SOLIDALIA SOCIETA' COOPERATIVA SOCIALE

via Del progresso, 26 Vigonza 35010 (PD)
Tel. 049.626980
Website: www.coopsolidalia.it
E-Mail: dpo@coopsolidalia.com

POLICY DI SICUREZZA INFORMATICA E PROCEDURE PER LA ICT SECURITY

ai sensi degli artt. 32 del Regolamento Generale Europeo sulla Protezione dei Dati G.D.P.R. 679/2016

Stato delle revisioni

Versione	*Data*	*Descrizione*	*Autore*
00	*27/05/2018*	*Prima emissione*	***Amm di Sistema***
01	*10/05/2020*	*Aggiornamento procedure*	***Amm di Sistema - D.P.O.***
02	*24/05/2022*	*Aggiornamento procedure*	***Amm di Sistema - D.P.O.***

SOMMARIO

PREMESSA

Premesso che i comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, tra i quali rientrano l'utilizzo delle risorse informatiche e telematiche, devono sempre ispirarsi al principio di diligenza e correttezza, l'azienda ha adottato il presente Disciplinare Interno diretto ad evitare che condotte inconsapevoli possano innescare problemi o minacce alla sicurezza dei dati o delle attrezzature aziendali.

Il presente documento contiene le istruzioni operative per il trattamento dei dati personali, ai sensi dell'art. 4 numero 1, 13, 14, 15 del Regolamento Ue 2016/679 (di seguito anche solo "GDPR").

I dipendenti, i collaboratori, i consulenti ed in generale tutte le persone autorizzate ad accedere ai dati personali e preposte allo svolgimento delle operazioni di trattamento relativa ai dati, devono ispirarsi a un principio generale di diligenza e correttezza.

Ogni utilizzo dei dati in possesso dell'Azienda diverso da finalità strettamente professionali, è espressamente vietato. Di seguito vengono esposte le regole comportamentali da seguire per evitare e prevenire condotte che anche inconsapevolmente potrebbero comportare rischi alla sicurezza del sistema informativo.

L'ambito lavorativo porta l'azienda a gestire una serie di dati e informazioni anche riguardanti i dati tutelati dall'art. 9 e 10 di persone fisiche (interessati).

Tali informazioni possono essere considerate, ai sensi dell'art. 4 numero 1, 13, 14, 15 del GDPR, "dati personali" quando sono riferite a persone fisiche e, per la loro gestione (Trattamento), sia cartacea che digitale, è necessario adottare una serie di misure adeguate e idonee ad assicurare la loro protezione.

Altre informazioni, pur non essendo classificabili "dati personali" sono in tutto e per tutto "informazioni riservate", ovvero informazioni tecniche, commerciali, contrattuali, di business o di altro genere per le quali l'azienda è chiamata a garantire la riservatezza, o per N.D.A. (Non Disclosure Agreement – accordo di non divulgazione e riservatezza), o per una più ampia tutela del patrimonio aziendale.

Ai fini di questo disciplinare si specifica, pertanto, che con il termine "dati" deve intendersi l'insieme più ampio di informazioni di cui un dipendente o un collaboratore può venire a conoscenza e di cui deve garantire la riservatezza e la segretezza e non solo i "dati personali" intesi a norma di legge.

Inoltre, nell'ambito della sua attività, l'azienda tratta "dati cartacei" ovvero informazioni su supporto cartaceo e "dati digitali" ovvero informazioni che vengono memorizzate o semplicemente transitano attraverso apparecchiature digitali.

In linea generale, ogni dato, nell'accezione più ampia sopra descritta, di cui l'autorizzato viene a conoscenza, nell'ambito della propria attività lavorativa, è da considerarsi riservato e non deve essere comunicato o diffuso a nessuno (anche una volta interrotto il rapporto lavorativo con l'azienda stessa o qualora parte delle informazioni siano di pubblico dominio) salvo specifica autorizzazione esplicita.

Anche tra colleghi, oppure tra dipendenti e figure esterne all'organico aziendale, è necessario adottare la più ampia riservatezza nella comunicazione dei dati conosciuti, limitandosi solo a quei casi che si rendono necessari per espletare al meglio l'attività lavorativa richiesta e comunque nel rispetto delle istruzioni ricevute.

