a seguito di **richiesta scritta** (trasmessa tramite lettera, PEC, fax o e-mail istituzionale) che consenta di verificarne l'identità del richiedente,l'autenticità, il contenuto e le finalità.
Ogni comunicazione non conforme potrà costituire **violazione della normativa vigente**, con le conseguenti responsabilità disciplinari, civili e penali in capo al soggetto responsabile della violazione.
Qualora il **fax sia ancora in uso**, **è consentita esclusivamente la ricezione di documenti**, attraverso apparecchiature aziendali presidiate o dotate di sistemi di archiviazione sicuri e/o l'invio di tali documenti a sedi e/o uffici aziendali.

La divulgazione dei dati personali è vietata salvo i casi **previsti dalla legge.**

TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Istruzioni per la custodia e per la protezione di dati personali

Gli atti, i documenti e i supporti contenenti dati personali devono essere **custoditi con la massima cura**, evitando che soggetti non autorizzati possano venirne a conoscenza. In particolare:

- **atti e documenti cartacei** contenenti dati personali, sensibili o riservati devono essere **conservati in armadi o cassetti chiusi a chiave**, collocati in **locali ad accesso controllato**;
- non è consentito **lasciare documenti incustoditi** su scrivanie, ripiani o in luoghi visibili a terzi, anche se si tratta di lettere, fax o copie cartacee temporanee;
- in caso di stampa di documenti tramite **stampanti condivise o in ambienti comuni**, i documenti devono essere **ritirati immediatamente**;
- **fotocopie o copie di documenti** devono essere conservate con le stesse modalità previste per gli originali.

- al termine delle attività, gli atti devono essere **riposti negli archivi dotati di serratura** e gli ambienti adeguatamente **chiusi e protetti** (porte, finestre, armadi).

Istruzioni per l'accesso agli spazi e protezione dell'ambiente fisico

Al fine di garantire la riservatezza, l'integrità e la sicurezza dei dati personali trattati, è necessario adottare misure adeguate per la **protezione degli ambienti fisici** in cui tali dati sono custoditi, sia su supporto cartaceo che elettronico.
In particolare:

- i **locali e gli uffici in cui si trovano archivi, dispositivi o documentazione contenente dati personali** devono essere **inaccessibili a soggetti non autorizzati**. L'accesso deve essere consentito **esclusivamente al personale espressamente incaricato** o autorizzato al trattamento dei dati, secondo le designazioni aziendali;
- laddove possibile, l'**accesso deve essere regolato da misure fisiche di protezione**, quali **chiusure a chiave, badge elettronici, serrature digitali**, oppure **sorvegliato visivamente da un incaricato** presente in loco;
- eventuali **visitatori, fornitori o soggetti terzi esterni** devono essere **accompagnati** o comunque trattenuti **in aree appositamente dedicate**, prive di documentazione riservata, dispositivi informatici attivi o elementi dai quali sia possibile desumere dati personali;
- al termine della giornata lavorativa, o comunque nei momenti di **assenza del personale**, è obbligatorio **chiudere porte e finestre** e verificare che **gli armadi o i contenitori di documentazione riservata siano regolarmente chiusi a chiave**;
- è inoltre raccomandata, nei casi in cui le attività si svolgono in ambienti condivisi, la predisposizione di misure che garantiscano la **protezione visiva e fisica dei dati**, come l'utilizzo di **paratie, coperture documentali o schermature per monitor**.

L'inosservanza delle misure sopra indicate può costituire violazione dei principi di **riservatezza, integrità e disponibilità** dei dati personali, come sanciti dal Regolamento (UE) 2016/679, e comportare responsabilità personali e disciplinari.

Istruzioni per la distruzione di dati personali

La distruzione dei **documenti cartacei contenenti dati personali**, qualora necessaria, deve essere effettuata in modo **sicuro, controllato e definitivo**, al fine di impedire qualsiasi possibilità di ricostruzione, accesso non autorizzato o riutilizzo delle informazioni in essi contenute.
In particolare:

- la distruzione deve avvenire preferibilmente **tramite apparecchiature specifiche**, quali **distruggi-documenti** a taglio incrociato o microframmentazione, in grado di ridurre il materiale cartaceo a frammenti non ricomponibili;
- nel caso in cui l'ufficio o il servizio non disponga temporaneamente di tali dispositivi, è necessario adottare **modalità alternative di distruzione**, che garantiscano comunque l'illeggibilità del contenuto. A titolo esemplificativo, i documenti dovranno essere **strappati manualmente in modo accurato** oppure sminuzzati in più parti, prestando attenzione a **separare fisicamente le sezioni contenenti dati personali** (es. nominativi, codici fiscali, dati sanitari) e a **smaltirle in contenitori diversi**;
- **non è ammesso il semplice cestinamento** dei documenti contenenti dati personali, anche se obsoleti o parzialmente inutilizzabili. Tali comportamenti sono contrari ai principi di sicurezza del trattamento e possono esporre l'organizzazione a sanzioni amministrative, civili e penali;
- l'eventuale **smaltimento tramite servizio esterno** deve avvenire solo **per il tramite di soggetti formalmente incaricati o nominati responsabili del trattamento**, che offrano **garanzie adeguate** in termini di riservatezza, sicurezza e tracciabilità delle operazioni;
- si raccomanda infine di **non accumulare documentazione da distruggere** per lunghi periodi: la distruzione deve avvenire **non appena i dati risultano non più necessari rispetto alle finalità per cui sono stati raccolti o trattati**, secondo quanto previsto dalle policy interne sulla conservazione dei dati.

TRATTAMENTI CON L'AUSILIO DI SUPPORTI RIMOVIBILI

Utilizzo dei Supporti Rimovibili

I **supporti rimovibili**, quali **chiavette USB, dischi esterni, CD, DVD, schede di memoria e altri dispositivi di archiviazione portatili**, rappresentano strumenti utili per il trasferimento e la conservazione temporanea di dati. Tuttavia, il loro impiego può comportare rischi significativi per la **sicurezza delle informazioni aziendali**, inclusi accessi non autorizzati, perdita o divulgazione indebita di dati e introduzione di malware nei sistemi informatici. Pertanto, è fondamentale attenersi alle seguenti linee guida:

- l'utilizzo di supporti rimovibili è **vietato**, salvo esplicita autorizzazione da parte della Direzione o del Responsabile. In caso di necessità operativa comprovata, il personale deve richiedere per iscritto l'autorizzazione, specificando le motivazioni e la tipologia di dati da trattare.
- sui supporti rimovibili possono essere memorizzate solo copie di dati personali. I dati sensibili o riservati trasferiti su supporti rimovibili devono essere **crittografati,** utilizzando strumenti conformi agli standard aziendali. Le chiavi di crittografia devono essere gestite secondo le policy interne.
- prima dell'utilizzo, ogni supporto rimovibile deve essere sottoposto a una **scansione antivirus completa** per prevenire l'introduzione di software malevolo nei sistemi aziendali.
- **i** supporti rimovibili devono essere conservati in **luoghi sicuri**, preferibilmente in armadi chiusi a chiave. Durante il trasporto, è necessario adottare misure atte a prevenire smarrimenti o furti, come l'utilizzo di custodie protettive e il mantenimento dei dispositivi sempre sotto controllo diretto;
- quando la necessità di utilizzo dei dati personali memorizzati sui supporti rimovibili si esaurisce, si deve provvedere alla loro tempestiva eliminazione e al ripristino del supporto alla sua configurazione originaria;
- quando un supporto rimovibile giunge al termine del suo ciclo di vita, deve essere **distrutto o reso inutilizzabile** in modo sicuro, per impedire il recupero dei dati in esso contenuti;
- **è vietato** l'utilizzo di supporti rimovibili personali per scopi lavorativi, così come l'uso di dispositivi aziendali per fini personali, al fine di prevenire contaminazioni incrociate e garantire la protezione dei dati aziendali.

L'inosservanza delle presenti disposizioni può comportare sanzioni disciplinari, in conformità con il regolamento interno e le normative vigenti, inclusi il **Regolamento (UE) 2016/679 (GDPR)** e il **D.Lgs. 196/2003**.

TRATTAMENTI CON L'AUSILIO DI STRUMENTI ELETTRONICI

Sicurezza logica

La **sicurezza logica** rappresenta l'insieme delle misure adottate per garantire che l'accesso ai sistemi informatici e ai dati personali avvenga in modo controllato, tracciabile e conforme alle disposizioni vigenti, assicurando **robustezza, affidabilità e riservatezza**.

Accesso ai dati personali sul Sistema Informativo

Per "Sistema Informativo" s'intende l'insieme degli strumenti informatici hardware e software, compresi account di posta elettronica, utilizzati per veicolare, condividere e archiviare e utilizzare i dati personali raccolti e utilizzati dalla Società come titolare del trattamento.

L'accesso ai dati personali trattati mediante il **Sistema Informativo** aziendale avviene esclusivamente attraverso dispositivi informatici dotati di **procedura di autenticazione**. Tale procedura prevede l'utilizzo di **account personali** composti da **USER ID,** al quale è associata una **PASSWORD**.

