YACHTLINE ARREDOMARE 1618 SPA

Viale Regina Margherita, 1
20122 Milano (MI)
Tel: 0587755931 - Fax: 0587756180
P.IVA 01298310507
PEC: arredomaresrl@pecimprese.it

REGOLAMENTO INTERNO SULL'USO DEL SISTEMA INFORMATIVO - ISTRUZIONI PER L'ADDETTO (allegato alle nomine degli addetti)

L'Art.29 Reg. UE 2016/679 definisce come persone autorizzate" le persone fisiche che sotto la responsabilità di un Titolare o di un Responsabile agiscono accedendo a dati personali".

Nell'ambito di competenza a lei assegnato nella Nomina dal Titolare o dal Responsabile, vengono sotto riportate le istruzioni a cui è tenuto ad attenersi nel trattamento di dati personali, in conformità alle normative vigenti sulla Privacy.

PROCEDURE PER LA CLASSIFICAZIONE DEI DATI

La Persona autorizzata deve essere sempre in grado di individuare il tipo di dato che sta trattando secondo quanto stabilito dalla Legge. Qualora non fosse in grado, deve fare riferimento al Responsabile o al Titolare del Trattamento.

La natura dei dati trattati

Vengono riportate di seguito le definizioni e i riferimenti normativi per una più chiara comprensione:

- **«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;

La Persona autorizzata o comunque il Dipendente o Collaboratore che, nell'esercizio delle sue Mansioni si trova a venire a conoscenza di dati riservati deve essere sempre in grado di individuarli. Qualora non fosse in grado, deve fare riferimento al Responsabile o al Titolare del Trattamento.

Viene riportata di seguito una definizione di "dati riservati"

- **"dati riservati":** si tratta di informazioni orali e/o scritte relative alla Società, agli Amministratori, dipendenti e collaboratori, ai prodotti realizzati dalla Società o comunque nella disponibilità della stessa, ai terzi con i quali la Società si relaziona nello svolgimento della propria attività d'impresa, quali Clienti e Potenziali clienti, Fornitori etc, incluse le informazioni relative a relazioni interne, manuali aziendali, rapporti interni, corrispondenza scritta, telefonica ed elettronica, studi, disegni, norme o specifiche, progetti e la relativa commessa nel suo complesso, prototipi, impianti, macchine, dispositivi, apparecchiature per i test ed i metodi impiegati, soluzioni tecniche e tecnologiche, informazioni tecniche e tecnologiche, costruttive e di processo, attrezzature/attrezzaggi per effettuare lavorazioni, aspetti tecnici, progettuali e brevettuali, procedure e metodologie, lay-out, dati, grafici, proposte, strategie, dichiarazioni finanziarie ed operative, programmi informatici e di training, elenchi fornitori e informazioni tecniche sui fornitori, elenchi clienti e informazioni tecniche sui clienti, iniziative commerciali, tecniche commerciali e di gestione della Società con i terzi (le "**Informazioni Riservate");** tutti dati di cui il dipendente o il collaboratore può venire a conoscenza in occasione dell'esecuzione del Contratto di Lavoro o del Contratto di Collaborazione

AFFIDAMENTO ALLE PERSONE AUTORIZZATE DI DOCUMENTI, CONTENENTI DATI PERSONALI, E MODALITÀ DA OSSERVARE PER LA CUSTODIA DEGLI STESSI

TRATTAMENTO SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Per il trattamento dei documenti cartacei rispettare sempre le indicazioni del Titolare o del Responsabile in merito agli archivi a cui poter accedere e ai documenti che è possibile trattare: non trattare nessun documento al di fuori delle autorizzazioni.

Una volta presi in carico, gli atti e i documenti, contenenti dati personali, non devono essere lasciati liberi di vagare senza controllo ed a tempo indefinito per gli uffici, ma occorre provvedere in qualche modo a controllarli e custodirli, per poi restituirli al termine delle operazioni affidate.

In caso di affidamento di atti e documenti contenenti dati di categorie particolari, il controllo e la custodia devono avvenire in modo tale, che ai dati non accedano persone prive di autorizzazione. A tale fine, è quindi necessario dotarsi di cassetti con serratura, o di altri accorgimenti aventi funzione equivalente, nei quali riporre i documenti contenenti dati sensibili o giudiziari prima di assentarsi dal posto di lavoro, anche temporaneamente (ad esempio, per recarsi in mensa). In mancanza di tali strumenti sollecitare la Direzione affinché provveda.

Assicurare l'accesso a tali archivi alle sole persone autorizzate da specifico e scritto profilo di autorizzazione ricordando loro di non abbandonare mai tali documenti e di riconsegnarli non appena terminato l'incarico che ne ha determinato il trattamento.

Qualora si debbano utilizzare anche nei giorni successivi i documenti potranno essere riposti in tali cassetti al termine della giornata di lavoro. Al termine del trattamento dovranno invece essere restituiti all'archivio.

I SISTEMI INFORMATICI AZIENDALI

Il personal computer (fisso o mobile) 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 e possono essere utilizzati solo per fini professionali (in relazione, ovviamente alle mansioni assegnate) e non per scopi personali, tanto meno per scopi illeciti; debbono essere prontamente segnalati all'azienda il furto, danneggiamento o smarrimento di tali strumenti.

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, l'integrità del proprio sistema informatico e la coerenza delle sue configurazioni e dei suoi archivi con le finalità aziendali. In questo contesto l'azienda potrà per necessità di sicurezza aziendale o per esigenze di continuità della normale attività lavorativa, accedere agli archivi di corrispondenza elettronica o ai file di log riservati alla tracciatura degli eventi di connessione.