Inoltre, la progressiva diffusione delle nuove tecnologie informatiche ed in particolare l'accesso diffuso alla rete internet attraverso i computer aziendali, espone l'azienda a possibili rischi di un coinvolgimento di rilevanza sia civile, sia penale, sia amministrativa, creando problemi alla sicurezza, al business e alla reputazione dell'azienda stessa.

Una gestione dei dati cartacei, un uso dei COMPUTER e di altri dispositivi elettronici (di seguito ANCHE SOLO "DISPOSITIVI") nonché dei servizi di internet e della posta elettronica difforme dalle regole contenute nel presente Disciplinare potrebbe esporre l'azienda ad aumentare la minaccia di accessi non autorizzati ai dati e/o al sistema informatico aziendale, furti o divulgazioni di informazioni riservate nonché furti o danneggiamenti del sistema informatico e/o malfunzionamenti in generale dell'intero sistema informatico.

Le informazioni contenute nel presente Disciplinare vengono rilasciate anche ai sensi dell'art. 13 del GDPR e costituiscono, quindi, parte integrante dell'informativa rilasciata agli autorizzati al trattamento dei dati e più in generale a tutti i dipendenti dell'azienda.

DEFINIZIONI

Secondo l'articolo 4 del GDPR, si definisce:

- **Dato personale**: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- **Trattamento**: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'utilizzo, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- **Violazione dei dati personali**: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

ADEMPIMENTI

Ciascun autorizzato del trattamento deve:

- Rispettare i principi generali del GDPR, con particolare riferimento alla liceità e correttezza del proprio agire, all'obbligo di procedere alla raccolta e alla registrazione dei dati per scopi determinati, espliciti e legittimi;
- Rispettare l'obbligo di riservatezza e segretezza e conseguentemente il divieto di comunicazione e diffusione dei dati trattati nel corso dell'incarico svolto;
- Utilizzare i dati, cui abbia accesso, solamente per finalità compatibili all'esecuzione delle proprie mansioni o dei compiti affidati, per cui è autorizzato ad accedere alle informazioni e ad utilizzare gli strumenti aziendali;
- Rispettare le misure di sicurezza idonee adottate dalla società, atte a salvaguardare la riservatezza e l'integrità dei dati;
- Segnalare eventuali malfunzionamenti di strumenti elettronici, perdite di dati o esigenze (sia di natura organizzativa, sia tecnica), che possano migliorare lo svolgimento delle operazioni affidate;
- Accedere ai dati strettamente necessari all'esercizio delle proprie funzioni e competenze;
- In caso di interruzione del lavoro, anche temporanea, verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- Mantenere riservate le proprie credenziali di autenticazione;
- Svolgere le attività previste dai trattamenti secondo le direttive del responsabile del trattamento dei dati; non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento dei dati;
- Rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- Informare l'ADS in caso di incidente di sicurezza che coinvolga dati particolari e non;
- Eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge.

TITOLARITA' DEI DISPOSITIVI E DEI DATI

L'azienda è esclusiva titolare e proprietaria dei dispositivi messi a disposizione del personale ai soli fini dell'attività lavorativa.

L'azienda è l'unica esclusiva titolare e proprietaria di tutte le informazioni, le registrazioni ed i dati contenuti e/o trattati mediante i propri dispositivi digitali o archiviati in modo cartaceo nei propri locali.

Il dipendente non può presumere o ritenere che le informazioni, le registrazioni ed i dati da lui trattati o memorizzati nei dispositivi aziendali (inclusi i messaggi di posta elettronica e/o chat inviati o ricevuti, i file di immagini, i files di filmati o altre tipologie di files) siano privati o personali, né può presumere che dati cartacei in suo possesso possano essere da lui copiati, comunicati o diffusi senza l'autorizzazione dell'organizzazione.

FINALITA' NELL'UTILIZZO DEI DISPOSITIVI

I dispositivi assegnati sono uno strumento lavorativo nelle disponibilità del dipendente esclusivamente per un fine di carattere lavorativo. I dispositivi, quindi, non devono essere utilizzati per finalità private e diverse da quelle aziendali, se non eccezionalmente e nei limiti evidenziati dal presente Disciplinare.

Qualsiasi eventuale tolleranza da parte della azienda, apparente o effettiva, non potrà, comunque, legittimare comportamenti contrari alle istruzioni contenute nel presente Disciplinare.

