AZIENDA TERRITORIALE PER L'EDILIZIA RESIDENZIALE DELLA REGIONE UMBRIA

REGOLAMENTO E ISTRUZIONI

per i dipendenti in merito a quanto stabilito dal Regolamento Europeo General Data Protection Regulation (GDPR) EU 679/2016
e dal d.lgs 196/2003
"Codice in materia di protezione dei dati personali"

APPROVATO CON D.C.A. n° 24 del 12/06/2019

Premessa

Il Regolamento del 27 aprile 2016, cosiddetto "General Data Protection Regulation" (di seguito brevemente "GDPR"), pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 4 maggio 2016, diviene definitivamente operativo ed applicabile in via diretta in tutti i Paesi membri dell'Unione Europea a partire dal 25 maggio 2018 e persegue il fine di rafforzare la protezione dei dati personali delle persone fisiche, sia all'interno che all'esterno dei confini europei, dunque a prescindere dal principio di territorialità, armonizzando le regole privacy di tutti gli Stati membri.

L'adozione delle misure tecniche ed organizzative adeguate è imposta dagli artt. 24 e seguenti del GDPR, ai sensi dei quali le politiche interne e le misure da attuare per soddisfare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default, devono tener conto, in concreto, della natura, dell'ambito di applicazione, del contesto e delle finalità di trattamento nonché del rischio per i diritti e le libertà delle persone fisiche.

Al fine di rispettare tale requisito, l'elaborazione del presente modello ha richiesto la preventiva esecuzione di una attenta e critica attività di auditing, che ha consentito l'esame della singola realtà aziendale e della valutazione d'impatto sulla protezione dei dati personali.

Pertanto, a seguito di tali attività, vengono impartite le seguenti istruzioni atte a garantire un trattamento lecito, corretto, trasparente e sicuro dei dati.

Introduzione

Privacy, che significa?

Nell'attuale società, definita anche società della comunicazione, i dati personali hanno un valore determinante. Lo sviluppo di tecnologie, che consentono la conoscibilità, la conservazione e la comunicazione di dati in quantità e con velocità sempre maggiore, induce alla necessità di proteggere la sfera privata dell'individuo e il suo diritto alla riservatezza. La necessità di tutelare la persona in modo da garantirgli il ruolo di vero padrone delle informazioni che lo riguardano deve però fare i conti con un contesto sociale, economico e politico in cui il cittadino vive e che esige di conoscere e trattare i suoi dati personali.

Qualsiasi forma di tutela deve quindi garantire costantemente nel tempo un delicatissimo equilibrio e bilanciamento di interessi e di esigenze provenienti dall'individuo e dalla società. In tale ottica, il diritto alla privacy è definito come il diritto di costruire liberamente e difendere la propria sfera privata, di scegliere il proprio stile di vita senza interferenze ed intromissioni indesiderate da parte di terzi. Tutelare la privacy significa allora consentire all'individuo di decidere autonomamente l'ambito entro cui i suoi dati personali, che ne rivelano l'identità e la sfera intima, possono essere portati a conoscenza di terzi e di controllare i trattamenti di tali dati, nel rispetto peraltro delle esigenze della società in cui vive.

Il Codice in materia di protezione dei dati personali, adottato con decreto legislativo 30 giugno 2003 n. 196 ed in vigore dal 1 gennaio 2004, ha appunto per natura e finalità essenziale la salvaguardia dei diritti, delle libertà fondamentali, della dignità della persona, con particolare riguardo alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali. L' art. 1 del Codice prescrive appunto, quale principio generale, che chiunque ha diritto alla protezione dei dati personali che lo riguardano.

Già con la legge n. 675/96, il legislatore italiano aveva attuato in Italia le parti più significative della Direttiva europea 95/46/CE. Ancora precedentemente, nella convenzione di Strasburgo n. 108/1981, si era manifestata l'esigenza e l'urgenza di dare protezione alle persone in relazione all'elaborazione automatica dei propri dati personali.

Con la suddetta Direttiva si sono quindi individuati standard di protezione minimi, validi a livello europeo, di cui si è imposta la ricezione nelle legislazioni nazionali.

Con la legge n. 675/96 prima e ora con il Codice, il legislatore italiano non si è limitato a recepire le linee guida sovranazionali ma per taluni aspetti si è spinto oltre. Ad esempio, ha inteso applicare la disciplina di tutela dei dati personali, anche alle persone giuridiche, enti ed associazioni oltre che alle persone fisiche. Il nuovo Codice si compone di tre parti, che contengono rispettivamente: le disposizioni generali (articoli da 1 a 45), riguardanti le regole sostanziali della disciplina del trattamento dei dati personali, applicabili a tutti i trattamenti, nonché le regole specifiche che si devono osservare per i trattamenti effettuati da soggetti pubblici e quelle che trovano applicazione per i trattamenti effettuati da soggetti privati e da enti pubblici economici; le disposizioni che si applicano a specifici trattamenti, in particolare quelli relativi al trattamento dei dati personali nell'ambito della pubblica amministrazione, in quello giudiziario e nel campo sanitario (articoli da 46 a 140); le disposizioni relative alle azioni di tutela dell'interessato e al sistema sanzionatorio (articoli da 141 a 172), cui si aggiungono le norme di modifica, finali e di carattere transitorio (articoli da 173 a 186).

Il Codice è completato inoltre da tre allegati, le cui disposizioni si devono quindi intendere come parte integrante dello stesso, contenenti:

i codici di deontologia (allegato A);

il disciplinare tecnico in materia di misure minime di sicurezza (allegato B);

l'elenco dei trattamenti non occasionali effettuati in ambito giudiziario o per fini di giustizia (allegato C).

Definizioni

Ai fini del GDPR ed in relazione ai concetti specificamente coinvolti dalle attività di trattamento effettuate ai sensi dell'art. 4 del GDPR si intende per:

- «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;

- «dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

- «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

- «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

- «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'organizzazione, 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;

- «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

- «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

- «pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

- «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

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

- «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

- «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

- <<interessato>> persona fisica identificata o identificabile cui si riferiscono i dati personali.

- «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

- «rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

- «impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

- «gruppo imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

- «norme vincolanti d'impresa»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del

trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

- «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

- «autorità di controllo interessata»: un'autorità di controllo interessata dal trattamento di dati personali in quanto:

  - a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;

  - b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure

  - c) un reclamo è stato proposto a tale autorità di controllo.

- «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

- «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;

- «stabilimento principale»:

  a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;

  b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

I compiti delle varie figure previste dalla normativa

- **il Titolare**

Definisce le finalità e le modalità dei trattamenti nonché le misure di sicurezza necessarie. Nomina i soggetti esterni responsabili del trattamento dei dati. Autorizza con atto formale, gli incaricati al trattamento. Vigila sul rispetto delle norme. Se necessario nomina gli Amministratori di sistema e il Responsabile per la protezione dei dati. Il titolare è il responsabile di fronte alla legge ed agli interessati di ogni trattamento effettuato per suo conto. Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.

- **il Responsabile**

Persona fisica o giuridica che presta servizi al Titolare (es. servizi IT, consulente del lavoro, studi legali, conservazione sostitutiva, provider, ecc.) sulla base di un contratto o di altro atto giuridico con il quale il titolare impartisce le disposizioni organizzative e operative per l'effettuazione del trattamento. Il responsabile fornisce agli incaricati le istruzioni per il trattamento dei dati, esegue gli opportuni controlli, autorizza gli incaricati all'accesso alle banche dati, sovrintende all'attuazione delle misure di sicurezza. Collabora con il titolare in ogni fase della gestione dei dati personali e fornisce supporto per gli audit periodici, in caso di data breach o di richiesta di accesso ai dati da parte di interessati.

- **l'Autorizzato al trattamento (incaricato)**

Sono gli operatori, gli impiegati ed in generale, chiunque effettui operazioni che riguardino il trattamento di dati personali. Opera sotto la supervisione del Responsabile e del Titolare e deve osservare le disposizioni organizzative e operative a lui impartite. Può accedere esclusivamente alle banche dati a cui è stato autorizzato e collabora con i referenti informatici ad attuare le misure di sicurezza; ad esempio, procede a tempo debito a cambiare la password del proprio personal computer di servizio. Se fra i suoi compiti vi è anche la raccolta dei dati personali, provvede a fornire l'informativa, in forma orale o scritta agli interessati e raccoglierne il consenso.

- **l'Amministratore Di Sistema**

Oltre alle figure indicate, mediante il provvedimento del 27 dicembre 2008 del Garante per la protezione dei dati personali, è stato prevista la figura dell'Amministratore di Sistema (AdS).

L'Amministratore di sistema è una figura assimilabile a quella del Responsabile e sono necessari i medesimi criteri per la designazione. L'amministratore di sistema ha il compito della gestione e della manutenzione di sistemi informatici e database, anche solo, ad esempio, per l'effettuazione delle copie di sicurezza.

E' compito del Titolare o del responsabile delegato, effettuare la valutazione delle caratteristiche richieste per l'AdS che sono; Esperienza, Competenza, Affidabilità. Il documento di nomina dell'AdS deve contenere l'elencazione dei compiti assegnati.