- Lo USER ID è personale e univoco, assegnato dall'Amministratore di Sistema. Non può essere condiviso con altri incaricati, nemmeno in tempi diversi.
- La PASSWORD deve essere modificata al primo utilizzo e, successivamente, con cadenza almeno **trimestrale**. A tal fine è attivo un sistema automatico di scadenza della password.
- In funzione della sensibilità dei dati trattati, possono essere previsti ulteriori meccanismi di autenticazione avanzata (es. **autenticazione a due fattori – MFA**, **PIN**, **impronta digitale**, **pattern grafico**), ove consentiti o richiesti.

Gestione degli account utente e delle profilazioni

L'Amministratore di Sistema assicura che ogni account sia **univocamente associato a un singolo utente**, e che siano adottate misure idonee a **prevenire l'uso improprio o la condivisione**.

- In fase di assunzione, o in caso di modifica delle mansioni, la Direzione comunica all'Amministratore di Sistema:
    - le esigenze di accesso alla rete;
    - l'attivazione della casella *e-mail* e delle aree di memorizzazione file;
    - i profili di accesso al *software* gestionale e alle banche dati pertinenti alle attività dell'utente.

Gestione della password

Ogni utente è **responsabile della propria password**, che deve essere trattata come **dato strettamente personale e riservato**. Una gestione poco attenta può compromettere la sicurezza dei dati e rendere inefficace il meccanismo di autenticazione.

- in caso di **sottrazione, sospetta compromissione o smarrimento**, il lavoratore deve **informare tempestivamente l'Amministratore di Sistema**, il quale provvederà a ripristinare l'accesso con una nuova password;
- l'utente è ritenuto **responsabile per tutti gli accessi effettuati con le proprie credenziali**, anche qualora ne abbia permesso l'uso improprio da parte di terzi;

Requisiti tecnici della password

La password deve rispettare le seguenti caratteristiche minime:

- essere composta da **almeno 8 caratteri alfanumerici** (o più, in base al sistema);
- contenere almeno **tre** dei seguenti elementi:
    - una **lettera maiuscola**;
    - una **lettera minuscola**;
    - un **numero**;
    - un **carattere speciale**;
- non essere **uguale alla precedente**;
- non contenere riferimenti facilmente riconducibili all'utente (es. nome, cognome, soprannome, data di nascita, nomi comuni, animali, città).

Buone prassi per la gestione sicura delle credenziali

Il lavoratore deve:

- non comunicare la propria password ad altri;
- non lasciare la password scritta su post-it o fogli visibili;
- non annotare la password su supporti cartacei incustoditi;
- non digitare la password in presenza di terzi.

Raccomandazioni aggiuntive:

- evitare di utilizzare la stessa password per più applicazioni;
- non usare parole tratte da proverbi, canzoni, film, nomi noti o dizionari;
- ricorrere a **tecniche mnemoniche** per creare password complesse ma memorizzabili.

Esempi di creazione di password efficaci:

- Nel 1998 ho traslocato a Modena → IO98->MO
- Il mio cane pesa 12 chili → ImC=12Kg
- Andare al mare o in montagna? → AaM!iM?

Accesso al Sistema Informativo in caso di assenza prolungata, programmata o non programmata

Al fine di garantire la continuità operativa dell'azienda e far fronte ad adempimenti di legge, sia in caso di assenza programmata che di assenza non programmata di un dipendente abilitato al trattamento di dati personali, i documenti e le informazioni aziendali sono preventivamente archiviati e condivisi in cartelle accessibili anche ad altro lavoratore dotato di ruolo, profilo, mansioni e autorizzazioni equivalenti.

Qualora documenti o informazioni siano detenuti unicamente da un singolo dipendente, e risultino indispensabili per adempiere ad obblighi di legge perentori o per far fronte a esigenze aziendali non procrastinabili, il Titolare del trattamento dovrà, in via prioritaria, tentare di contattare il dipendente assente, affinché quest'ultimo possa, anche da remoto, collaborare nella gestione del caso.

Ove non sia possibile stabilire un contatto con il dipendente, e ricorrano le condizioni sopra descritte, è eccezionalmente consentito all'Amministratore di sistema, previa comunicazione al Titolare del trattamento, autorizzare l'accesso ai dati da parte di altro lavoratore, preferibilmente e preventivamente indicato dal dipendente assente, con ruolo, profilo e mansioni equivalenti, limitatamente allo spazio del server aziendale assegnato al dipendente assente.