UTILIZZO DELLA RETE INTERNET AZIENDALE

La connessione alla rete internet dal dispositivo avuto in dotazione 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 disciplinare.

In particolare, si vieta l'utilizzo dei social network, se non espressamente autorizzati.

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

In particolare, nell'uso della rete internet il dipendente si deve attenere alle seguenti disposizioni:

- È vietata la navigazione nei siti che possono rivelare le opinioni politiche religiose, sindacali e di salute del dipendente poiché potenzialmente idonea a rivelare dati sensibili ai sensi del GDPR;
- È fatto divieto di accedere 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;
- È vietato al dipendente il download di software (anche gratuito) disponibile nei siti web;
- È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dal Titolare e con il rispetto delle normali procedure di acquisto;
- È vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
- È vietata la partecipazione a forum non professionali, l'utilizzo di chat line, di bacheche elettroniche o partecipare a gruppi di discussione o lasciare commenti ad articoli o iscriversi a mailing list usando il marchio o la denominazione dell'azienda, salvo specifica autorizzazione dell'organizzazione stessa;
- È vietata la memorizzazione di documenti informatici di natura oltraggiosa, diffamatoria e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;
- È vietato al dipendente di promuovere utile o guadagno personale attraverso l'uso di Internet o della posta elettronica aziendale;
- È vietato accedere dall'esterno alla rete interna dell'organizzazione, salvo con le specifiche procedure previste dall'ente stesso;
- È vietato utilizzare l'accesso ad 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 s.m.i., d.lgs. 6 maggio 1999, n. 169 e legge 18 agosto 2000, n. 248). In particolare, è vietato il download di materiale soggetto a copyright (testi, immagini, musica, filmati, file in genere, …) se non espressamente autorizzato dall'organizzazione;
- È vietato, infine, creare siti web personali sui sistemi dell'organizzazione nonché acquistare beni o servizi su portali di e-commerce a meno che l'articolo acquistato non sia stato approvato a titolo di spesa professionale.

Ogni eventuale navigazione di questo tipo, comportando un illegittimo utilizzo di Internet, nonché un possibile illecito trattamento di dati personali e sensibili è posta sotto la personale responsabilità dell'Incaricato inadempiente.

ISTRUZIONI PER L'USO DEGLI STRUMENTI INFORMATICI E DELLA POSTA ELETTRONICA

Come principio generale, sia i dispositivi di memorizzazione del proprio personal computer desktop o laptop sia le unità di rete, devono contenere informazioni strettamente professionali e non possono essere utilizzate per scopi diversi (immagini, video e documenti personali).

Di seguito sono riportate le indicazioni per la gestione dei diversi strumenti informatici per il trattamento dati:

Gestione strumenti elettronici

Ciascun autorizzato è responsabile del corretto utilizzo e della custodia degli strumenti elettronici in dotazione (a

titolo esemplificativo ma non esaustivo personal computer desktop o laptop, periferiche, lettori di smart card, cellulari, tablet). Si devono adottare le misure di sicurezza per la tutela della riservatezza, consistenti nell'evitare che l'accesso ai dati possa avvenire da parte di soggetti estranei all'azienda o non specificamente autorizzati. Al fine di verificare il corretto utilizzo degli strumenti in dotazione potranno essere svolti controlli a campione mediante la raccolta e l'analisi di dati aggregati e anonimi. Inoltre, nel caso di provato o constatato uso illecito o non consentito degli strumenti elettronici, risultante dalla verifica delle informazioni in modalità aggregata e anonima, può essere necessario procedere alla verifica delle registrazioni delle sessioni di lavoro, al fine di sanzionare condotte illecite, anche su richiesta dell'autorità giudiziaria, cui le informazioni potranno essere comunicate, senza alcun consenso dell'interessato.