Il Titolare deve inoltre predisporre un sistema di registrazione degli accessi ai sistemi informatici degli AdS al fine di poterne valutare l'operato. I log devono essere registrati in formato non modificabile e verificabile e devono contenere data ed ora di accesso ed uscita dal sistema. Annualmente il Titolare o il responsabile delegato devono effettuare una verifica dell'operato dell'AdS al fine di valutarne la rispondenza alle disposizioni di legge in materia di trattamento di dati personali

- **Il Responsabile della protezione dei dati**

Devono nominare obbligatoriamente un Responsabile della protezione dei dati personali (il c.d. data protection officer) tutte le pubbliche amministrazioni ed enti pubblici, eccetto le autorità giudiziarie.

L'obbligo riguarda anche tutti i soggetti (enti e imprese) che trattano su larga scala dati sensibili, relativi alla salute o alla vita sessuale, genetici, giudiziari e biometrici, oppure che svolgono attività in cui i trattamenti richiedono il controllo regolare e sistematico degli interessati.

Un gruppo di imprese o soggetti pubblici possono nominare un unico Responsabile della protezione dei dati. Le imprese, che non ricadono invece nell'obbligo di legge, potranno comunque decidere di dotarsi ugualmente di un data protection officer, o di un privacy officer.

I titolari del trattamento devono nominare come "data protection officer" un professionista che possieda un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali, che

sia in grado di adempiere alle proprie funzioni in piena indipendenza e in assenza di conflitti di interesse, operando come dipendente, oppure anche sulla base di un contratto di servizi.

Ai sensi dell'art. 37, questo deve essere "designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati, e della capacità di adempiere ai compiti".

E' richiesto inoltre che il titolare metta a disposizione del Responsabile della protezione dei dati personali le risorse umane e finanziarie necessarie all'adempimento dei suoi compiti.

Il Responsabile della protezione dei dati personali (data protection officer), ha il compito di informare e consigliare il titolare o il responsabile del trattamento da lui preposto, nonché i dipendenti, in merito agli obblighi derivanti dal Regolamento Europeo e dalle altre disposizioni dell'UE o delle normative locali degli Stati membri relative alla protezione dei dati.

Dovrà poi verificare che la normativa vigente e le policy interne del titolare siano correttamente attuate ed applicate, incluse le attribuzioni delle responsabilità, la sensibilizzazione e la formazione del personale, ed i relativi audit. Su richiesta, dovrà fornire pareri in merito alla valutazione d'impatto sulla protezione dei dati, sorvegliandone poi i relativi adempimenti.

Il Responsabile della protezione dei dati fungerà inoltre da punto di contatto sia con il Garante della Privacy che con gli interessati, che potranno rivolgersi a lui anche per l'esercizio dei loro diritti.

ISTRUZIONI per gli autorizzati all'accesso ai dati personali

Trattamento dei dati personali

Il trattamento dei dati personali deve essere effettuato esclusivamente in conformità alle finalità previste e dichiarate dall'azienda e, pertanto, in conformità alle informazioni che l'azienda ha comunicato agli interessati.

L'eventuale raccolta di dati dovrà avvenire nel rispetto delle procedure e dei modelli di informativa e/o consenso elaborati dall'azienda.

L'incaricato deve prestare particolare attenzione all'esattezza dei dati trattati e provvedere, inoltre, all'aggiornamento degli stessi.

Accesso a dati personali

I trattamenti di dati personali cui l'incaricato è autorizzato ad accedere per effettuare i trattamenti (sia informatici che cartacei), sempre strettamente pertinenti alle mansioni svolte e per le finalità previste dall'azienda, rispettando i principi fondamentali sanciti dalla normativa sono indicati nelle *Lettere di autorizzazione* predisposte dal Titolare e/o dai delegati individuati.

Creazione nuove banche dati. Gestione programmi

Senza preventiva autorizzazione del Titolare o del Responsabile del Trattamento non è permesso creare nuovi trattamenti di dati personali con finalità diverse da quelle già previste.

Comunicazione e diffusione dei dati

In relazione alle banche dati di cui è autorizzato il trattamento nello svolgimento delle mansioni affidate, è autorizzata la comunicazione dei dati stessi esclusivamente ai soggetti esterni indicati dall'azienda.

Ogni ipotesi diversa di comunicazione o, addirittura, di diffusione dei dati dovrà essere preventivamente autorizzata di volta in volta dall'Azienda .

Possono essere trasmessi al di fuori dell'azienda soltanto i dati personali di cui é consentita la comunicazione o la diffusione, nei limiti e secondo le modalità previste.

I dati personali di cui é consentita la diffusione possono essere trasmessi secondo le normali procedure di trasmissione avendo cura che i dati non possano essere modificati da terzi.

I dati personali di cui é consentita la comunicazione devono essere trasmessi in modo da garantire la non modificabilità dei dati ed in modo che solo il destinatario abilitato alla ricezione possa leggerne il contenuto. Ad esempio, in caso di trasmissione su supporto magnetico si può utilizzare un formato compresso Zip protetto con password a conoscenza esclusiva del destinatario.

Nel caso in cui terzi debbano intervenire e modificare i dati ad essi trasmessi o diffusi é necessario che sia garantita la verifica delle modifiche intervenute.

La posta elettronica in uscita inviata a più destinatari è inviata in maniera da rendere visibile a ciascun destinatario solo il proprio indirizzo.

Informativa e consenso

Nessun dato personale **di persone fisiche** potrà essere raccolto e trattato se non è stata preventivamente comunicata all'interessato l'informativa prevista. Tale informativa potrà essere comunicata verbalmente o in formato scritto, in forma colloquiale e facilmente comprensibile. Potrà inoltre non contenere informazioni già in possesso dell'interessato.

Il consenso dovrà essere acquisito, ove necessario, in forma scritta se relativo al trattamento di dati sensibili od in forma verbale se relativo al trattamento di dati personali comuni. L'incaricato dovrà provvedere ad annotare tale acquisizione sul relativo documento o su apposito registro.

Il consenso deve essere univoco, libero ed informato. Non è permesso subordinare la prestazione di un servizio alla concessione del consenso al trattamento di dati personali non necessario all'esecuzione di tale servizio.

Il consenso non è necessario per il trattamento di dati personali effettuato a seguito di attività economiche, per esempio per proporre offerte, stipulare contratti, effettuare attività legate ai contratti sottoscritti, effettuare attività disposte da obblighi di legge come ad esempio gli obblighi fiscali e tributari.

E' esclusa la necessità di richiedere il consenso anche per i trattamenti di dati sensibili quali i dati sanitari dei dipendenti quando questi siano limitati ai soli certificati medici privi di diagnosi a trattati a seguito di normative.

L'interessato potrà in qualunque momento revocare il proprio consenso con la stessa facilità con le quali lo ha concesso.

Il trattamento dei dati relativi a persone giuridiche, enti, associazioni non è sottoposto alla normativa sulla privacy ma si ricorda che in ogni rapporto con terzi si andrà necessariamente a raccogliere dati personali delle persone fisiche con le quali si entrerà in contatto: rappresentanti legali, dipendenti, collaboratori, consulenti, ecc.

Gestione dei curricula

Il trattamento di un Curriculum può essere effettuato a seguito della necessità di selezione di personale oppure in caso di invio spontaneo da parte dell'aspirante candidato.

A seguito delle semplificazioni introdotte dalla legge 12 luglio 2011, n. 106, l'informativa non è dovuta in caso di ricezione di curricula spontaneamente trasmessi dagli interessati ai fini dell'eventuale instaurazione di un rapporto di lavoro. Al momento del primo contatto successivo all'invio del curriculum, il titolare è tenuto a fornire all'interessato, anche oralmente, una informativa

breve contenente almeno:

- le finalità e le modalità del trattamento cui sono destinati i dati;
- i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
- gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato e del responsabile.

Il trattamento del curriculum è possibile solo se viene resa l'informativa all'interessato. Pertanto deve essere prevista adeguata informativa per i candidati da pubblicare sul sito web o consegnare al momento del ricevimento di un curriculum. Nel caso di pubblicazione di un annuncio di ricerca personale su giornali deve essere inserita nell'annuncio una informativa breve che rimandi ad esempio all'informativa completa sul sito web.

Nel caso di ricevimento di un curriculum inviato spontaneamente da un candidato, dovrà essere inviata l'informativa prima di effettuarne il trattamento, ad esempio per un colloquio di lavoro.

Per gli scopi per i quali viene effettuato il trattamento non sono necessari dati sensibili. In caso di ricezione di curriculum contenente dati sensibili, questo viene restituito al mittente oppure vengono cancellati i dati sensibili e se ciò non fosse possibile, il curriculum viene distrutto senza effettuarne trattamento.

Nel caso di necessità di dati sensibili (p.e. Categorie speciali), deve essere acquisito il consenso prima di effettuare il trattamento.

I curriculum ricevuti devono essere sottoposti alle misure di sicurezza previste dalla normativa. In particolare:

- I curriculum ricevuti in formato cartaceo vengono conservati in un apposito armadio chiuso a chiave.
- I curriculum ricevuti in formato elettronico sono conservati in una apposita cartella sul server alla quale ha accesso solo il personale incaricato del trattamento.

I curriculum ritenuti non interessanti dovranno essere distrutti mentre per la conservazione di quelli ritenuti interessanti dovrà essere richiesto specifico consenso.

