ECO LAN

ECOLOGICA LANCIANO

LANCIANO

(Provincia di Chieti)

REGOLAMENTO

per la sicurezza dei dati aziendali

INDICE

1. INTRODUZIONE

Il presente documento definisce alcune regole di utilizzo delle risorse informatiche ECO. LAN. S.P.A. per i propri dipendenti. Il documento si presenta strutturato come segue:

- Assegnazione e gestione del personal computer
- Credenziali di autenticazione
- Internet e posta elettronica
- Antivirus
- Backup
- Disattivazione temporanea del personal computer
- Regole per gli incaricati al trattamento di dati personali nello svolgimento delle attività di trattamento

Tutti i dipendenti ECO. LAN. S.P.A. che hanno ricevuto in dotazione risorse informatiche aziendali devono attenersi alle regole elencate.
Le regole dell'ultimo paragrafo devono essere rispettate da tutti i dipendenti che, in funzione delle mansioni svolte, effettuano operazioni di trattamento di dati personali e per ciò sottoscrivono una lettera di incarico.
Per quanto qui non specificato è richiesto comunque un atteggiamento ispirato alla correttezza ed alla buona fede.
In caso di problemi tecnici, necessità di informazioni, ecc., ciascun dipendente può rivolgersi al Help Desk ECO. LAN. S.P.A. al numero 0872.716332.
In caso di necessità di informazioni in merito ai trattamenti di dati personali effettuati in azienda, ciascun dipendente può rivolgersi agli uffici amministrativi.

2. ASSEGNAZIONE E GESTIONE DEL PERSONAL COMPUTER

A ciascun dipendente ECO. LAN. S.P.A. può essere assegnato un personal computer in funzione delle esigenze connesse alle mansioni svolte in azienda e su richiesta del responsabile dell'unità organizzativa cui appartiene.
L'assegnazione del PC avviene previa sottoscrizione della dichiarazione di accettazione dello strumento.
Le risorse informatiche così assegnate dall'azienda al dipendente devono essere da questo conservate con la massima cura ed utilizzate per le sole attività aziendali e non per scopi personali.
Devono essere prontamente segnalati all'azienda il furto, il danneggiamento e lo smarrimento.
Onde evitare il grave pericolo di introdurre virus informatici nonché di alterare la stabilità delle applicazioni dell'elaboratore non è consentito installare alcun programma, proveniente dall'esterno o dall'interno, se non espressamente autorizzati dall'Amministratore di Sistema.
In ogni caso l'azienda si riserva il diritto ad accedere in qualunque momento alle risorse informatiche assegnate al dipendente per effettuare attività di monitoraggio, controllo e/o aggiornamento, al fine della gestione del parco pc e della sicurezza del sistema e della rete, nel rispetto delle norme legali e contrattuali.
Per ogni malfunzionamento dello strumento il dipendente può rivolgersi all' Help Desk ECO. LAN. S.P.A..

3. CREDENZIALI DI AUTENTICAZIONE

Natura e caratteristiche delle Credenziali di Autenticazione.
A ciascun dipendente ECO. LAN. S.P.A. sono attribuite una o più credenziali di autenticazione per accedere al personal computer assegnatogli, alla rete aziendale ed ai suoi servizi. Le credenziali di autenticazione consistono in:

- un codice identificativo (nome utente)
- una parola chiave (password)

3.1 Natura e caratteristiche del codice identificativo

Il codice identificativo (nome utente) è costituito da una sequenza di lettere e caratteri coincidenti per convenzione con il nome e cognome del dipendente separati da un punto.
Tale codice deve essere:

- individuale: non può essere assegnato a persone diverse
- non è riutilizzabile: una volta assegnato ad una persona non può essere riassegnato nemmeno nell'ipotesi che l'originario assegnatario abbia cessato le proprie funzioni (in caso di omonimie, si provvederà a diversificare il codice utente mediante variazioni della sua composizione rispetto alla convenzione adottata)

3.2 Natura e caratteristiche della parola chiave

La parola chiave (password) rappresenta la componente riservata delle credenziali di autenticazione. La parola chiave deve essere sicura, conosciuta esclusivamente dalla persona cui è stata assegnata e dall'amministratore di sistema e non intuibile da altre persone. Per tali ragioni il dipendente deve utilizzare solo parole chiavi con la seguente struttura :