Per la gestione della sessione di lavoro sul personal computer desktop o laptop, è necessario che:

- al termine delle ore di servizio, il personal computer desktop o laptop deve essere spento, a meno che non stia svolgendo elaborazioni particolari. In tal caso gli uffici debbono tassativamente essere chiusi a chiave;
- Se l'autorizzato si assenta momentaneamente dalla propria postazione deve accertarsi che l'eventuale sessione di lavoro aperta non sia accessibile da altre persone. Pertanto, deve chiudere la sessione di lavoro sul personal computer desktop o laptop facendo Log out, oppure in alternativa deve avere attivo un salvaschermo (screen- saver) protetto dalle credenziali di autenticazione;
- Relativamente all'utilizzo dello screen-saver, occorre osservare le seguenti norme:
    - Non deve mai essere disattivato;
    - Il suo avvio automatico deve essere previsto non oltre i primi 5 minuti di inattività del personal computer desktop o laptop;
    - Deve essere messo in funzione manualmente ogni volta che si lascia il personal computer desktop o laptop incustodito ed acceso;
- Quando si esegue la stampa di un documento contenente dati personali, in particolare su una stampante condivisa, occorre ritirare tempestivamente i documenti stampati per evitare l'accesso a soggetti non abilitati al trattamento;
- Per l'utilizzo dei computer portatili valgono le regole elencate per i computer connessi alla rete, con le seguenti ulteriori raccomandazioni:
    - Prima della riconsegna, rimuovere eventuali file elaborati;
    - Quando il computer portatile è nei locali dell'Azienda, non lasciarlo mai incustodito;
    - Quando il computer portatile è all'esterno dell'Azienda, soprattutto in luogo aperti al pubblico ed in presenza di estranei, non lasciarlo mai incustodito;
    - Per assenze prolungate, anche qualora l'ambiente venga ritenuto "affidabile", è necessario custodire il portatile in modo opportuno es. cassaforte o armadio messo in sicurezza (chiuso a chiave);
    - In caso di furto del computer portatile è necessario avvertire tempestivamente l'ADS, il D.P.O. e il titolare del trattamento, onde prevenire possibili usi impropri dei dati ivi contenuti e/o intrusioni ai sistemi aziendali e valutare l'opportunità di avvio della procedura di Data Breach al Garante della Privacy;
    - In caso di viaggio aereo trasportare tassativamente il computer portatile come bagaglio a mano;
    - Eseguire periodicamente salvataggi dei dati e non tenere i supporti di backup insieme al computer portatile.

Gestione username e password

L'accesso al personal computer desktop o laptop, sia esso collegato in rete o meno, è protetto da un sistema di autenticazione che richiede all'Autorizzato di inserire sulla videata di accesso all'elaboratore un codice utente (username) ed una parola chiave (password). L'adozione ed il corretto utilizzo della combinazione username / password è fondamentale per il corretto utilizzo del personal computer desktop o laptop, in quanto:

- Tutela l'autorizzato al trattamento ed in generale l'Azienda da accessi illeciti, atti di vandalismo e, in generale, violazioni e danneggiamenti del proprio patrimonio informativo;
- Tutela l'autorizzato al trattamento da false imputazioni, garantendo che nessuno possa operare a suo nome e che, con il suo profilo (ossia con le sue user id e password) solo lui possa svolgere determinate azioni;
- È necessario per gestire correttamente gli accessi a risorse condivise.

Ciascun l'autorizzato al trattamento deve scegliere le password in base ai seguenti criteri (su indicazione del ADS):

- Devono essere lunghe almeno otto caratteri;
- Non devono fare riferimento ad informazioni agevolmente riconducibili ai soggetti utilizzatori o ai loro famigliari;
- Devono contenere una combinazione di numeri e/o segni speciali, lettere, maiuscole e minuscole;
- Non deve essere uguali alle precedenti.

Per la corretta gestione della password è necessario:

- Modificare la password almeno ogni 3 mesi;
- In caso di assegnazione di password di primo utilizzo, questa va modificata e sostituita con una personale, nel più breve tempo possibile;
- Conservare la password in un luogo sicuro;
- Non rivelare o condividere la password con i colleghi di lavoro, famigliari e amici, soprattutto attraverso il telefono e/o e-mail;
- Le password non devono essere memorizzate su alcun tipo di supporto, quali, ad esempio, Post-It (sul monitor o sotto la tastiera) o agende (cartacee, posta elettronica, telefono cellulare);
- Evitare di digitare la propria password in presenza di altri soggetti che possano vedere la tastiera, anche se collaboratori o dipendenti dell'azienda;
- Non utilizzare la funzione, offerta da alcuni software, di salvare automaticamente la password per successivi utilizzi delle applicazioni.

Installazione di hardware e software

L'installazione di hardware e software, nonché la modifica dei parametri di configurazione, possono essere eseguiti solamente dall'ADS.