Riscontro all'interessato

L'interessato ha diritto (artt da 15 a 22 del reg. UE 679/2016) di accedere in ogni momento ai dati che lo riguardano, chiederne l'esibizione od una copia, richiedere la correzione, l'aggiornamento o l'integrazione dei dati inesatti o incompleti, ovvero la cancellazione o la limitazione per quelli trattati in violazione di legge, o per motivi legittimi da evidenziare nella richiesta.

Della ricezione della richiesta e di ogni operazione effettuata deve essere data comunicazione all'interessato. La richiesta deve essere evasa entro 30 giorni dalla ricezione.
Nel caso sorgessero delle difficoltà nell'accoglimento della richiesta, questo deve essere comunicato immediatamente all'interessato. In questo caso il termine massimo entro il quale soddisfare la richiesta diventa di 3 mesi.

In caso di richiesta di cancellazione, limitazione, aggiornamento, rettifica, integrazione dei dati, l'interessato deve ricevere l'attestazione che di tali operazioni è stata data conoscenza anche a tutti i soggetti ai quali i dati personali erano stati comunicati o diffusi.

Non esistono formalismi per effettuare la richiesta che può essere rivolta anche oralmente. In tal caso il responsabile per il riscontro deve prenderne nota scritta.

La richiesta deve essere presentata dall'interessato, correttamente identificato o da un suo delegato nominato per iscritto.

Il titolare deve essere certo dell'identità del richiedente. Qualora il titolare del trattamento nutra ragionevoli dubbi circa l'identità della persona fisica che presenta la richiesta può richiedere ulteriori informazioni necessarie per confermare l'identità dell'interessato.

I dati devono essere comunicati in forma intelligibile e facilmente accessibile, anche in base al supporto sul quale si trovano, e possono nel caso essere trasmessi all'interessato, anche in formato elettronico.

Se i dati personali si trovano all'interno di documenti (p.e. fotocopie, file) che contengono dati personali di terzi, questi dovranno essere oscurati.

Per maggiori informazioni consultare gli artt. 7, 8, 9, 10, 146 del D.lgs 196/2003 e gli artt. Da 12 a 23 del GDPR.

Campo di applicazione del regolamento

Il regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'azienda a prescindere dal rapporto contrattuale con la stessa intrattenuto (lavoratori somministrati, collaboratore a progetto, in stage, specializzandi, ecc.) oltre che ai dipendenti delle società esterne affidatarie di servizi autorizzati ad accedere alla rete informatica dell'Azienda.

Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente e collaboratore (collaboratore a progetto, in stage, specializzando, consulente, ecc.) in possesso di specifiche credenziali di autenticazione. Tale figura potrà anche venire indicata quale "incaricato del trattamento".

Sistemi informatici

I personal computer (fissi o portatili) ed i relativi programmi e/o applicazioni affidati al dipendente sono, come è noto, strumenti di lavoro, pertanto:

- tali strumenti vanno custoditi in modo appropriato;
- tali strumenti hardware e software sono assegnati in ragione di specifiche competenze e responsabilità;
- possono essere utilizzati solo per fini professionali (in relazione, ovviamente alle mansioni assegnate) e non per scopi personali, tanto meno per scopi illeciti;
- è di competenza del dipendente/collaboratore/utente evitare l'uso improprio o l'accesso alle risorse da parte di personale non autorizzato;
- ai sensi della vigente normativa in materia di protezione dei dati personali è fatto divieto di comunicazione e/o divulgazione a qualsiasi titolo delle informazioni presenti nelle banche dati del Titolare, anche se di terzi, se non autorizzate preventivamente dallo stesso per specifiche attività svolte nel rispetto delle norme vigenti;
- debbono essere prontamente segnalati all'Azienda il furto, danneggiamento o smarrimento di tali strumenti o comunque ogni incidente di sicurezza;
- in caso di assenza del Dipendente l'Azienda si riserva il diritto di accedere a tali strumenti così da garantire la continuazione delle attività lavorative;
- l'Azienda ha adottato le politiche di sicurezza descritte in questo documento ed è obbligo di tutti adottarle e rispettarle.

Al fine di garantire la sicurezza dei dati e dei sistemi, vengono messe in atto alcune attività di verifica e controllo, compresa la registrazione di log del traffico internet in formato anonimo. Tali log sono a disposizione dell'amministratore di sistema e vengono mantenuti per un periodo di un anno.

Per prevenire possibili danni ai sistemi informativi sono attivi sistemi di filtraggio del traffico che impediscono l'accesso a determinate categorie di siti internet in base ad un sistema di “Black list”. Inoltre è attivo un sistema antivirus che esamina tutto il traffico web e mail per individuare eventuali virus od altri programmi malevoli.

Si ricorda infine che i sistemi operativi ed i programmi installati sui computer aziendali effettuano autonomamente operazioni che lasciano sul disco traccia delle operazioni effettuate (log, cache, history, file temporanei, coockie) pertanto l'Azienda non è in grado di garantire che non sia possibile anche in maniera fortuita accedere ad informazioni personali relative all'utilizzatore del computer, ad esempio durante operazioni di manutenzione.

Non è consentito installare autonomamente programmi senza la preventiva autorizzazione dell'Ufficio Informatica e/o del Titolare, sussistendo infatti il grave pericolo di introdurre Virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti.

L’inosservanza della presente disposizione espone la stessa Azienda a gravi responsabilità civili; si evidenzia inoltre che le violazioni della normativa a tutela dei diritti d’autore sul software che impone la presenza nel sistema di software regolarmente licenziato vengono sanzionate anche penalmente.

L'acquisto e l'installazione di dotazioni informatiche Hardware e Software è infatti di esclusiva pertinenza del Servizio Affari generali, nei casi in cui per, particolari e motivate esigenze, venissero effettuati degli acquisti/installazioni da parte di dipendenti, è necessario che essi concordino prima dell'acquisto con il servizio Affari generali o con il Titolare, le specifiche tecniche del prodotto da acquisire e installare.

I personal computer (fisso o mobile) ed i relativi programmi e/o applicazioni affidati al dipendente sono, come è noto, strumenti di lavoro, pertanto:

a) tali strumenti vanno custoditi in modo appropriato;

b) tali strumenti possono essere utilizzati solo per fini professionali (in relazione , ovviamente alle mansioni assegnate) e non per scopi personali, tanto meno per scopi illeciti;

c) debbono essere prontamente segnalati all’Azienda il furto, danneggiamento o smarrimento di tali strumenti;

d) in caso di assenza del Dipendente l’Azienda si riserva il diritto di accedere a tali strumenti così da garantire la continuazione delle attività lavorative.

Ai fini sopra esposti sono quindi da evitare atti o comportamenti contrastanti con le predette indicazioni come, ad esempio, quelli qui di seguito richiamati a titolo indicativo.

Misure di sicurezza

L’art 32 del GDPR prescrive l’adozione di misure di sicurezza adeguate alla protezione dei dati personali senza peraltro specificare prescrizioni tecniche ma lasciando al titolare del trattamento l’obbligo si mettere in atto **misure tecniche e organizzative adeguate** per garantire un livello di sicurezza adeguato al rischio.

Con la nuova normativa Europea, le nome sulle misure di sicurezza previste dalla formulazione dell'art. 32 lasciano al titolare del trattamento la responsabilità della definizione delle misure adeguate in funzione delle analisi di rischio effettuate. Questo non significa che le misure minime di sicurezza, obbligatorie nella precedente normativa, possano essere tralasciate; sono anzi da intendere come la base di partenza per la costruzione di un sistema sicuro.

Si raccomanda la massima sensibilità ed attenzione alla sicurezza. Il mondo della sicurezza è in continua evoluzione e misure che sino a ieri sembravano insuperabili possono rapidamente diventare obsolete. Ecco perché si raccomanda di mantenere uno stretto contatto con il Titolare od il suo delegato e con il DPO per essere sempre aggiornati sulle misure di sicurezza in atto, quelle previste e su possibili debolezze che si manifestino nel tempo.

Ogni incaricato è tenuto ad osservare tutte le misure di protezione e sicurezza atte a evitare rischi di distruzione, perdita, accesso non autorizzato, trattamento non consentito, predisposte dall'Azienda, nonché quelle che in futuro verranno comunicate.

Uso delle password

Assegnazione e Gestione delle credenziali di autenticazione

Le credenziali di autenticazione per l'accesso alla rete, ai programmi, alla casella di posta elettronica aziendale, vengono assegnate dal Servizio Affari generali al momento della creazione delle nuove utenze o successivamente in caso di necessità su richiesta del Titolare o del Responsabile.
Nel caso di collaboratori esterni la preventiva richiesta verrà inoltrata direttamente dal Responsabile dell'Ufficio o dal Gestore di Filiale con il quale il collaboratore si coordina nell'espletamento del proprio incarico. Lo stesso dicasi nel caso di revoca dell'incarico e/o trasferimento di personale.

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dal Servizio Affari generali, associato ad una parola chiave (password) riservata che dovrà venir gestita dall'incaricato con la massima diligenza e non divulgata.
Non è consentita l'attivazione di una ulteriore password senza preventiva autorizzazione da parte del Servizio Affari generali
È necessario procedere alla modifica della parola chiave a cura dell'utente al primo utilizzo e successivamente almeno ogni sei mesi oppure ogni tre mesi in caso di trattamento di dati sensibili.

La parola chiave, formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato (date di nascita, nome e cognome, ecc…).
Qualora la parola chiave dovesse venire sostituita per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, l'utente provvederà a definire una nuova password di accesso seguendo le medesime istruzioni.