Il lavoratore autorizzato all'accesso dovrà operare nel rispetto del principio di minimizzazione, trattando esclusivamente i dati strettamente necessari per far fronte alla specifica esigenza.

Di tale circostanza verrà data tempestiva comunicazione al dipendente interessato, non appena possibile.

Passi da seguire in caso di cessazione del rapporto di lavoro

Alla **cessazione del rapporto di lavoro**:

- l'account personale di accesso al Sistema informativo dovrà essere disattivata entro **10** giorni dalla cessazione del rapporto di lavoro;
- La cancellazione effettiva dell'account, con relativi file log di sistema e di navigazione, sarà effettuata entro **30** giorni dalla disattivazione dell'account.

Prima della cessazione del rapporto di lavoro, Il Responsabile di riferimento e il lavoratore individuano soluzioni atte a mantenere la disponibilità dei documenti e delle informazioni aziendali, compresi quelli contenenti dati personali della Società, memorizzati nel Sistema Informativo del lavoratore.

L'utilizzo dei PC fissi e portatili

Il personal computer (fisso o portatile), le relative applicazioni e i software installati costituiscono **strumenti di lavoro assegnati al dipendente** per l'espletamento delle proprie mansioni. Ogni utilizzo che non sia strettamente connesso all'attività lavorativa può determinare **disservizi, costi aggiuntivi e vulnerabilità per la sicurezza informatica** aziendale.

Il dipendente è **personalmente responsabile** dell'uso corretto e diligente del personal computer.

Regole di utilizzo

- il personal computer deve essere **custodito con attenzione** e utilizzato esclusivamente per fini **aziendali**, in relazione alle mansioni affidate;
- l'utilizzo per **scopi personali** è vietato, così come qualunque uso contrario alla legge o alle politiche aziendali.

Comportamenti vietati

Al lavoratore non è consentito:

- utilizzare strumenti hardware o software atti a **intercettare, alterare, falsificare o sopprimere comunicazioni o documenti informatici**;
- installare o utilizzare **software non approvati o non licenziati ufficialmente** dalla Direzione;
- modificare le **configurazioni preimpostate** sul proprio PC;
- scaricare o visualizzare file da **supporti magnetici/ottici privi di attinenza con le attività lavorative** (es. file musicali o multimediali);
- installare **modem o mezzi di comunicazione propri**;
- ascoltare file audio o musicali se non per esigenze strettamente connesse all'attività lavorativa;
- riprodurre o duplicare software in violazione della normativa sul diritto d'autore (L. n. 128/2004);
- eseguire **sistemi operativi "live"** (es. da CD/DVD, chiavi USB, hard disk esterni) o utilizzare **tecniche di virtualizzazione** non autorizzate;
- collegare **dispositivi personali** (PC portatili, smartphone, tablet) alla rete aziendale senza preventiva autorizzazione della Direzione.

Obblighi di sicurezza

- il **PC deve essere spento** al termine della giornata lavorativa o in caso di assenza prolungata dall'ufficio;
- in caso di allontanamento temporaneo dalla postazione, è obbligatorio **attivare il salvaschermo protetto da password** oppure **disconnettersi dal sistema**;
- lasciare un computer incustodito e connesso alla rete rappresenta un **rischio per la sicurezza** e può consentire accessi non autorizzati non tracciabili, di cui l'utente potrebbe essere ritenuto responsabile.

Buone prassi

- si raccomanda di mantenere **ordinato il desktop** del proprio PC. Un'eccessiva presenza di file, icone o collegamenti rallenta il caricamento del profilo all'avvio e può compromettere la produttività e le prestazioni della macchina.

Utilizzo della rete Wi-Fi aziendale da parte di persone esterne

L'accesso alla rete informatica della Società è **strettamente regolamentato**, al fine di tutelare la sicurezza dei sistemi aziendali e prevenire accessi non autorizzati.

- **ai visitatori occasionali non è consentito connettere i propri dispositivi alla rete aziendale**;
- **ai Consulenti, collaboratori e soggetti esterni che operano stabilmente e/o in modo continuativo** presso la Società potrà essere resa disponibile la rete Wi-Fi aziendale, ovvero, ove disponibile, una **rete Wi-Fi "Guest"**, separata logicamente dalla rete interna e priva di accesso alle risorse aziendali;

Qualsiasi violazione delle presenti disposizioni potrà comportare l'immediata revoca dell'accesso e, ove ne ricorrano i presupposti, la segnalazione alle competenti autorità.