Pertanto, si raccomanda agli utenti dei personal computer desktop o laptop di rispettare i seguenti divieti:

- Non utilizzare sul personal computer desktop o laptop dispositivi personali, o comunque non aziendali, quali lettori dispositivi di memorizzazione dei dati;
- Non installare sistemi per connessione esterne (es: modem, Wi-Fi); tali connessioni, aggirando i sistemi preposti alla sicurezza della rete aziendale, aumentano sensibilmente i rischi di intrusioni e di attacchi dall'esterno;
- Non installare programmi, anche in versione demo. In particolare, è vietata l'installazione di giochi, programmi in prova (shareware), programmi gratuiti (freeware), programmi pirata, e in generale tutti i software non autorizzati;
- Non modificare i parametri di configurazione del proprio personal computer desktop o laptop senza espressa autorizzazione e senza il supporto di personale tecnico qualificato.

Si ricorda che normalmente la condivisione di aree e di risorse del proprio personal computer desktop o laptop è vietata. Può essere autorizzata dall'ADS, solo in casi eccezionali e solo per il tempo strettamente necessario allo svolgimento delle attività di lavoro. In questi casi devono essere adottate password di lettura e scrittura e la condivisione deve operare solo su singole directory del personal computer desktop o laptop, e non sull'intero disco rigido.

Gestione posta elettronica aziendale

Il servizio di posta elettronica viene fornito per permettere la comunicazione con soggetti terzi interni ed esterni per le finalità della Azienda e in stretta connessione con l'effettiva attività e mansioni del lavoratore che utilizza tale funzionalità.

I dipendenti assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

Al fine di non compromettere la sicurezza della Azienda e di prevenire conseguenze legali a carico della stessa, bisogna adottare le seguenti norme comportamentali:

- Se si ricevono e-mail da destinatari sconosciuti contenenti file di qualsiasi tipo, procedere alla loro immediata eliminazione senza scaricare e/o aprire gli allegati sospetti;
- È fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list, salvo diversa ed esplicita autorizzazione;
- È vietato inviare, tramite la posta elettronica, anche all'interno della rete aziendale, materiale a contenuto violento, sessuale o comunque offensivo dei principî di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazione del pensiero, anche politico;
- È vietato inviare messaggi di posta elettronica, anche all'interno della rete aziendale, che abbiano

contenuti contrari a norme di legge ed a norme di tutela dell'ordine pubblico, rilevanti ai fini della realizzazione di una fattispecie di reato, o che siano in qualche modo discriminatori della razza, dell'origine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap;

- Qualora l'Incaricato riceva messaggi aventi tale contenuto, è tenuto a cancellarli immediatamente e a darne comunicazione all'ADS;
- La casella di posta elettronica assegnata deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti come dimensione;
- È vietato utilizzare il servizio di posta elettronica per trasmettere a soggetti esterni dell'azienda informazioni riservate o comunque documenti aziendali, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte;
- Nell'ipotesi in cui la e-mail debba essere utilizzata per la trasmissione di dati particolari (ex dati sensibili), si raccomanda di prestare attenzione a che:
    - l'indirizzo del destinatario sia stato correttamente digitato;
    - l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile;
    - nel corpo del messaggio sia presente il disclaimer in cui si avverta della confidenzialità/riservatezza del messaggio.

Nel caso di assenza prolungata si deve attivare il servizio di risposta automatica.

In alternativa e in tutti i casi in cui sia necessario un presidio della casella di e-mail per ragioni di operatività aziendale, il dipendente deve nominare un collega fiduciario con lettera scritta che in caso di assenza inoltri i files necessari a chi ne abbia urgenza.

Qualora l'Incaricato non abbia provveduto ad individuare un collega fiduciario o questi sia assente o irreperibile, l'organizzazione, mediante personale appositamente incaricato, potrà verificare il contenuto dei messaggi di posta elettronica dell'incaricato, informandone l'incaricato stesso e redigendo apposito verbale.

Gestione del salvataggio dei dati
Per i dati ed i documenti che risiedono sui server gestiti centralmente, come ad esempio cartelle di rete e database, il Servizio Informatico esegue i salvataggi con la possibilità di ripristinare in toto oppure selettivamente eventuali files distrutti, ad esempio per guasti hardware oppure per cancellazioni involontarie.