Il soggetto preposto alla ulteriore modifica delle credenziali di autenticazione alla rete informatica su richiesta dell'utente è il personale del Servizio Affari generali.
Nei casi in cui è indispensabile ed indifferibile accedere ai dati trattati dall'incaricato ed agli strumenti informatici in dotazione allo stesso, sia per le esigenze produttive sia per la sicurezza ed operatività dello stesso sistema informatico (ad esempio nei casi di prolungata assenza od impedimento dell'incaricato), l'Azienda potrà, previa autorizzazione scritta del Responsabile dell'Ufficio o Gestore di Filiale, accedere tramite l'intervento dell'amministratore del sistema; il Servizio Affari generali provvederà nel contempo alla comunicazione dell'intervento all'incaricato. Terminata la necessità di accesso alle risorse, le credenziali di autenticazione verranno disabilitate. Al rientro in servizio dell'incaricato provvederà alla creazione di nuove credenziali di autenticazione.

La password deve essere strettamente personale e non deve essere assolutamente divulgata per nessun motivo a nessuno.

La password deve essere sostituita dall'incaricato al primo utilizzo e successivamente ogni 6 mesi.

In caso di inutilizzo della password per almeno 6 mesi deve essere disabilitata.

E' dovere dell'operatore utilizzare con diligenza la parola chiave, cambiandola spesso e non rivelandola ad alcuno. Inoltre la selezione della parola chiave, che è affidata all'incaricato, dovrebbe essere governata da criteri di casualità, evitando nel modo più assoluto di scegliere lettere tutte eguali, lettere o numeri comunque collegati alla persona come date di nascita, nomi personali di familiari e simili. Studi effettuati hanno dimostrato come l'obbligare gli operatori all'uso di complicate misure di sicurezza ha avuto come effetto la diminuzione dell'efficacia delle stesse (p.e. Scrivere la password su post it attaccati allo schermo).

Ecco qualche prezioso consiglio su come scegliere una parola chiave facile da ricordare ma sufficientemente robusta.

Non usare il nome di login (o codice di identificazione personale) in qualsiasi forma (come è, invertito, in maiuscole, duplicato, ecc.).

Non scegliere il nome o cognome, comunque modificato.

Non scegliere il nome del partner o dei figli.

Non usare informazioni personali che possono esser facilmente recuperate, come la targa dell'autovettura, il numero di telefono, il codice fiscale, la marca della autovettura, il nome della via ove si abita, ecc.

Non scegliere parola chiave di meno di 8 caratteri alfanumerici.

Non scegliere una parola di senso compiuto in lingua italiana od una lingua straniera assai diffusa, come l'inglese.

Non usare caratteri sequenziali ripetuti (ad esempio 1111, aaaa, ecc.).

Non usare cifre tutte a salire o scendere.

Scegliere una parola chiave con caratteri minuscoli e maiuscoli.

Scegliere una parola chiave con segni di interpunzione.

Scegliere una parola chiave facile da ricordare, per non doverla trascrivere.

Scegliere una parola chiave facile da digitare, senza bisogno di scrutare la tastiera, per rendere difficile l'osservazione indiscreta.

Scegliere un verso di una canzone che ben si conosce e si ricavi la parola chiave dalle iniziali delle prime parole o simili combinazioni.

Alternare consonanti e vocali, per creare parola chiave pronunciabili e quindi più facili da ricordare.

Scegliere due parole brevi e concatenarle con segni di interpunzione.

Cambiare spesso la parola chiave, almeno ogni 6 mesi (tre mesi in caso di trattamento di dati sensibili)

Si ricorda che l’azienda titolare del trattamento, nei casi in cui è indispensabile ed indifferibile accedere ai dati trattati dall’incaricato ed agli strumenti informatici in dotazione allo stesso sia per le esigenze produttive aziendali sia per la sicurezza ed operatività dello stesso sistema informatico

(ad esempio nei casi di prolungata assenza od impedimento dell'incaricato), potrà accedere tramite l'intervento o dell'amministratore del sistema, o del Responsabile del Servizio; la password, verrà successivamente sostituita dall'incaricato e la busta contenente le nuove credenziali di autenticazione dovrà essere riconsegnata al Responsabile di servizio.

Utilizzo del personal computer

Il Personal Computer affidato all'utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.
Il personal computer deve essere custodito con cura evitando ogni possibile forma di danneggiamento.
Il personal computer dato in affidamento all'utente permette l'accesso alla rete dell'Azienda solo attraverso specifiche credenziali di autenticazione come meglio descritto al successivo punto "*Utilizzo del Personal Computer*" del presente Regolamento.
L'Azienda rende noto che il personale incaricato, che opera presso il Servizio Affari generali dell'Azienda o anche dei servizi esternalizzati, è stato autorizzato a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento / sostituzione / implementazione di programmi, manutenzione hardware etc.).
Detti interventi potranno anche comportare l'accesso in qualunque momento, ai dati personali degli operatori, ivi compresi gli archivi di posta elettronica, nonché alla verifica dei siti internet acceduti dagli utenti abilitati alla navigazione esterna. La stessa facoltà, sempre ai fini della sicurezza del sistema e per garantire la normale operatività dell'Azienda, si applica anche in caso di assenza prolungata od impedimento dell'utente.

Il personale incaricato dal Servizio Affari generali ha la facoltà di collegarsi e visualizzare in remoto, previa comunicazione all'interessato, il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc.
L'intervento viene effettuato su richiesta dell'utente o, in caso di oggettiva necessità**,** a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione all'utente della necessità dell'intervento stesso.

Non è consentito il collegamento alla rete aziendale di dispositivi non aziendali salvo specifica richiesta da parte di un Responsabile e autorizzazione da parte del Servizio Affari generali.

Salvo preventiva espressa autorizzazione del Servizio Affari generali, non è consentito all'utente modificare le caratteristiche impostate sul proprio PC né procedere ad installare dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, …).

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il Servizio Affari generali nel caso in cui siano rilevati virus ed adottando quanto previsto dal presente Regolamento in relazione alle procedure di protezione antivirus.

Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici, o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo, salvo indicazioni contrarie da parte dei Responsabili del Servizio o del Servizio Affari generali.
In ogni caso, lasciare un elaboratore incustodito può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso e pertanto deve essere evitato.

Onde evitare il grave pericolo di introdurre virus informatici nonché di alterare la stabilità delle applicazioni dell'elaboratore non è consentita l'installazione di programmi di qualsiasi tipo senza l'autorizzazione;

Non è consentito utilizzare strumenti software e/o hardware atti ad intercettare, falsificare, alterare o sopprimere il contenuto di comunicazioni e/o documenti informatici;

Non è consentito modificare le configurazioni impostate sul proprio PC;

Non è consentita l'installazione sul proprio PC di mezzi di comunicazione propri (come ad esempio chiavette usb);

Non è consentita la manomissione, distacco, spostamento del PC senza autorizzazione;

- Non lasciate visualizzati sullo schermo, in vostra assenza, dei dati personali.
- Attivate un salvaschermo con password o chiudete la sessione se vi allontanate dalla postazione.
- Accertatevi che estranei non possano osservare i dati sullo schermo, ad esempio attraverso le pareti vetrate di un corridoio.
- Evitate di discutere, anche con i colleghi, informazioni relative a dati personali, se non attinenti al lavoro che dovete svolgere.
- Cancellate sempre tutti i dati residui presenti nel computer, quando non più utilizzati.
- Se vi accorgete di aver accesso a dati e programmi di trattamento non di vostra competenza, informate subito il titolare o il responsabile.
- Non utilizzate supporti con dati e programmi di provenienza ignota, per evitare infezioni da virus nel computer e di danneggiare i dati.
- Occorre inoltre ricordarsi di effettuare periodicamente l'aggiornamento dei sistemi anti virus, perché purtroppo gli attacchi dei virus stanno diventando una piaga, avente sviluppo esponenziale, soprattutto da quando i sistemi informativi sono sempre più frequentemente collegati via Internet a sistemi di posta elettronica. Il disciplinare prevede esplicitamente tale aggiornamento a scadenza semestrale, ma è necessario provvedere, se possibile, anche tutti i giorni.
- Al termine del trattamento chiudere sempre i programmi secondo le appropriate procedure di sicurezza.
- Proteggere sempre i computer, gli apparati terminali ed i supporti di registrazione da condizioni climatiche sfavorevoli, come ad esempio estremi di temperatura ed umidità, vapori corrosivi, liquidi, fumi, polvere od altre sostanze contaminanti.
- Ricordarsi che tutti i componenti dei computer possono andare in avaria. Predisporre sempre copie di riserva di dati ed applicazioni critici, e conservare tali copie in una area sicura, preferibilmente separata dallo stesso ambiente ove si trova il computer. Il disciplinare prevede esplicitamente che tutti i dati sensibili vengano riversati in copie di sicurezza, a scadenze almeno settimanali.