- avere una lunghezza minima di 8 (otto) caratteri
- essere costituita da una combinazione di caratteri alfabetici e numerici
- non essere facilmente associabile all'utilizzatore (non costituita da nomi propri, nomi di familiari, date di nascita, targhe autoveicoli, numeri telefonici)
- non essere costituita da sequenze di caratteri comunemente utilizzati (abcdefg.., aaaaaaa.., 111111.., ecc)
- non essere costituita da una semplice variazione sequenziale rispetto alla parola chiave precedente (parola chiave 1; parola chiave 2; ecc....)

3.3 Procedura di assegnazione

L'assegnazione delle credenziali di autenticazione consistenti nella parola chiave e nel codice identificativo avviene secondo la seguente procedura:

- il responsabile dell'area personale ovvero il responsabile dell'unità operativa presso la quale l'incaricato dovrà svolgere le proprie funzioni inoltra, anche tramite e.mail, all'Amministratore di Sistema, la richiesta di abilitazione del nuovo dipendente
- l'Amministratore di Sistema, ricevuta la richiesta, provvede all'assegnazione della parola chiave e del codice identificativo per il primo accesso alla rete ed ai vari applicativi consegnandola in busta chiusa all'utente

- l'Amministratore di Sistema, contestualmente all'assegnazione della parola chiave e del codice identificativo, abilita per ciascun nuovo dipendente, sulla base delle necessità operative dello stesso, un profilo utente, anche per classi, in linea con l'organigramma aziendale approvato.

Le Credenziali di Autenticazione saranno disattivate dall'Amministratore di sistema nel caso in cui vengano a mancare le ragioni che avevano giustificato l'attribuzione del diritto di accesso a dati

3.4 Utilizzo della parola chiave

Ciascun dipendente deve custodire e conservare con diligenza e riservatezza la propria parola chiave. Questo non deve consentire a terzi l'uso della propria parola chiave e deve ridurre al minimo i rischi che la stessa venga conosciuta da altri.
A tal riguardo la parola chiave non deve:

- essere scritta su foglietti o su altri supporti cartacei presenti all'interno della struttura lavorativa
- essere memorizzata su computer

Ciascun dipendente deve:

- sostituire la parola chiave assegnata, subito dopo averla ricevuta e comunque non più tardi del primo accesso all'elaboratore e/o ai dati;
- sostituire la propria parola chiave a intervalli non più lunghi di sei mesi, ridotti a tre in caso il dipendente sia stato incaricato al trattamento di dati sensibili o giudiziari. Si consiglia, ove possibile, di cambiare la password con più frequenza
- sostituire immediatamente la propria parola chiave se vi è ragione di temere che qualcuno l'abbia individuata

Ogni qualvolta venga sostituita la parola chiave il dipendente deve altresì comunicare la nuova password all'amministratore di sistema per l'uniformità con il sistema centrale e per l'aggiornamento dell'elenco password.

3.5 Procedure di emergenza

Nell'ipotesi in cui il dipendente non sia più in grado di ricordare e/o reperire la propria parola chiave oppure non sia fisicamente reperibile e vi sia la necessità di accedere ai dati da lui trattati, il soggetto interessato dovrà rivolgersi all' Help Desk ECO. LAN. S.P.A. che attiverà le dovute procedure di emergenza.

4. INTERNET E POSTA ELETTRONICA

Nel precisare che Internet e la Posta Elettronica sono strumenti di lavoro, si ritiene utile segnalare che non è consentito navigare in siti e utilizzare la posta elettronica (interna ed esterna) per motivi non attinenti allo svolgimento delle mansioni assegnate.
Ogni email inviata mediante utilizzo della casella di posta elettronica ECO. LAN. S.P.A.
dovrà obbligatoriamente riportare in calce la seguente frase:

Ai sensi del D.Lgs. 196/2003 si precisa che le informazioni contenute in questo messaggio sono riservate ed a uso esclusivo del destinatario. Qualora il messaggio in parola Le fosse pervenuto per errore, La invitiamo ad eliminarlo senza copiarlo e a non inoltrarlo a terzi, dandocene gentilmente comunicazione. Inoltre le dichiarazioni contenute nel presente messaggio nonché nei suoi eventuali allegati devono essere attribuite esclusivamente al mittente; opinioni, conclusioni o altre informazioni riportate nella e-mail, che non siano relative alle attività e/o alla missione aziendale di ECO. LAN. S.P.A. si intendono non attribuibili alla società stessa, né la impegnano in alcun modo. ECO. LAN. S.P.A. non assume responsabilità per eventuali intercettazioni, modifiche o danneggiamenti del presente messaggio di e-mail.

Si suggerisce di inserirla nel campo firma del sistema di gestione della posta elettronica in modo tale che il suo inserimento sia gestito in automatico dal software.

Si ricorda inoltre che sono **tassativamente vietate** e perseguibili amministrativamente, civilmente e, in taluni casi, anche penalmente le seguenti attività:

- accedere a siti ed acquisire o comunque diffondere prodotti informativi lesivi del comune senso del pudore;
- diffondere prodotti informativi lesivi dell'onorabilità, individuali o collettivi;
- diffondere prodotti informativi di natura politica al di fuori di quelli consentiti dalla legge e dai regolamenti;
- diffondere, in rete o con qualsiasi altro mezzo di comunicazione, informazioni riservate di qualunque natura;
- svolgere ogni tipo di acquisto o vendita di prodotto/servizi non riconducibili alla propria mansione o alla normale operatività aziendale;
- compiere attività che possono rappresentare una violazione della legge in materia di Copyright, fra le quali la copia non autorizzata di software, CD audio e video, clonazione o programmazione di smart card;
- compiere attività che compromettono in qualsiasi modo la sicurezza delle risorse informatiche e della rete aziendale;
- registrarsi a siti i cui contenuti non siano legati all'attività lavorativa;
- ogni altra attività illegale qui non elencata.

Poiché in caso di violazioni contrattuali o giuridiche, sia l'azienda, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'azienda si riserva il diritto di verificare, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e dell'integrità del proprio sistema informatico anche ai fini di garanzia della sicurezza del sistema e della rete.

5. ANTIVIRUS

Tutti i personal computer ECO. LAN. S.P.A. devono disporre di software antivirus, con
cadenza di aggiornamento automatico giornaliera.

Si suggerisce di verificare quotidianamente l'esito delle operazioni di aggiornamento mediante la visualizzazione del registro apposito (vedi le istruzioni operative).
Nel caso in cui il software antivirus non fosse installato o correttamente configurato il dipendente deve contattare l'Help Desk ECO. LAN. S.P.A. per le necessarie operazioni di installazione e/o configurazione.

5.1 Istruzioni operative per la verifica della installazione dell'antivirus

Per verificare l'installazione del software antivirus sul proprio pc si dovrà:

1. cliccare su START, in basso a sinistra sullo schermo
2. scegliere l'opzione PROGRAMMI e cliccare
3. scegliere l'opzione Microsoft Security Essentials e cliccare
4. scegliere la finestra Home
5. Verificare che le definizioni risultino aggiornate

Periodicamente l'amministratore di sistema procede ad effettuare controlli sul corretto funzionamento dell'antivirus.

6. SALVATAGGI PERIODICI

6.1 Gestione dei salvataggi periodici

I backup dei dati aziendali vengono gestiti centralmente mediante unità esterne di backup ed hanno cadenza due volte al giorno. Periodicamente l'amministratore di sistema provvede ad effettuare una copia di sicurezza dell'unità di backup.

6.2 Istruzioni operative per il backup

Per disporre di una copia di backup dei propri dati ogni utente deve utilizzare la cartella di rete a sua disposizione per il salvataggio dei dati aziendali da lui prodotti quotidianamente.
Tutti i dati salvati eventualmente sul proprio pc non saranno pertanto soggetti a backup automatico.

Le cartella di rete personale (identificata con il nome dell'utente) è accessibile dalla cartella "Rete CCSRL" disponibile sulla schermata desktop di ogni utente.