Per i dati ed i documenti che risiedono esclusivamente sul personal computer desktop o laptop, ogni Autorizzato deve eseguire almeno una volta alla settimana la copia (salvataggio, o backup). Questo allo scopo di garantire la disponibilità ed il ripristino dei Dati Personali nel caso di una generica compromissione delle risorse (cancellazioni accidentali, guasti, furti…).

Gestione dei supporti rimovibili
Ai dipendenti può essere assegnata una memoria esterna (quale un dispositivo USB, un hard disk esterno, una memory card, …) su cui copiare temporaneamente dei dati per un facile trasporto, o altri usi (es. macchine fotografiche con memory card, videocamere con dvd, …).

Questi dispositivi devono essere gestiti con le stesse accortezze di cui all'articolo precedente e devono essere utilizzati esclusivamente dalle persone a cui sono state affidate e, in nessun caso, devono essere consegnate a terzi.

I supporti rimovibili, quando contengono dati personali devono essere custoditi in luogo protetto e non accessibile (cassaforte, armadio chiuso a chiave, etc.). Quando non sono più utilizzati devono essere distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altro personale non autorizzato al trattamento degli stessi dati, soltanto dopo essere stati formattati. Tali operazioni vengono effettuate a cura dell'ADS. Il trasferimento di file contenenti dati personali, dati particolari (ex dati sensibili) e giudiziari su supporti rimovibili, è da eseguire unicamente in via transitoria, ponendo la massima attenzione alla destinazione di trasferimento e cancellando i file appena possibile. I dati particolari giudiziari devono essere crittografati.

Gestione protezione dai virus informatici
Per prevenire eventuali danneggiamenti al software causati dalla presenza o dall'azione di programmi virus informatici, su ogni elaboratore dell'Azienda è stato installato un software antivirus aziendale che si aggiorna automaticamente all'ultima versione disponibile.

L'antivirus aziendale non deve mai essere disattivato o sostituito con altro antivirus non ufficialmente approvato ed installato.

Nel caso il programma antivirus installato sul proprio personal computer desktop o laptop riscontri la presenza di un virus, oppure si sospetti la presenza di un virus non rilevato dal programma antivirus è necessario darne immediatamente segnalazione all'ADS.

Si raccomanda di non scaricare e né tantomeno aprire file provenienti via e-mail da mittenti sconosciuti. Tali file, possono essere portatori di virus e compromettere la funzionalità del personal computer desktop o laptop, l'integrità dei dati in essa contenuti e soprattutto l'integrità dei sistemi collegati al personal computer desktop o laptop stesso.

ISTRUZIONI PER L'USO DEGLI STRUMENTI "NON ELETTRONICI"

Per "non elettronici" si intendono sia documenti in formato cartaceo sia documenti in qualsiasi altro formato come ad esempio microfilm, badge, tessere identificative plastificate. I documenti di questo tipo contenenti dati particolari devono essere protetti in appositi armadi dotati di chiavi. Tutti i documenti contenenti dati particolari che si ritiene debbano essere eliminati devono essere distrutti definitivamente in modo irrecuperabile e non gettati nei cestini.

Per proteggere i dati personali è opportuno evitare il deposito di documenti di qualsiasi genere negli ambienti di transito o pubblici (corridoi o sale riunioni), come pure l'abbandono in vista sulle scrivanie quando ci si debba assentare dal proprio posto di lavoro. Nel caso di dati particolari, il rispetto di queste norme è obbligatorio.

Distruzione delle copie cartacee

Coloro che sono preposti alla duplicazione di documentazione (con stampanti o fotocopiatrici o altre periferiche) ovvero che utilizzano strumenti per la riproduzione cartacea di documenti digitali, sono tenuti a procedere alla relativa distruzione del supporto, qualora si verifichino errori o la riproduzione non sia corretta, evitando di riutilizzare i fogli di carta, distruggendoli definitivamente e immediatamente per mezzo di adeguate macchine distruggi documenti.