Utilizzo di PC portatili, tablet, palmari, smartphone ed altri dispositivi mobili

L'utente è responsabile del PC o altro dispositivo mobile (tablet, palmari, smartphone, ecc…) assegnatogli dal Servizio Affari generali deve custodirlo con diligenza sia durante gli spostamenti, sia durante l'utilizzo nel luogo di lavoro.
Ai PC e agli altri strumenti portatili si applicano le regole di utilizzo previste dal presente regolamento, con particolare attenzione alla rimozione di eventuali file salvati sul dispositivo al termine dell'utilizzo.
I PC portatili utilizzati all'esterno devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.
Tali disposizioni si applicano anche nei confronti di incaricati esterni quali consulenti, collaboratori, ecc.

I PC portatili e tutti gli altri dispositivi vanno restituiti al Servizio Affari generali al termine del rapporto.

Particolare attenzione viene posta nell'utilizzo di notebook (computer portatili) e dei dispositivi di memorizzazione portatili (chiavi USB, dischi esterni, flash card, ecc) in quanto la possibilità di essere utilizzati al di fuori della struttura può comportare rischi derivati da virus, backdoor od altri programmi maligni installati tramite connessioni internet non sicure o connessione con computer infetti.
Esiste inoltre il fondato rischio di sottrazione pertanto vengono utilizzati di sistemi operativi sicuri con password forti, sistemi di crittografia, utilizzo di memorie di massa alternative (chiavi USB con crittografia, ecc) per i documenti riservati.

Utilizzo e conservazione dei supporti rimovibili

Tutti i supporti magnetici rimovibili forniti dall'Azienda (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati personali ed in particolare dati sensibili nonché informazioni costituenti patrimonio aziendale, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.
Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente dovrà contattare il Servizio Affari generali e seguire le istruzioni da questo impartite.
In ogni caso, i supporti magnetici contenenti dati sensibili devono essere dagli utenti adeguatamente custoditi in armadi chiusi.
E' vietato l'utilizzo di supporti rimovibili personali, salvo i casi espressamente autorizzati dal Responsabile dell'Ufficio o dal Gestore di Filiale.
L'utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.

Non è consentito scaricare file contenuti in supporti magnetici/ottici non aventi alcuna attinenza con la propria prestazione lavorativa;

Tutti i supporto rimovibili di provenienza incerta o esterna, ancorché attinenti all'attività lavorativa, devono essere sottoposti ad un controllo eseguito con un software antivirus aggiornato.

I supporti rimovibili debbono essere conservati in contenitori chiusi a chiave. Nel caso debbano essere riutilizzati, il contenuto deve essere cancellato in modo sicuro con appositi strumenti. Nel caso di dismissione debbono essere distrutti o resi inutilizzabili

Utilizzo della rete Aziendale

Per l'accesso alla rete locale aziendale ciascun utente deve essere in possesso delle credenziali di autenticazione personali.

È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato a meno di creazione in via eccezionale, da parte del Servizio Affari generali di utenze di ufficio o reparto comune.
Le parole chiave d'ingresso alla rete ed ai programmi sono personali e vanno tenute segrete.
Le cartelle utenti presenti nei server dell'Azienda 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.

Su queste unità vengono svolte regolari attività di controllo, amministrazione e backup da parte del Servizio Affari generali.
L'Azienda si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericoloso per la sicurezza del sistema ovvero acquisiti o installati in violazione del presente Regolamento.

Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

Non è consentito connettere alla rete locale aziendale computer personali o di visitatori senza la necessaria autorizzazione del Servizio Affari generali.

Utilizzo della rete Internet e dei relativi servizi Navigazione in Internet:

Il PC abilitato alla navigazione Internet e/o la connessione fornita dal Titolare, i tablet o gli apparecchi telefonici salvo diverso accordo specifico ed i casi di "benefit" e/o comunque di intestazione dei contratti al collaboratore, costituiscono un ulteriore "bene strumentale aziendale" necessario allo svolgimento della propria attività lavorativa. Non è quindi consentita la navigazione in siti ove sia possibile rivelare opinioni politiche, religiose o sindacali dell'utilizzatore e non è consentito, inoltre, visitare siti e memorizzare documenti informatici dai contenuti di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.
È assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa, salvo le indicazioni presenti nel successivo punto "*Regolamentazione uso Internet per Finalità non Istituzionali*".
In questo senso, a titolo puramente esemplificativo, **l'utente non potrà utilizzare internet** per:

- l'upload o il download di software gratuiti (freeware) e shareware, nonché l'utilizzo di documenti provenienti da siti web o http, se non strettamente attinenti all'attività lavorativa (p.e. filmati e musica);
- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, fatti salvi i casi direttamente autorizzati dal Responsabile dell'Ufficio e/o dal Servizio Affari generali e comunque nel rispetto delle normali procedure di acquisto;
- ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa; la partecipazione a Forum non professionali, l'utilizzo di chatline (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames) se non espressamente autorizzati dal Responsabile ~~d'ufficio~~ di Servizio.
- Non è consentito navigare in siti non attinenti allo svolgimento delle mansioni assegnate, soprattutto in quelli che possono rivelare le opinioni politiche, religiose o sindacali del dipendente;
- E' vietata ogni forma di registrazione a siti in cui contenuti non siano legati all'attività lavorativa;

- Non è permessa la partecipazione, per motivi non professionali a Forum, l'utilizzo di chat line, di bacheche elettroniche, instant messanging e le registrazioni in guest book anche utilizzando pseudonimi (o nicknames);

- Non è consentita la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;

- Non è consentito lo scarico di software gratuiti (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dalla Direzione;

- Non è consentito lo scarico e la memorizzazione di filmati video, file musicali, programmi e di ogni altro tipo di file non attinente all'attività lavorativa;

- Non è consentito l'uso di programmi di file sharing o qualunque altro tipo di condivisione delle risorse del proprio PC in Internet.

L'accesso, tramite internet, a caselle webmail di posta elettronica personale è consentito solo nel rispetto di quanto riportato al punto "*Regolamentazione uso Internet per finalità non istituzionali"*.

Al fine di evitare la navigazione in siti non pertinenti all'attività lavorativa, l'Azienda rende peraltro nota l'adozione di uno specifico sistema di blocco o filtro automatico che previene determinate operazioni quali l'upload o l'accesso a determinati siti inseriti in una black list gestita tramite la classificazione dei siti.
L'azienda si attiverà nell'individuazione di categorie di siti considerati correlati con la prestazione lavorativa e di siti compatibili con le finalità non istituzionali di cui al successivo punto "*Regolamentazione uso Internet per finalità non istituzionali"*..
Gli eventuali controlli, compiuti dal personale incaricato dal Servizio Affari generali ai sensi di quanto previsto dal presente regolamento, potranno avvenire mediante un sistema di controllo dei contenuti (p.e. proxy server, antivirus) o mediante analisi dei "file di log" della navigazione svolta preventivamente resi temporaneamente anonimi mediante oscuramento dell'indirizzo IP. Il controllo sui file di log non è continuativo ed i file stessi vengono conservati non oltre 1 anno, ossia il tempo indispensabile per il corretto perseguimento delle finalità organizzative e di sicurezza dell'azienda.
Anche nel caso di autorizzazione o di attinenza all'attività svolta, il dipendente risponde direttamente dei contenuti espressi ed è consapevole che in ogni caso dovrà manlevare esplicitamente per i contenuti stessi il Titolare e tutti i soggetti ad esso collegati a qualunque titolo eventualmente coinvolti, specificando all'occorrenza che quanto scritto viene fatto a titolo e con diretta responsabilità personale, non necessariamente rispecchiando le posizioni del Titolare e degli altri soggetti aziendali. In caso di contestazioni il Titolare potrà svolgere tutti gli accertamenti tecnici che riterrà opportuni, volti ad identificare il reale autore dei contenuti e rivalersi, nelle sedi e nei modi che riterrà appropriati, nei confronti del collaboratore.
Il Titolare e/o il Servizio Affari generali si riservano di applicare per singoli e/o gruppi di utenti politiche di navigazione personalizzate in base alle mansioni ed eventuali disposizioni concordate con i responsabili al fine di ottimizzare l'uso delle risorse, gli investimenti e le prestazioni delle connessioni esistenti.
E' vietato agli utenti della rete autorizzare autonomamente, quindi senza il coinvolgimento diretto, l'autorizzazione scritta e/o la presenza di personale tecnico incaricato dal Servizio Affari generali, l'accesso agli applicativi utilizzati e/o al proprio pc da parte di terzi, interni e/o esterni all'organizzazione del Titolare. Questo al fine di limitare potenziali attacchi e intrusioni ed aumentare il livello di protezione dei dati personali.

Regolamentazione uso Internet per finalità non istituzionali

L'Azienda, potrà consentire la consultazione di determinati siti internet e l'accesso a caselle webmail di posta elettronica personale laddove le modalità di consultazione siano compatibili con le misure di sicurezza implementate a protezione del sistema informatico.
Tale modalità non deve in ogni caso avvenire in misura eccedente e pregiudizievole rispetto agli obblighi che l'utente ha nei confronti dell'Azienda.

Uso della posta elettronica

La casella di posta elettronica assegnata all'utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
È fatto divieto di utilizzare le caselle di posta elettronica ***utente@azienda.it*** per motivi diversi da quelli strettamente legati all'attività lavorativa, salvo le indicazioni presenti nel punto 8.