Copyright e licenze d'uso

Solamente il software coperto da licenza d'uso può essere utilizzato nell'ambito del Sistema Informativo, pertanto, relativamente a qualsiasi software (programmi, file, immagini, testi, video, suoni, ecc.), gli utenti si impegnano a richiedere alla Direzione un'autorizzazione scritta prima di procedere a qualsiasi copia, download o installazione di qualsiasi genere

Ciascuna Direzione Aziendale provvederà a:

- redigere e mantenere aggiornato un elenco delle licenze d'uso disponibili in Società
- verificare periodicamente (almeno una volta ogni anno) il sw installato sui computer.

Utilizzo dei Server Aziendali

I server di 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 o sui PC locali.
Ogni utente è tenuto a memorizzare i propri file nella/e area/e del Sistema Informativo appositamente predisposta/e, e non dovrà memorizzare file nel "desktop" in quanto quest'ultimo non è sottoposto alle procedure di backup.
Particolare attenzione deve essere riposta nell'archiviare documenti a carattere riservato all'interno di cartelle situate sui server e condivisibili da più utenti del medesimo servizio o da parte di più uffici; è necessario infatti evitare che tali documenti possano essere letti o addirittura modificati da persone non autorizzate.
Sui Server vengono inoltre svolte le comuni e regolari attività di controllo, amministrazione e backup da parte del personale addetto.

Prevenzione dei malware

I virus sono programmi in grado di trasmettersi in modo autonomo e possono causare effetti dannosi. Alcuni virus si limitano a riprodursi senza ulteriori effetti, altri si limitano alla semplice visualizzazione di messaggi sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido.
Oggi, meglio che soltanto di virus, è più corretto parlare di *malware*, che oltre ai virus comprendono -a titolo esemplificativo e non esaustivo- i cosiddetti *trojan* (cavalli di Troia), gli *Spyware* e altri strumenti e modalità di attacco difficilmente classificabili.
I mezzi a disposizione per difendersi dai *malware* includono la protezione dagli accessi non autorizzati, il ricorso esclusivo a fonti note e sicure per dati e programmi, l'uso dei software *antimalware* aggiornati.

L'Amministratore di Sistema, provvederà a:

- far installare e mantenere aggiornato un adeguato software antimalware;
- cancellare ogni malware intercettato e documentare ogni caso che si verifichi;
- segnalare la presenza di file potenzialmente dannosi e richiederne la rimozione.
-
- E' responsabilità dell'utente:
- evitare di introdurre consciamente un malware nei computer;
- utilizzare esclusivamente i supporti di memorizzazione (CD, DVD, USB, cassette, ecc.) ricevuti in dotazione;
- non utilizzare programmi non autorizzati o software gratuito prelevato da siti Internet o in allegato a riviste o libri;
- ogni programma deve essere sottoposto alla scansione prima di essere installato;
- non utilizzare supporti già adoperati in precedenza o preformattati;
- non scaricare da Internet, se non previa autorizzazione, file eseguibili o documenti da siti FTP;
- non scaricare da Internet file di cui non si conosce o non si è ragionevolmente sicuri della fonte;
- evitare di navigare in siti non consentiti o non affidabili (vedi anche più avanti l'apposito paragrafo "L'utilizzo di Internet");
- non aprire e-mail di cui non si è certi della fonte, né i relativi allegati, in particolare se si dovesse trattare di file eseguibili (.exe) o compressi (.zip);
- evitare di "cliccare" sui collegamenti (link) proposti all'interno delle e-mail;
- contattare immediatamente l'Amministratore di Sistema qualora dovesse riscontrare o sospettare la presenza di malware nel computer che sta utilizzando.

La Società 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 del presente manuale.

Gestione dei backup / Archiviazione

Dati gestiti sui server centralizzati.

I dati e i file di lavoro devono essere archiviati sulle partizioni personali o dell'ufficio di appartenenza dei server centralizzati.
Il sistema di rete è predisposto per la copia automatizzata dei dati contenuti nei server centralizzati.
Costituisce buona regola la pulizia periodica (almeno ogni sei mesi) degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. E' infatti assolutamente da evitare un'archiviazione ridondante.

Dati gestiti sui PC locali o portatili

Ove per l'archiviazione dei dati non siano utilizzati server centralizzati ma PC locali o portatili, sarà cura dell'incaricato stesso provvedere a trasferire appena possibile nella propria area di memorizzazione (cartella) del Sistema Informativo i dati salvati nel PC: i dati saranno così soggetti alle procedure di backup standard controllate dall'Amministratore di Sistema.

Il trasferimento dei dati nelle cartelle del server deve avvenire con frequenza commisurata alla frequenza con cui i dati sono aggiornati o, nel caso di utilizzo di PC portatili, ogni volta che l'utente rientra in sede e si collega alla rete aziendale.