Al suo interno la cartella "Rete CCSRL" contiene anche ulteriori cartelle accessibili in funzione dei permessi specifici di ogni utente dove salvare copia dei dati soggetti a condivisione con altri utenti.

Nel caso in cui cartella "Rete CCSRL" non fosse raggiungibile dal proprio desktop il dipendente deve contattare l'Help Desk ECO. LAN. S.P.A. per le necessarie operazioni di configurazione.

7. DISATTIVAZIONE TEMPORANEA DEL PC

Al fine di una maggior riservatezza dei dati presenti sul proprio pc si suggerisce di

attivare la funzionalità screen saver con password. Tale funzionalità attiva uno screen saver dopo un certo numero di minuti di inattività del pc. Il ritorno alla normale operatività è subordinata all'inserimento di una password, conosciuta esclusivamente dall'utente.

7.1 Istruzioni operative per attivare screen saver con password

Per attivare lo screen saver con password sul proprio pc si dovrà:

1. cliccare con il pulsante destro del mouse su un punto qualunque del desktop
2. scegliere l'opzione PROPRIETA' e cliccare
3. cliccare sulla voce SCREEN SAVER
4. scegliere uno screen saver a proprio piacimento, inserire un flag alla voce protezione e indicare il tempo di attesa (tempo di inattività del pc trascorso il quale si attiva lo screen saver; impostarlo a 10 minuti)

In seguito a tali operazioni ogni qualvolta il pc sarà lasciato inattivo per più di 10 minuti si attiverà lo screen saver selezionato ed il ritorno alla normale operatività del pc sarà subordinata all'inserimento della password.

8. REGOLE PER GLI INCARICATI AL TRATTAMENTO DI DATI PERSONALI

8.1 Definizioni del Decreto legislativo 196/2003

Nel seguito si definiscono alcuni termini presenti nel regolamento che segue e connessi alla normativa in materia di protezione dei dati personali (Decreto legislativo 196/2003):

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;

Dato Personale: qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

Dato Sensibile: 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 organizzazioni a carattere religioso, filosofico, politico o sindacale, nonchè i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

Dato Giudiziario: i dati personali idonei a rivelare provvedimenti, 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;

Titolare è 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;

Responsabile è la persona fisica o giuridica preposta dal Titolare al trattamento dei dati personali;

Incaricato è il soggetto incaricato per iscritto dal Titolare o dal Responsabile di compiere operazioni di trattamento di dati personali e che opera sotto la loro diretta autorità;

Interessato è la persona fisica, giuridica l'ente o l'associazione, cui si riferiscono i dati personali.

In applicazione della normativa vigente in materia di protezione dei dati personali (D.Lgs. 196/2003), alcuni dipendenti sono stati "incaricati" al trattamento delle categorie di dati definite sopra. Di seguito si dettagliano le modalità di nomina, gli obblighi e alcune regole supplementari.

8.2 Nomina degli incaricati al trattamento di dati personali

L'incaricato è nominato dal Titolare del trattamento (ECO. LAN. S.P.A.) mediante atto scritto. Nella designazione dell'incaricato è individuata puntualmente l'unità operativa di appartenenza al fine di poter determinare l'ambito di trattamento consentito.

8.3 Obblighi degli incaricati al trattamento di dati personali

L'incaricato nell'effettuare le operazioni di trattamento dei dati deve rispettare tutte le istruzioni che verranno impartite dal Titolare e/o dal suo diretto responsabile. Tra queste dovrà:

- effettuare le operazioni di trattamento dei dati in modo lecito e secondo correttezza, esclusivamente al fine di adempiere agli obblighi insiti nel rapporto di lavoro, attenendosi alle regole relative alla tutela dei dati e delle informazioni – sia in termini di sicurezza che in materia di riservatezza;
- accedere ai soli dati personali la cui conoscenza sia strettamente necessaria e strumentale per l'espletamento delle mansioni affidate nell'ambito dell'unità operativa di appartenenza;
- verificare che i dati personali trattati siano esatti e completi e, se necessario, correggerli e aggiornarli;
- verificare che i dati personali trattati siano pertinenti e non eccedenti le finalità per le quali sono stati raccolti;