Nel precisare che anche la posta elettronica è uno strumento di lavoro, si ritiene utile segnalare che:

Non è consentito utilizzare la posta elettronica Aziendale (interna ed esterna) per motivi non attinenti allo svolgimento delle mansioni assegnate;

Non è consentito l'uso di mail personali, anche se tramite server esterni alla rete Aziendale; (vedi: Procedura per accesso alle risorse in caso di assenza dell'incaricato)

Non è consentito inviare o memorizzare messaggi (interni ed esterni) di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica;

Non è consentito l'utilizzo dell'indirizzo di posta elettronica Aziendale per la partecipazione a dibattiti, Forum o mailing list, salvo diversa ed esplicita autorizzazione;

Si deve limitare al massimo l'invio di messaggi con allegati; a tal fine si raccomanda:

1) le immagini eventualmente allegate devono essere in formato compresso Jpeg;

2) è da evitare l'uso di allegati Word od in altro formato per l'invio di comunicazioni che potrebbero essere fatte tramite un semplice messaggio di testo;

3) si devono limitare per quanto possibile le dimensioni degli allegati, anche spezzando i file in più invii e /o mediante tecniche di compattazione

In caso di invio dello stesso messaggio a più destinatari contemporaneamente si dovrà utilizzare la funzione BCC (Blind Carbon Copy) o CCN (Copia Conoscenza Nascosta) al fine di mantenere riservata la lista dei destinatari evitando di distribuire gli indirizzi personali di posta a tutti gli altri.

Il sistema di posta elettronica è, per sua natura intrinseca, insicuro sia per quanto riguarda la sicurezza dei contenuti sia per quanto riguarda l'effettiva consegna al destinatario. Poiché in caso di violazioni contrattuali e giuridiche, sia l'Azienda, sia il singolo lavoratore sono potenzialmente perseguibili con sanzioni, anche di natura penale, l'Azienda verificherà, nei limiti consentiti dalle norme legali e contrattuali, il rispetto delle regole e l'integrità del proprio sistema informatico

In questo senso, a titolo puramente esemplificativo, l'utente non potrà utilizzare la posta elettronica per:
- l'invio e/o il ricevimento di allegati contenenti filmati o registrazioni audio (es.mp3 musicali) non legati all'attività lavorativa;

- l'invio e/o il ricevimento di messaggi personali o per la partecipazione a dibattiti, aste on line, concorsi, forum o mailing-list;
- la partecipazione a catene telematiche (o di Sant'Antonio). Se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al Servizio Affari generali. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi.
- la casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti. La conservazione on line dei messaggi di posta elettronica è garantita per un periodo di tempo limitato.
- ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per l'Azienda, ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere visionata od autorizzata dal Responsabile di Servizio o dal Servizio Affari generali.
- è possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario.

Si evidenzia però che le comunicazioni ufficiali, da inviarsi mediante gli strumenti tradizionali (fax, posta, …), devono essere autorizzate e/o firmate dalla Direzione Generale e/o dai Responsabili dell'Ufficio o dal Gestore di Filiale, a seconda del loro contenuto e dei destinatari delle stesse.
- Sono state attivate delle caselle di posta certificata (PEC) dalle quali è possibile trasmettere e ricevere documenti ufficiali in sostituzione della posta raccomandata cartacea.
- È obbligatorio porre la massima attenzione nell'aprire i file allegati messaggi di posta elettronica verificandoli con un antivirus aggiornato prima del loro utilizzo.

- E' vietato scaricare file eseguibili o documenti di ogni genere da siti Web o FTP non autorizzati.
- Al fine di garantire la continuità dell'attività aziendale e di ridurre al minimo la necessità di accesso al proprio account, in caso di assenze programmate (ad es. per ferie e permessi) l'utente attiverà la funzionalità "assenza ufficio" nel programma di posta, inserendo le "coordinate" di posta elettronica di un altro soggetto o altre utili modalità di contatto dell'Ufficio.

Sarà comunque consentito al superiore gerarchico dell'utente, dopo aver preventivamente avvisato l'utente se possibile o comunque a persona individuata dall'azienda come garante, accedere alla casella di posta elettronica dell'utente per ogni ipotesi in cui si renda necessario (ad es.: mancata attivazione della funzionalità di risposta automatica o assenza non programmata) al solo fine di garantire la continuità dell'attività aziendale.
Il Servizio Affari generali o altro personale esterno a ciò incaricato, nell'impossibilità di procedere come sopra indicato e nella necessità di non pregiudicare la necessaria tempestività ed efficacia dell'intervento, potrà accedere alla casella di posta elettronica esclusivamente al fine di garantire l'assistenza tecnica e la normale attività operativa o per motivi legati alla sicurezza dei sistemi, delle informazioni aziendali e dei dati personali.
L'assegnatario risponde direttamente dei contenuti espressi ed è consapevole che in ogni caso dovrà manlevare esplicitamente per i contenuti stessi il Titolare e tutti i soggetti ad esso collegati a qualunque titolo eventualmente coinvolti, specificando all'occorrenza che quanto scritto viene fatto a titolo e con diretta responsabilità personale, non necessariamente rispecchiando le posizioni del Titolare e degli altri soggetti.
In caso di contestazioni il Titolare potrà svolgere tutti gli accertamenti tecnici che riterrà opportuni, volti ad identificare il reale autore dei messaggi e rivalersi nelle sedi e nei modi che riterrà appropriati, nei confronti del collaboratore.
Si rammenta che i sistemi di posta elettronica non consentono di garantire la riservatezza delle informazioni trasmesse, si raccomanda quindi agli utenti di non inoltrare dati ed informazioni classificabili "sensibili" o "riservate" con questo mezzo a terzi, ivi inclusi gli stessi indirizzi email aziendali, salvo espressa autorizzazione del Titolare e/o dal Servizio Affari generali.
Al fine di ribadire agli interlocutori la natura esclusivamente aziendale della casella di posta elettronica, i messaggi devono contenere il seguente avvertimento standardizzato:

" Il contenuto di questa e-mail è riservato al solo destinatario e potrebbe contenere informazioni riservate, coperte da segreto professionale, e non soggette a divulgazione ai sensi di legge. Se non ne siete i corretti destinatari, con la presente siete informati che non Vi è assolutamente permessa alcuna divulgazione, copia, distribuzione, o altro uso delle informazioni in essa

contenute. Se per errore avete ricevuto questo messaggio, Vi chiedo cortesemente di informarmi immediatamente al mio indirizzo di posta elettronica. Si ricorda la natura non personale di questo messaggio, essendo questo indirizzo e-mail uno strumento aziendale le risposte potranno essere conosciute nell'organizzazione del mittente".

La **Posta Elettronica Certificata** è oggi utilizzata sempre più frequentemente. Secondo la normativa vigente bisogna considerare i documenti elettronici ricevuti ed inviati equiparabili a posta ordinaria A/R, aventi pieno valore legale.
E' responsabilità dell'assegnatario la custodia delle credenziali, nonché la frequente consultazione della casella stessa, eventualmente delegando un altro dipendente in caso di assenza prolungata al fine di garantire la corretta gestione di eventuali scadenze normative o comunicazioni legali e/o giudiziarie contenute nei documenti ricevuti.

Protezione della postazione, antivirus e aggiornamenti dei sistemi

Il sistema informatico dell'Azienda è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.
Nel caso il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer, disconnettendolo dalla rete e segnalando prontamente l'accaduto al Servizio Affari generali.
Ogni supporto informatico di provenienza esterna all'Azienda dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e nel caso venga rilevato un virus, dovrà essere prontamente consegnato al Servizio Affari generali.
Il sistema informatico mantiene quotidianamente aggiornati i sistemi operativi di ogni pc.
L'utente deve porre attenzione a non interrompere la completa esecuzione degli aggiornamenti.

Infine, si ricorda che la postazione informatica non va lasciata incustodita lasciando accessibili i dati; in caso di allontanamento deve essere attivato un salva schermo protetto con password.

Utilizzo dei sistemi di videoconferenza, telefoni, messaggistica istantanea e centralini VOIP

Il telefono aziendale affidato all'utente è uno strumento di lavoro. Ne viene concesso l'uso esclusivamente per lo svolgimento dell'attività lavorativa, non essendo quindi consentite comunicazioni a carattere personale o comunque non strettamente inerenti l'attività lavorativa stessa.
La ricezione o l'effettuazione di telefonate personali è consentita solo nel caso di comprovata necessità ed urgenza, mediante il telefono fisso aziendale a disposizione. Qualora venisse assegnato un cellulare aziendale all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia.
Al cellulare aziendale si applicano le medesime regole sopra previste per l'utilizzo del telefono aziendale: in particolare è vietato l'utilizzo del telefono cellulare messo a disposizione per inviare o ricevere SMS, MMS od altre tipologie di messaggistica (es. Whatsapp, Telegram, ecc) di natura personale o comunque non pertinenti rispetto allo svolgimento dell'attività lavorativa.
L'eventuale uso promiscuo (anche per fini personali) del telefono cellulare aziendale è possibile soltanto in presenza di preventiva autorizzazione scritta e in conformità delle istruzioni al riguardo impartite.

Se vengono richiesti via telefono dati personali, l'utente deve accertarsi sempre che il richiedente abbia titolo a richiederli. In caso di dati sensibili o di circostanze particolari, l'utente deve valutare la possibilità di utilizzare mezzi più sicuri per la comunicazione dei dati.

I centralini utilizzati presso le nostre filiali hanno funzionalità VOIP (rete interna), grazie alla quale le telefonate tra filiali possono essere effettuate utilizzando il prefisso di ogni sede a costo zero.