INTERNET

L'utilizzo di Internet

Il sistema informativo ed i dati in esso contenuti possono subire gravi danneggiamenti per un utilizzo improprio della connessione alla rete Internet; inoltre, attraverso la rete possono essere introdotti nel sistema virus informatici Spyware, Malware, e possono attraverso "backdoor" penetrare utenti non autorizzati.

Internet è da considerarsi uno strumento aziendale e pertanto l'utilizzo di Internet da parte dei lavoratori dovrà essere adeguato a scopi e obiettivi aziendali e conforme agli standard di comportamento dell'Azienda.

E' sempre vietato l'utilizzo di Internet per scopi illegali, non etici o rischiosi per l'Azienda.

Per salvaguardare la sicurezza del Sistema Informativo, è impedito, tramite l'uso di strumenti software dedicati, l'accesso ad alcune categorie di siti internet considerati potenzialmente pericolosi o incompatibili con l'etica della Società.

E' sempre espressamente vietato:

- navigare in siti che possono rivelare le opinioni politiche, religiose o sindacali del lavoratore;
- accedere a siti web dal contenuto offensivo, pornografico, discriminatorio per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica o comunque illegale in qualsiasi formato (programmi, immagini, testi, video, suoni, …)
- memorizzare documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- scaricare file di grandi dimensioni ed effettuare navigazioni ad elevato consumo di banda, se non espressamente autorizzato dalla Direzione;
- scaricare software gratuiti (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dalla Direzione;

A corollario di quanto sopra, si raccomanda di non fornire a terzi notizie relative a strumenti informatici, nominativi di utenti, procedure o qualsiasi altro elemento potenzialmente utilizzabile per attacchi miranti a danneggiare il Sistema Informativo.

Documentazione dell'attività di navigazione

L'accesso ai siti internet da parte degli utenti può essere documentato automaticamente in un file di log che riporta, in forma anonima e tale da precludere l'immediata identificazione degli utenti, i dettagli della navigazione, ed elenca i siti e i documenti che gli utenti hanno consultato.
I log file sono memorizzati in modo protetto e potranno eventualmente essere visionati da:

- Legali rappresentanti dell'Azienda;
- Amministratori di sistema (solo per fini legati alla sicurezza informatica).

POSTA ELETTRONICA

Utilizzo della posta elettronica

Si precisa che la casella di posta aziendale assegnata al dipendente è uno strumento di lavoro; pertanto l'utente dovrà assicurarsi che ogni contatto sulla propria email aziendale sia dovuto a ragioni esclusivamente professionali.

Le persone assegnatarie delle casella di posta elettronica sono responsabili del corretto utilizzo delle stesse. In particolare queste dovranno di norma controllare la posta in arrivo almeno una volta al giorno e, se necessario, inoltrare correttamente e tempestivamente la posta in entrata non a loro direttamente indirizzata.

Ai dipendenti non è consentito:

- utilizzare l'account personale di posta elettronica aziendale ("nome.cognome@dominio.società.it) per motivi non attinenti allo svolgimento delle mansioni assegnate;
- utilizzare l'account personale di posta elettronica aziendale per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail-list salvo diversa ed esplicita autorizzazione assegnate;
- spedire o far circolare catene di messaggi ("catene di Sant'Antonio" e simili);
- richiedere su detto account l'invio di e-mail ad uso personale o che non riguardano le attività lavorative;
- inviare o ricevere messaggi dal contenuto offensivo, pornografico, discriminatorio per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica o comunque illegale in qualsiasi formato (programmi, immagini, testi, video, suoni, …);
- diffondere opinioni personali come se fossero opinioni aziendali;
- diffondere messaggi di provenienza dubbia;
- utilizzare la mail personale (non aziendale) per comunicare con l 'azienda, ove sia stata fornita una utenza aziendale.

Si ricorda che i messaggi di posta elettronica viaggiano in chiaro e sono pertanto intercettabili da chiunque con pochissima difficoltà. Si richiede quindi particolare attenzione nell'utilizzare la posta elettronica esterna per inviare documenti di lavoro "riservati" in quanto possono essere intercettati da estranei.

La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati di grande dimensione.

Si raccomanda di fare attenzione agli allegati di posta elettronica prima del loro utilizzo, non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti e, in caso di dubbio, contattare l'Amministratore di Sistema.

Procedura per accedere alla posta del lavoratore assente.

La società adotta le opportune procedure al fine di garantire la continuità del servizio in caso di assenza del lavoratore.