- cercare di limitare al massimo l'utilizzabilità di dati personali e di dati identificativi quando le finalità del trattamento consentono l'utilizzo del dato anonimo;
- astenersi dal trasferire, comunicare e diffondere i dati personali a soggetti terzi, se non per gli scopi connessi e strumentali alle mansioni affidate nell'ambito della unità operativa di appartenenza;
- astenersi, in caso di cessazione del rapporto di lavoro, dal conservare, duplicare, comunicare o diffondere a terzi i dati, di cui sia venuto a conoscenza in costanza del rapporto;
- in caso di allontanamento, anche temporaneo, dal posto di lavoro, verificare che non vi sia possibilità da parte di terzi, anche se dipendenti dell'azienda del Titolare, di accedere ai dati personali per i quali era in corso una qualunque operazione di trattamento, anche non automatizzata;
- in caso di allontanamento, anche temporaneo, dal posto di lavoro, spegnere l'elaboratore o bloccarne l'utilizzo tramite richiesta password.
- conservare i dati personali nel più rigoroso rispetto delle misure di sicurezza predisposte dal Titolare, avendo sempre cura di garantire la massima riservatezza in ogni operazione di trattamento effettuata;
- rispettare le disposizioni del presente regolamento.

8.4 Reimpiego dei supporti di memorizzazione

Le misure di sicurezza che seguono trovano applicazione nella gestione dei soli supporti di memorizzazione, contenenti dati che il D.lgs 196/2003 definisce come "sensibili o giudiziari".
Si tratta dei supporti utilizzati per il salvataggio e lo scambio di file, singolarmente o a gruppi. Si considerano quindi come supporti di memorizzazione i supporti magnetici e ottici come dischi fissi, floppy disk, pen drive, cd-rom, DAT, DLT. Il reimpiego dei supporti di memorizzazione effettuato con le modalità non rispondenti a quanto prescritto nel seguito costituisce una duplice minaccia alla sicurezza dei dati e ciò sotto il profilo della confidenzialità (perché i dati precedentemente salvati sul supporto sono leggibili da parte di colui che lo sta riutilizzando) e della integrità (perché il metodo della sovrascrittura rende inaffidabile il salvataggio), ed è pertanto vietato.

Al fine di evitare che l'utilizzo e il reimpiego dei supporti di memorizzazione costituisca una minaccia per la sicurezza dei dati dell'azienda, gli incaricati dovranno rispettare rigorosamente le seguenti regole:

- custodire i supporti di memorizzazione all'interno delle relative custodie avendo cura che gli stessi non siano accessibili a soggetti non autorizzati;
- reimpiegare i supporti che abbiano raggiunto la massima capacità di memorizzazione solo dopo aver proceduto ad una loro formattazione (la semplice cancellazione dei file non è sufficiente);
- nell'ipotesi in cui il personal computer utilizzato segnali che il disco fisso ha raggiunto la massima capacità di memorizzazione, avvertire immediatamente il proprio responsabile.

8.5 Procedure per il trattamento dei dati personali su supporti cartacei

Monitoraggio e classificazione degli archivi
Per archivi cartacei devono intendersi i vari luoghi ove sono fisicamente conservati gli atti e i documenti contenenti dati personali.

Vengono pertanto considerati archivi:
- gli armadi e i contenitori in genere contenenti atti e documenti ubicati all'interno dei singoli uffici (archivi di ufficio);
- i locali adibiti esclusivamente a contenere gli atti e i documenti presenti all'interno della struttura aziendale (archivi di piano);
- le unità immobiliari esterne alla struttura aziendale, adibite alla conservazione degli atti e dei documenti aziendali (archivi generali).

Il Titolare e/o il Responsabile del trattamento provvedono a censire, con cadenza annuale, gli archivi cartacei aziendali verificando le tipologie di dati personali presenti in ognuno di essi e la loro ubicazione.

Gli archivi cartacei aziendali devono essere classificati e suddivisi a seconda che contengano:
- soltanto dati personali comuni;
- anche dati sensibili o giudiziari.