Teleassistenza

Per ridurre i tempi di intervento o i costi di gestione dei servizi è consentito attivare sistemi di teleassistenza a disposizione del personale interno o delle ditte esterne per l'accesso ai pc/server del Titolare.
I sistemi di teleassistenza devono prevedere, in caso di accesso ai pc dell'utente, un meccanismo di notifica e accettazione del collegamento. E' infatti vietato attivare sistemi di controllo che consentano la teleassistenza a insaputa dell'utente. I sistemi di teleassistenza da parte di ditte esterne devono essere in ogni caso approvati dai sistemi informatici. Non sono consentiti sistemi di teleassistenza realizzati mediante tecnologie (es. siti web specializzati) che non lasciano traccia dell'avvenuto accesso e non offrono adeguate garanzie per la tutela dei dati personali.

Procedura per accesso alle risorse in caso di assenza dell'incaricato

In caso di prolungata assenza dell'incaricato ed effettiva necessità di accesso alle risorse protette il responsabile del trattamento autorizza il responsabile dei Sistemi informativi a cambiare la password dell'incaricato assente al solo fine di permettere l'accesso alle risorse provvedendo nel contempo alla comunicazione dell'intervento all'incaricato. Terminata la necessità di accesso alle risorse, la credenziale di autenticazione deve essere disabilita. Al rientro in servizio dell'incaricato si provvederà alla creazione di nuove credenziali di autenticazione.

In caso di Assenza programmata l'operatore dovrà attivare il servizio "fuori sede" previsto da Outlook indicando a chi, in sua assenza, dovranno essere inviate le e-mail attinenti le proprie mansioni di servizio.

Trattamento in outsourcing

Possono essere trasmessi al di fuori dei locali del trattamento soltanto i dati personali di cui é consentita la comunicazione o la diffusione, nei limiti e secondo le modalità previste. I dati personali di cui é consentita la diffusione possono essere trasmessi secondo le normali procedure di trasmissione avendo cura che i dati non possano essere modificati da terzi. I dati personali di cui é consentita la comunicazione devono essere trasmessi in modo da garantire la immodificabilità dei dati ed in modo che solo il destinatario abilitato alla ricezione possa leggerne il contenuto. Ad esempio, in caso di trasmissione su supporto magnetico si può utilizzare un formato compresso Zip protetto con password a conoscenza esclusiva del destinatario. Nel caso in cui terzi debbano intervenire e modificare i dati ad essi trasmessi o diffusi é necessario che sia garantita la verifica delle modifiche intervenute.

Trasmissione di dati personali a mezzo fax.

Possono essere trasmessi al di fuori dell'azienda soltanto i dati personali di cui é consentita la comunicazione o la diffusione, nei limiti e secondo le modalità previste. I dati personali di cui é consentita la diffusione possono essere trasmessi secondo le normali procedure di trasmissione avendo cura che solo il destinatario abilitato alla ricezione possa leggerne il contenuto. Accertarsi inoltre che il destinatario sia pronto a riceverlo per evitare che il fax rimanga abbandonato sulla macchina ricevente a disposizione di chiunque. I documenti inviati a mezzo fax sono preceduti dall'apposito modulo contenente, oltre l'intestazione della Azienda e del destinatario la dicitura:

"Questo messaggi0 è ad esclusivo uso del destinatario. Tutte le informazioni contenute sono soggette a riservatezza; la diffusione, la distribuzione e/o la copiatura del presente documento, dei suoi allegati o di sue parti da parte di qualsiasi soggetto diverso dal destinatario è proibita, sia ai sensi dell'art. 616 c.p., che ai sensi del D. Lgs. n. 196/2003. Se avete ricevuto questo messaggio per errore, nello scusarci per l'accaduto, vi preghiamo di distruggerlo e di avvertirci telefonando al numero"

Il documento inviato è archiviato a cura di colui che ha effettuato la spedizione, unitamente al rapporto di trasmissione. Si applicano inoltre tutte le istruzioni relative al trattamento di dati cartacei.

Telefono

Se vi vengono richiesti via telefono dati personali, accertatevi sempre che il richiedente abbia titolo a richiederli.

In caso di dati sensibili od in circostanze particolari, valutate la possibilità di utilizzare mezzi più sicuri di comunicazione dei dati.

Quando dovete comunicare dati personali via telefono, accertatevi che terzi estranei nelle vicinanze non possano udirli.

Ricordatevi che i telefoni cellulare possono contenere dati personali anche sensibili e che possono essere facilmente sottratti o attaccati tramite connessione bluetooth.

Utilizzo dei fax, scanner, fotocopiatrici aziendali

È vietato l'utilizzo dei fax aziendali per fini personali, tanto per spedire quanto per ricevere documentazione, salva diversa esplicita autorizzazione da parte del Responsabile dell'Ufficio.

Possono essere trasmessi al di fuori dell'Azienda soltanto i dati personali di cui è consentita la comunicazione o la diffusione, nei limiti e secondo le modalità previste.

I dati personali di cui è consentita la diffusione possono essere trasmessi secondo le normali procedure di trasmissione, avendo cura che solo il destinatario abilitato alla ricezione possa leggerne il contenuto. L'utente deve accertarsi inoltre che il destinatario sia pronto a riceverlo per evitare che il fax rimanga abbandonato sulla macchina ricevente a disposizione di chiunque. I documenti inviati a mezzo fax sono preceduti da una pagina contenente, oltre l'intestazione dell'Azienda e del destinatario la dicitura:

"Le informazioni contenute nella presente pagina e nei relativi allegati possono essere riservate e sono destinate esclusivamente al su indicato destinatario. La diffusione, la distribuzione e/o la copiatura del presente documento, dei suoi allegati o di sue parti da parte di qualsiasi soggetto diverso dal destinatario è proibita, sia ai sensi dell'art. 616 c.p. che ai sensi del Regolamento UE 769/2016 Se avete ricevuto questo messaggio per errore, vi preghiamo di distruggerlo e di informarci immediatamente telefonicamente oppure inviando una email a: privacy@sogesispa.it"

Il documento inviato è archiviato a cura di colui che ha effettuato la spedizione, unitamente al rapporto di trasmissione. Si applicano inoltre tutte le istruzioni relative al trattamento di dati cartacei.

È vietato l'utilizzo delle fotocopiatrici aziendali per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile di ufficio.

Quando si effettuano copie fotostatiche di documenti contenenti dati personali, è compito dell'utente accertarsi di non lasciare nella macchina il documento originale. Non debbono essere effettuata più copie di quante effettivamente necessarie. Le eventuali copie inutilizzabili o in eccesso debbono essere distrutte immediatamente. Le copie fotostatiche debbono essere distrutte dopo l'utilizzo. Le copie fotostatiche debbo essere trattate con la medesima cura dei documenti originali

Gli stessi accorgimenti sono dovuti in caso di utilizzo delle stampanti condivise in rete locale.

È vietato l'utilizzo di scanner aziendali per fini personali, salvo preventiva ed esplicita autorizzazione da parte del Responsabile di ufficio.

Gestione dati cartacei e pratiche contenenti dati personali

Scopo della presente parte di regolamento è quello di descrivere le modalità di una idonea custodia degli atti e documenti affidati agli incaricati in formato non elettronico contenenti dati personali.

Si considerano soggetti ad ulteriore maggior tutela i dati cartacei contenenti dati sensibili e/o giudiziari.

Sebbene i dati custoditi nei sistemi informativi siano maggiormente protetti da accessi illeciti, per gli atti ed i documenti su supporto cartaceo spesso accade che le precauzioni siano insoddisfacenti. L'utente deve assolutamente evitare di lasciare documenti contenenti dati personali, in particolar modo dati sensibili, abbandonati e incustoditi e deve accertarsi che non siano accessibili in alcun modo a terzi estranei.

Gli atti e documenti su supporto cartaceo, organizzati per pratiche, devono essere conservati all'interno dei seguenti contesti sicuri:

- Armadi protetti mediante ante chiuse a chiave;
- Schedari, archivi, raccoglitori posti all'interno di stanze/uffici, protetti mediante chiusura a chiave.

Nei suddetti contesti è vietato l'accesso a qualsiasi persona diversa dai Responsabili, dai collaboratori e dai dipendenti incaricati preliminarmente autorizzati o altrimenti designati.

Qualora i documenti dovessero essere trasportati all'esterno del posto di lavoro, l'incaricato deve tenere sempre con sé la cartella o la borsa, nella quale i documenti sono contenuti; deve inoltre evitare che sia possibile esaminare, da parte di un soggetto terzo non autorizzato, i documenti trasportati.

Il prelievo di pratiche o singoli documenti dai contesti sicuri nei quali questi sono solitamente conservati va effettuato solo dal responsabile o dall'incaricato che deve effettuare il trattamento per il tempo necessario al trattamento stesso.

Ogni incaricato e/o Responsabile deve controllare e custodire, per l'intero ciclo necessario allo svolgimento del proprio lavoro, gli atti e i documenti contenenti dati personali.

Una volta terminato il trattamento, la pratica va rimessa al suo posto, all'interno della posizione dalla quale è stata prelevata. L'incaricato / il responsabile deve ricordarsi di chiudere a chiave il contenitore, l'armadio o l'ufficio prima di abbandonare la stanza ovvero prima di lasciare incustodita la pratica.