In caso di assenza programmata, al lavoratore è richiesto di attivare la funzione di risposta automatica contenente l'indicazione della durata dell'assenza e di un contatto alternativo al quale rivolgersi in caso di urgenza, oppure l'inoltro automatico a un collega .

Nel caso di assenza non programmata, salvo che non vi possa provvedere il dipendente anche da remoto, l'Amministratore di sistema, su richiesta del titolare del trattamento che segnala tale impossibilità, attiva la procedura prevista per l'assenza programmata.

In caso di estrema urgenza tale da poter compromettere l'operatività aziendale o l'adempimento di obblighi di legge, solo qualora non possa provvedervi personalmente il lavoratore, ove le modalità sopra descritte non siano risultate sufficienti (es. ricezione di una e-mail prima dell'attivazione del risponditore automatico in caso di assenza non programmata), su disposizione scritta del titolare del trattamento, sarà consentito all'Amministratore di sistema, di accedere eccezionalmente alle e-mail strettamente necessarie alla risoluzione della problematica e verificare il contenuto dei messaggi. Di tale procedura viene data comunicazione al dipendente non appena possibile.

Procedura in caso di cessazione del rapporto di lavoro

La casella di posta elettronica con dominio aziendale ad uso personale sarà disattivata entro 10 giorni dalla cessazione del rapporto di lavoro, con contestuale impostazione di un messaggio automatico contenente dati di contatto alternativi per le future comunicazioni aziendali. Detta casella di posta elettronica sarà cancellata entro 30 giorni dalla sua disattivazione.
Il Titolare del trattamento informa preventivamente il dipendente nel caso in cui la sua casella di posta elettronica aziendale ad uso personale dovesse essere conservata per esigenze di operatività aziendale, sicurezza e *compliance*. In tal caso, salvo che non sia possibile individuare soluzioni alternative, il Titolare del trattamento raccoglie esplicito consenso scritto da parte del dipendente, il quale avrà cura di eliminare eventuali comunicazioni elettroniche strettamente personali (es. buste paga e/o referti medici al Medico competente, ecc.).

Posta elettronica di gruppo

Gli account di posta elettronica aziendale non nominativi (es. info@..., segreteria@..., ecc.), riferibili a specifiche aree o uffici, possono essere utilizzati da più dipendenti appartenenti al medesimo ufficio o area di competenza, a condizione che ciascun soggetto sia formalmente autorizzato al trattamento dei dati personali eventualmente contenuti nelle comunicazioni gestite tramite tale account.

TELEFONI AZIENDALI FISSI

Telefoni aziendali fissi

I telefoni aziendali sono uno strumento di lavoro dato in dotazione dall'Azienda ai lavoratori per l'espletamento delle loro mansioni.
Se si hanno a disposizione dei telefoni con dispositivo 'Viva Voce', ci si deve sincerare che l'ascolto della conversazione sia effettuato con la porta chiusa evitando che persone non interessate alla conversazione possano ascoltare.

TELEFONI CELLULARI AZIENDALI

Telefoni cellulari

I telefoni cellulari (compresi smartphone e altri dispositivi di telefonia mobile) sono assegnati in dotazione per l'uso lavorativo.
In generale, i telefoni non possono essere ceduti né fatti utilizzare a terzi, compresi colleghi, collaboratori, consulenti, salvo che il telefono non sia sin dall'origine destinato ad uso promiscuo.
In particolare, in modo non esaustivo, vengono posti i seguenti divieti:

- non è consentito modificare le caratteristiche hardware e software impostate sul telefono.
- non è consentita l'installazione di programmi (App) diversi da quelli autorizzati.
- non è consentita la riproduzione, la duplicazione, il salvataggio o lo scarico (download o file sharing) di programmi o file di ogni tipo (testo, immagini, video, audio, eseguibili) in violazione delle norme sul diritto d'autore, ai sensi delle Legge n. 128 del 21 maggio 2004.
- non è consentita l'installazione di ulteriori dispositivi rispetto a quelli in dotazione.
- non è consentito l'uso di qualsiasi dispositivo esterno collegabile al telefono, se non quelli aziendali o quelli autorizzati.

I telefoni cellulari assegnati al personale sono **protetti da codice PIN**, definito dall'**Ufficio Ragioneria**, che lo comunica direttamente al dipendente al momento della consegna del dispositivo.
Il **PIN assegnato non è modificabile**, salvo **casi eccezionali** debitamente motivati. In tali ipotesi, il dipendente è tenuto a **comunicare tempestivamente la modifica all'Ufficio Ragioneria**, fornendo le necessarie motivazioni.
È **vietato l'utilizzo di sistemi di riconoscimento biometrico** (quali impronte digitali o riconoscimento facciale) per l'accesso al dispositivo aziendale, al fine di garantire il rispetto delle politiche interne in materia di protezione dei dati personali e sicurezza informatica.
I dati personali presenti su cellulari o palmari aziendali ad uso personale saranno cancellati, mediante inizializzazione o ripristino delle impostazioni di fabbrica, entro 30 giorni dalla loro consegna e comunque prima che siano assegnati ad altro dipendente.