Prescrizioni per gli autorizzati

L'Autorizzato deve attenersi alle seguenti prescrizioni:

- In nessun caso è concesso l'accesso a documentazione contenente Dati Personali per motivi non dettati da esigenze di lavoro strettamente connesse ai trattamenti dichiarati, autorizzati e tutelati dal Titolare;
- La documentazione contenente Dati Personali che, per ragioni di praticità operativa, risiede sulle scrivanie degli Incaricati deve comunque essere rimossa e messa in sicurezza al termine dell'orario di lavoro;
- L'accesso ai supporti deve essere limitato al tempo necessario a svolgere i Trattamenti previsti;
- I supporti devono essere archiviati in ambiente ad accesso controllato;
- I documenti contenenti dati personali non devono essere lasciati incustoditi in un ambiente non controllato (ad es. a seguito della stampa dei documenti su stampante di rete);
- Il numero di copie di documenti contenenti Dati Personali deve essere strettamente funzionale alle esigenze di lavoro;
- Cassetti ed armadi contenenti documentazione riservata debbono tassativamente essere chiusi a chiave fuori dell'orario di lavoro;
- L'accesso fuori orario lavorativo a documenti contenti Dati particolari può avvenire da parte di personale Autorizzato, o tramite autorizzazione di quest'ultimo, unicamente previa registrazione dell'accesso a tali documenti;
- La distruzione di documenti contenenti Dati Personali deve essere operata, ove possibile, direttamente dal personale Autorizzato;
- Ove il volume dei documenti da distruggere sia tale da imporre il ricorso al servizio di macero, il personale Autorizzato che avvia al macero la documentazione è tenuto a confezionare tale documentazione in modo che il pacco risulti anonimo e solido;
- Quando gli atti e i documenti contenenti dati personali, dati particolari sono affidati agli autorizzati per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli autorizzati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate;
- L'accesso agli archivi contenenti dati particolari deve essere controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono

essere preventivamente autorizzate.
- È severamente vietato utilizzare documenti contenenti Dati personali, dati particolari come carta da riciclo o da appunti.

DATI DI INTERESSATI COMUNICATI ALLA NOSTRA AZIENDA DA ALTRI TITOLARI

Quando altri clienti e/o imprese/enti ci comunicano dati di persone fisiche (per qualsiasi motivo), la nostra azienda è comunque responsabile del corretto trattamento, mentre rimane titolare dei dati chi li comunica alla nostra azienda.

In questi casi l'autorizzato al trattamento deve richiedere al titolare una dichiarazione che ha verificato e ottenuto le autorizzazioni dagli interessati per la comunicazione/diffusione del dato.

CLEAR DESK POLICY

I dipendenti sono responsabili del controllo e della custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali.

I dipendenti devono adottare la "politica della scrivania pulita", trattando dati cartacei solo se necessario, privilegiando, ove possibile, l'utilizzo degli strumenti digitali messi a disposizione dell'azienda.

I principali benefici della "politica della scrivania pulita" sono:

- Una buona impressione a clienti e fornitori che visitano la nostra azienda;
- La riduzione della possibilità che informazioni confidenziali possano essere viste da persone non abilitate a conoscerle;
- La riduzione che documenti confidenziali possano essere sottratti all'organizzazione.

In particolare, si invita a non lasciare in vista sulla propria scrivania dati cartacei quando ci si allontana dalla stessa oppure quando è previsto un incontro con un soggetto non abilitato alla conoscenza dei dati in essi contenuti.

Prima di lasciare la propria postazione (per esempio per la pausa pranzo o per una riunione) sarà cura dei dipendenti riporre in luogo sicuro (armadio, cassettiera, archivio, …) i dati cartacei ad esso affidati, affinché gli stessi non possano essere visti da terzi non autorizzati (es. addetti alle pulizie) o da terzi (visitatori) presenti nell'ente.

A fine giornata deve essere previsto il riordino della scrivania e la corretta archiviazione di tutte le pratiche d'ufficio, in modo da lasciare la scrivania completamente sgombra.

Ove possibile, si invita ad evitare la stampa di documenti digitali, anche ai fini di ridurre l'inquinamento ed il consumo delle risorse in ottica ecologica.

Ove possibile, si invita ad effettuare la scansione dei documenti cartacei ed archiviarli digitalmente.

ISTRUZIONI PER L'USO DI DISPOSITIVI, CELLULARI E SMARTPHONE PERSONALI

Ai dipendenti non è permesso svolgere la propria attività su PC fissi, portatili, dispositivi personali.

Al dipendente, se espressamente autorizzato dall'azienda, è permesso solo l'utilizzo della posta elettronica aziendale sul dispositivo personale.