In base al principio di stretta pertinenza dei trattamenti rispetto alle mansioni svolte, potrà accedere solo agli archivi relativi alle banche dati di tipo cartaceo relative ai trattamenti per i quali si è incaricati.

L'incaricato nel trattare documenti contenenti dati sensibili o giudiziari è tenuto a custodirli fino alla restituzione in modo da evitare l'accesso agli stessi dati a persone prive di autorizzazione. L'incaricato deve, inoltre, custodire gli archivi contenenti documenti con dati sensibili e giudiziari, ed evitare che personale non autorizzato vi acceda.

I documenti (o copia degli stessi) non possono, senza specifica autorizzazione, essere portati fuori dai luoghi di lavoro, salvo i casi di comunicazione dei dati a terzi preventivamente autorizzati in via generale dall'azienda.

Mantenere la propria scrivania il più possibile sgombra da carte o fascicoli riportanti dati personali o sensibili in vista.

Non fare uso di cartelle trasparenti per Conservare i documenti cartacei a meno che non siano contenute all'interno degli appositi raccoglitori.

Eseguire copie fotostatiche solo dei documenti ai quali si ha diritto di accedere.

Distruggere le copie fotostatiche utilizzate al termine del trattamento.

Prestare attenzione a non dimenticare documenti presso la macchina fotocopiatrice.

Trattare con un distruggi documenti la documentazione cartacea da cestinare, comprese le copie fotostatiche in eccesso o errate.

L'accesso ai locali che ospitano gli armadi contenenti la documentazione cartacea non è consentito a personale esterno se non in presenza di personale incaricato.

I documenti necessari per lo svolgimento delle proprie mansioni sono affidati agli operatori che ne debbono garantire la custodia in maniera che ad essi non abbiano accesso persone prive di autorizzazione e sono restituiti al termine delle operazioni affidate.

Per custodire e trasportare qualsiasi tipo di documento, inoltre, non si deve far uso di cartelle trasparenti, a meno che non siano contenute all'interno degli appositi raccoglitori.

Raccomandazioni relative al trasporto di dati personali su supporto cartaceo o informatico

Mentre i dati personali custoditi nei sistemi informativi e all'interno di archivi protetti sono ragionevolmente difesi da accessi illeciti, accade purtroppo spesso che le precauzioni che vengono adottate in fase di trasporto da un insediamento all'altro non siano soddisfacenti.
Può capitare assai spesso che documenti cartacei contenenti dati personali, anche sensibili, vengano inseriti in una busta ed abbandonati sul sedile di una autovettura, che talvolta viene lasciata incustodita anche per lungo tempo. Inoltre può capitare che tali dati vengano inseriti nella borsetta, dove si trova anche un borsellino od un telefono cellulare, che possono rappresentare un attraente bersaglio per uno scippatore.
Le stesse preoccupazioni valgono per i dati che vengono riversati su un personal computer portatile, che viene trasportato in giro per il mondo, lasciato talvolta incustodito nelle camere di albergo in condizioni tali che un attaccante, debitamente preparato, potrebbe esser in condizione di estrarre da questo computer dati, che la legge vuole siano tutelati con particolare attenzione.
Ecco perché la legge si preoccupa di dare specifiche indicazioni, in merito al fatto che ad esempio un CD-Rom,un DVD, una penna USB od altri supporti informatici, nonché i documenti su supporto cartaceo, vengano debitamente protetti in fase di trasporto. Per dati ad alto rischio, come i dati sensibili genetici, si prescrive perfino l'utilizzo di un contenitore con serratura, che potrebbe anche

essere una borsa con un lembo di chiusura protetto da una serratura a codice o da chiave, oppure con altri accorgimenti, come ad esempio una busta sigillata, che mette in immediata evidenza una possibile violazione.
Indipendentemente dallo strumento specifico di protezione dei dati, è indispensabile che l'incaricato, che occasionalmente o sistematicamente trasporta questi dati, archiviati su qualsiasi tipo di supporto, presti particolare attenzione, non abbandonando mai i dati stessi ed accertandosi che essi non siano, in alcun modo, accessibili a terzi estranei.

Non per nulla, il disciplinare di sicurezza impone che i dati, che vengono trasferiti su supporto informatico, se particolarmente sensibili, debbano addirittura essere preventivamente cifrati con un algoritmo crittografico, in modo che anche l'eventuale sottrazione non comporti la diffusione dei dati personali.

Accesso alla Sede

Diligenza della custodia e restituzione

Il dipendente che abbia ricevuto in custodia una o piu' chiavi di accesso alla sede è tenuto a conservarla con diligenza applicando le seguenti istruzioni:

- conservare in luogo ignoto e non accessibile a terzi, ivi inclusi altri dipendenti aziendali e familiari;
- non esibire le chiavi stesse;
- non divulgare il fatto che le chiavi sono state a lui affidate in custodia;
- non affidare, neppure temporaneamente, a chicchessia le chiavi stesse;
- la chiavi non devono essere mai lasciate abbandonate, neppure per pochi istanti, in quanto è possibile la copia con mezzi meccanici oppure "leggerle" o memorizzarle".
- non attaccare nessun contrassegno alle chiavi che ne rilevi in qualche modo la destinazione e l'uso.
- non portare le chiavi al seguito durante i fine settimana, i periodi feriali o le uscite serali.
- conservare le chiavi nella propria abitazione in luogo difficilmente individuabile e separato dalle altre chiavi della propria abitazione.

Denuncia di smarrimento

Il depositario della chiave deve denunciare l'eventuale smarrimento delle chiavi, a lui affidata in custodia, non appena se ne sia reso conto, alle Autorità competenti.
E' vietata la divulgazione dell'avvenuto smarrimento della chiave a chiunque altro.

Cessazione della custodia

E' fatto obbligo al dipendente che per ragione del suo incarico o della natura della sua attività abbia ricevuto in custodia una o più chiavi, di restituirle al Responsabile del Servizio Affari Generali nel momento in cui cessano le ragioni per le quali le chiavi gli sono state affidate in custodia.
Qualora, all'atto della riconsegna le chiavi consegnate risultassero alterate e/o mancanti, si applicheranno al dipendente adeguate sanzioni disciplinari per l'infrazione eventualmente commessa.

Documentazione della custodia

Al momento della consegna e al ritiro delle chiavi il Responsabile del Servizio Affari Generali provvederà a redigere apposito verbale.

Duplicazione chiavi

E' tassativamente proibito a chicchessia, di procedere in proprio, o autorizzare altri a realizzare duplicati delle chiavi.

Accesso ai dati trattati dall'utente e Sistemi di Controllo

Oltre che per motivi di sicurezza del sistema informatico, anche per motivi tecnici e/o manutentivi (ad esempio, aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware, etc.) o per finalità di controllo e programmazione dei costi aziendali (ad esempio, verifica costi di connessione ad internet, traffico telefonico, etc.), comunque estranei a qualsiasi finalità di controllo dell'attività lavorativa, è facoltà della Direzione Aziendale, tramite il Servizio Affari generali o addetti alla manutenzione, accedere direttamente, nel rispetto della normativa sulla privacy, a tutti gli strumenti informatici aziendali e ai documenti ivi contenuti, nonché ai tabulati del traffico telefonico.

In caso di anomalie, il personale incaricato dal Servizio Affari generali effettuerà controlli anonimi che si concluderanno con avvisi generalizzati diretti ai dipendenti dell'area o del settore in cui è stata rilevata l'anomalia, nei quali si evidenzierà l'utilizzo irregolare degli strumenti aziendali e si inviteranno gli utenti ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base individuale potranno essere compiuti solo in caso di successive ulteriori anomalie e per i casi di particolare gravità solo su autorizzazione della Direzione.

In nessun caso verranno compiuti controlli prolungati, costanti o indiscriminati; non verranno attivati sistemi o raccolti dati che possano ledere la privacy dei dipendenti. Tutti i dati raccolti saranno trattati in forma pseudonimizzata.

In ogni caso, i tempi di conservazione dei log non saranno mai superiori ai 15 giorni, escluso il caso di necessità per specifiche esigenze tecniche, esercizio di un diritto in sede giudiziaria o per ordine dell'Autorità.

La non osservanza del presente regolamento può comportare sanzioni disciplinari, civili e penali come previsti dal contratto di lavoro, dalle norme e dalle leggi dello Stato.

Osservanza delle disposizioni in materia di Privacy

È obbligatorio attenersi alle disposizioni in materia di Privacy e protezione dei dati personali, come indicato nella lettera di designazione ad incaricato ed autorizzazione al trattamento dei dati personali ai sensi del GDPR (General Data Protection Regulation) regolamento UE 679/2016 e del "Codice Privacy" (Codice in materia di protezione dei dati personali) D.Lgs. n. 196/2003.

Sanzioni

È fatto obbligo a tutti gli utenti di osservare le disposizioni portate a conoscenza con il presente Regolamento. Il mancato rispetto o la violazione delle regole sopra ricordate è perseguibile nei confronti del personale dipendente con provvedimenti disciplinari e risarcitori previsti dal vigente CCNL nonché con tutte le azioni civili e penali consentite.

Aggiornamento e revisione

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente Regolamento. Le proposte verranno esaminate dalla Direzione Generale e dal Servizio Affari generali.

Il presente Regolamento è soggetto a revisione con frequenza annuale.