CONTROLLI E VIOLAZIONI

La società si riserva la facoltà di effettuare controlli difensivi, anche a distanza tramite gli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e per registrare gli accessi e delle presenze. Detti controlli difensivi possono essere collettivi oppure individuali, ed essere svolti in presenza del dipendente o in sua assenza. I controlli difensivi, inoltre, sono svolti purché sussistano comprovate esigenze di protezione di interessi e beni aziendali. Sono pertanto vietati controlli generici o immotivati, preventivi e sistematici. Sono inoltre ammessi ulteriori controlli a difesa del patrimonio aziendale se legittimati da accordi sindacali ai sensi dell'art. 4, c. 3, Statuto dei lavoratori.

Oltre a tali controlli, l'Azienda, ai fini di sicurezza o per motivi tecnici e per la propria tutela, si riserva di effettuare controlli, saltuari ed occasionali, nei limiti consentiti dalle norme vigenti e nelle modalità previste dal citato provvedimento del Garante. Detti controlli vengono eseguiti in modo preliminare su dati aggregati e comunque anonimi, nel pieno rispetto dei principi di pertinenza e non eccedenza e, salvo impossibilità dettata dall'urgenza, conclusi da avvisi generalizzati. Perdurando le condizioni di anomalia, saranno a questo punto giustificati controlli su base individuale. Nei casi di accertata violazione delle disposizioni contenute nel presente regolamento, è demandata alla Direzione che ha la competenza del servizio l'applicazione dei necessari provvedimenti disciplinari, fermo restando l'obbligo di segnalare alla competente Autorità Giudiziaria eventuali violazioni costituenti reato. La responsabilità, anche penale, specificatamente prevista dal D.Lgs. 196 del 30 giugno 2003 per un eventuale uso dei dati personali conosciuti non conforme alle indicazioni impartite dal titolare o dal responsabile, resta a carico della singola persona cui l'uso illegittimo sia imputabile. In caso di sanzioni di natura pecuniaria o richieste di risarcimento danni, l'Azienda ha la facoltà di rivalersi sull'autore materiale dell'illecito.

GESTIONE DELLE RICHIESTE DA PARTE DEGLI INTERESSATI

In conformità a quanto previsto dal **Regolamento (UE) 2016/679 (GDPR)**, i dipendenti che ricevono, in qualunque forma, una richiesta da parte di un interessato relativa all'**esercizio dei diritti in materia di protezione dei dati personali** (quali, a titolo esemplificativo: accesso, rettifica, cancellazione, limitazione, opposizione, portabilità) sono tenuti a **non rispondere autonomamente**, salvo **espressa autorizzazione da parte del Titolare del trattamento**.
Tali richieste devono essere **tempestivamente trasmesse al Titolare del trattamento**, anche per il tramite del proprio responsabile, corredate da ogni elemento utile alla corretta istruttoria.
Il Titolare, eventualmente con il supporto del Responsabile della protezione dei dati (DPO) ove designato, **valuterà la fondatezza della richiesta e provvederà a riscontrarla nei termini e con le modalità previste dalla normativa vigente**.
Il rispetto di tale procedura è essenziale per garantire **l'uniformità, la correttezza e la tracciabilità** delle risposte fornite agli interessati e per tutelare l'Ente da eventuali responsabilità in caso di risposte inappropriate o incomplete.

SEGNALAZIONI INCIDENTI DI SICUREZZA

Il personale è tenuto a **comunicare tempestivamente al Titolare del trattamento**, anche per il tramite del proprio responsabile, **qualsiasi incidente di sicurezza**, anche solo **presunto**, che possa comportare una **violazione dei dati personali**.
La segnalazione dovrà includere **ogni informazione utile** a consentire al Titolare del trattamento di **valutare la gravità dell'evento** e di adempiere agli **obblighi previsti dalla normativa vigente**, con particolare riferimento:

1. agli **obblighi di notifica al Garante per la protezione dei dati personali**, ai sensi dell'art. 33 del Regolamento (UE) 2016/679 (GDPR);
2. all'eventuale **comunicazione della violazione agli interessati**, ai sensi dell'art. 34 del medesimo Regolamento.