In tal caso è necessario che il dispositivo abbia password di sicurezza stringenti approvate dall'azienda e l'eventuale furto o smarrimento del dispositivo deve essere immediatamente segnalato anche all'azienda per eventuali provvedimenti di sicurezza.

Al dipendente è vietato l'utilizzo di memorie esterne personali (quali chiavi USB, memory card, cd-rom, DVD, macchine fotografiche, videocamere, tablet, …).

Durante l'orario di lavoro, comprese le eventuali pause, ai dipendenti è concesso l'utilizzo del telefono cellulare personale ma solo per comunicazioni di emergenza o strettamente collegate all'ambito lavorativo.

In caso di trasferte lavorative all'esterno degli uffici dell'azienda, il telefono personale può rimanere acceso, anche per facilitare la comunicazione con l'organizzazione stessa ove fosse necessario.

In questo caso si invita, comunque, a non utilizzarlo per fini personali, in modo particolare alla presenza di clienti o fornitori.

USO DEL CLOUD COMPUTING

Utilizzare un servizio di cloud computing per memorizzare dati personali o sensibili, espone l'azienda a potenziali problemi di violazione della privacy perché i dati vengono memorizzati nelle server farms di aziende che spesso risiedono in uno stato diverso da quello dell'azienda.

Il cloud provider, in caso di comportamento scorretto o malevolo, potrebbe accedere ai dati personali per eseguire ricerche di mercato e profilazione degli utenti.

Con i collegamenti wireless, il rischio sicurezza aumenta e si è maggiormente esposti ai casi di pirateria informatica a causa della minore sicurezza offerta dalle reti senza fili.

In presenza di atti illegali, come appropriazione indebita o illegale di dati personali, il danno potrebbe essere molto grave per l'azienda, con difficoltà di raggiungere soluzioni giuridiche e/o rimborsi se il fornitore risiede in uno stato diverso da paese dell'utente.

Si ribadisce che tutti i dati memorizzati nel cloud sono seriamente esposti a eventuali casi di spionaggio industriale.

È vietato ai dipendenti l'utilizzo di sistemi cloud non espressamente approvati dall'azienda. Per essere approvati i sistemi cloud devono rispondere ad almeno i seguenti requisiti:

- Essere sistemi cloud esclusivi e non condivisi;
- Essere sistemi cloud posizionati fisicamente in Italia;
- L'azienda che fornisce il sistema in cloud deve essere preventivamente nominata Responsabile al Trattamento dei dati da parte dell'ente;
- L'azienda che fornisce il sistema in cloud deve comunicare all'ente, almeno una volta all'anno, i nominativi degli amministratori di sistema utilizzati;
- Dovranno essere verificate tutte le indicazioni e prescrizioni previste dal Garante della Privacy nei suoi provvedimenti sugli Amministratori di Sistema e sul cloud.

RESTITUZIONE DEI DISPOSITIVI E DATI CARTACEI

A seguito di una cessazione del rapporto lavorativo con l'azienda o, comunque, al venir meno, ad insindacabile giudizio dell'azienda, della permanenza dei presupposti per l'utilizzo dei dispositivi aziendali e dati cartacei, i dipendenti hanno i seguenti obblighi:

- Procedere immediatamente alla restituzione dei dispositivi in uso;
- Divieto assoluto di formattare o alterare o manomettere o distruggere i dispositivi o i dati cartacei assegnati o rendere inintelligibili i dati in essi contenuti tramite qualsiasi processo.

NON OSSERVANZA DELLA NORMATIVA AZIENDALE

Il mancato rispetto o la violazione delle regole contenute nel presente disciplinare è perseguibile con provvedimenti disciplinari nonché con le azioni civili e penali consentite.

VALIDITA'

Il presente Disciplinare sarà oggetto di aggiornamento ogni volta che se ne ravvisi la necessità, in caso di variazioni tecniche dei sistemi dell'organizzazione o in caso di mutazioni legislative. Ogni variazione del presente Disciplinare sarà comunicata agli incaricati.

AFFISSIONE

Il presente Disciplinare verrà affisso nella bacheca aziendale e pubblicato sulla intranet aziendale ai sensi dell'art. 7 della legge 300/70 e del CCNL.

AGGIORNAMENTO E REVISIONE

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente disciplinare. Le proposte verranno esaminate dalla Direzione.