Modalità di archiviazione
Gli incaricati, addetti a ciascuna unità operativa, possono accedere esclusivamente a quei dati personali necessari per svolgere le mansioni connesse con l'unità stessa.

Gli atti e i documenti contenenti dati personali devono essere conservati all'interno di archivi con **accesso selezionato**.

Gli atti e i documenti contenenti dati sensibili o giudiziari devono essere conservati all'interno di archivi con **accesso selezionato e controllato**.

Questo comporta che:
- gli archivi di ufficio devono essere chiusi a chiave quando viene meno la possibilità di controllo diretto (quando cioè non vi sia alcun incaricato presente in ufficio), ovvero quando sono posizionati nei corridoi esterni all'ufficio. La chiave degli archivi di ufficio deve essere conservata da un responsabile individuato all'interno dell'ufficio stesso.
- gli archivi di ufficio devono contenere esclusivamente i dati personali necessari per svolgere le mansioni connesse con l'unità operativa di cui fa parte l'ufficio;
- gli archivi di piano devono essere sempre chiusi a chiave. La chiave deve essere conservata a cura di un responsabile a cui spetta selezionare gli accessi;
- gli archivi di piano, contenenti dati personali afferenti a trattamenti di unità operative diverse, devono essere dotati di una compartimentazione interna che non permetta l'accesso indiscriminato a tutti i dati;

- gli archivi generali devono essere accessibili solo da personale a ciò incaricato.

Modalità di accesso agli archivi
Gli incaricati hanno accesso di norma agli archivi dalle ore 8.00 alle ore 14.00 dal lunedì al venerdì e dalle ore 15.30 alle ore 18.30 nei giorni di martedì e giovedì. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

Archivi di ufficio
Detti archivi sono liberamente accessibili da tutti gli incaricati facenti parte dell'unità operativa alla quale appartiene l'ufficio. Gli altri incaricati per poter consultare detti archivi dovranno rivolgersi al responsabile dell'unità operativa il quale, verificati i diritti di accesso del richiedente, ne consente l'accesso.

Archivio di piano
Detti archivi non sono liberamente accessibili dagli incaricati. L'incaricato per poter consultare detti archivi dovrà rivolgersi al soggetto responsabile delle chiavi il quale, verificati i diritti di accesso del richiedente, ne consente l'accesso.

Archivi generali
Detti archivi non sono liberamente accessibili dagli incaricati. L'incaricato per poter consultare detti archivi deve inoltrare una richiesta scritta al personale incaricato all'accesso, il quale provvede a reperire l'atto e il documento richiesto e alla consegna all'incaricato.

Modalità di consultazione
Regole per la consultazione di atti e di documenti contenenti dati personali:

- gli atti e i documenti contenenti dati personali devono essere sempre conservati negli archivi ed affidati agli incaricati solo per il tempo strettamente necessario per il trattamento;
- gli atti e i documenti contenenti dati personali prelevati dagli archivi devono essere conservati a cura dell'incaricato e restituiti al termine delle operazioni affidate.

Se gli atti e i documenti contengono dati sensibili o giudiziari:
- gli stessi devono, durante il periodo in cui sono prelevati dall'archivio e fino alla restituzione, essere conservati in contenitori muniti di serratura;
- non è consentito lasciarli sulle scrivanie, o in luoghi comunque accessibili anche se in fase di temporanea sospensione della trattazione.

Trasferimento degli atti e dei documenti
Il trasferimento dei dati, non può avvenire a soggetti diversi da quelli incaricati e autorizzati al trattamento, in ragione della mansione svolta ed entro i limiti della stessa.

L'invio degli atti e dei documenti contenenti dati sensibili o giudiziari, anche all'interno della struttura aziendale, deve avvenire:

- se consegnati a mano: avendo cura di recapitarli personalmente al destinatario in busta chiusa, evitando di lasciarli incustoditi su scrivanie o altri luoghi accessibili;
- se via posta (anche interna): in busta chiusa o pacco chiuso riservato al destinatario;
- se via fax: avendo cura di inviarli sull'apparecchio fax ubicato all'interno dell'unità operativa del destinatario ovvero avendo cura di preavvertire lo stesso prima dell'invio.