Utilizzo del personal computer

- è consentito installare programmi provenienti dall'esterno solo se espressamente autorizzati dal Titolare o dal Responsabile; non è consentito scaricare file dalla rete o contenuti in supporti magnetici e/o ottici non aventi alcuna attinenza con la propria prestazione lavorativa;
- 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 consentita l'installazione sul proprio PC di mezzi di comunicazione propri (come ad esempio i modem);
- non è consentito condividere file, cartelle, hard disk o porzioni di questi del proprio computer, per accedere a servizi non autorizzati di peer to peer al fine di scaricare materiale elettronico tutelato dalle normative sul Diritto d'Autore (software, file audio, film, etc.);
- i Personal Computer "stand alone" o in rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo, essere utilizzate per scopi diversi. Pertanto, qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità; l'azienda si riserva la facoltà di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la sicurezza del sistema ovvero acquisiti o installati in violazione delle presenti istruzioni.
- E' obbligatorio provvedere allo spegnimento del personal computer al termine della giornata lavorativa. Ciò per motivi non solo di sicurezza ma anche per garantire una maggiore sostenibilità aziendale (risparmio energetico)

Utilizzo di internet

- non è consentito navigare in siti non attinenti allo svolgimento delle mansioni assegnate;
- a maggior ragione non è consentito navigare in siti che accolgono contenuti contrari alla morale e alle prescrizioni di Legge;
- non è inoltre consentito navigare in siti che possano rivelare una profilazione dell'individuo relativa a dati 'particolari' ai sensi del Reg. UE 2016/679: quindi siti la cui navigazione palesi elementi attinenti alla fede religiosa, alle opinioni politiche e sindacali del dipendente o le sue abitudini sessuali;
- non è consentita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo casi direttamente autorizzati dal Titolare o dal Responsabile del Trattamento e con il rispetto delle normali procedure di acquisto;
- non è consentito lo scarico di software gratuiti trial, freeware e shareware prelevati da siti Internet, se non espressamente autorizzato dal Titolare o dal Responsabile;
- non è consentito lo scarico di materiale elettronico tutelato dalle normative sul Diritto d'Autore (software, file audio, film, etc.) né attraverso Internet né attraverso servizi di peer to peer;
- è vietata ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
- non è permessa la partecipazione durante l'orario di lavoro, per motivi non professionali a Forum e giochi in rete pubblica, l'utilizzo di chat line, di bacheche elettroniche 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.

Utilizzo di applicazioni di intrattenimento musicale

E' consentito l'utilizzo di applicazioni di intrattenimento musicale (spotify Apple Music, Webradio, etc) durante l'attività lavorativa a patto che venga utilizzato sul proprio device personale (smartphone, iPhone). Tale specifica è dovuta al fine di non saturare la connettività internet aziendale.

Utilizzo delle reti Wifi

Yachtline 1618 S.p.A. dispone di più reti wifi ciascuna con scopi ben precisi. Il loro utilizzo è determinato in funzione dello scopo.

L'azienda mette a disposizione anche un wifi specifico per uso personale: l'addetto che abbia necessità di utilizzare il wifi dovrà rivolgersi all'**Ufficio IT** che indicherà lo strumento da utilizzare.

Utilizzo del servizio di posta elettronica

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

- non è consentito utilizzare la posta elettronica (interna ed esterna) per motivi non attinenti allo svolgimento delle mansioni assegnate;
- 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;
- la posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei, e dunque, non deve essere usata per inviare informazioni, dati o documenti di lavoro "strettamente Riservati";
- non è consentito l'utilizzo dell'indirizzo di posta elettronica aziendale per la partecipazione a dibattiti, Forum o mail-list; solo in questo ultimo caso è possibile, previa autorizzazione per la verifica della validità dell'emittente, iscriversi a servizi di informazione strettamente inerenti all'attività aziendale;
- nel caso esista un dominio di proprietà aziendale (es.: nomeazienda.it) al quale sia collegato un servizio di posta e la relativa casella (es.: rossi@nomeazienda.it), non è consentito utilizzare web mail esterni, ovvero caselle di posta elettronica non appartenenti al dominio o ai dominii aziendali salvo diversa ed esplicita autorizzazione.

L'Azienda può attivare account di mail relativi a caselle di tipo generico (info@, amministrazione@, ufficio@ etc…) sia a caselle di tipo nominale (n.cognome@, nome.cognome@, cognome@, nome@ etc…).

L'utente, in caso di improvvisa o prolungata assenza o impedimento, può **delegare un altro utente** (C.d. fiduciario) all'accesso ai dati registrati negli strumenti elettronici in uso all'utente medesimo, se ritenuti rilevanti per lo svolgimento dell'attività lavorativa. Dell'avvenuto conferimento della delega l'utente delegante deve informare tempestivamente il Dirigente/Responsabile dell'ufficio di relativa appartenenza. Per agevolare la nomina di un fiduciario l'Azienda mette a disposizione dell'utente un **modulo di delega a fiduciario.** Il modulo è disponibile presso l'Ufficio IT. Di ciascun accesso dovrà essere redatto apposito verbale e informato l'utente delegante alla prima occasione utile. Sarà comunque consentito al superiore gerarchico dell'utente o, comunque, sentito l'utente, a persona individuata dall'azienda, accedere alla casella di posta elettronica dell'utente per ogni ipotesi in cui si renda necessario.

Il personale dell'Ufficio IT, 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 per le sole finalità di manutenzione del sistema

Il personale dell'Ufficio IT, per conto dell'azienda potrà effettuare "query" ovvero interrogazioni dei database di posta elettronica ai fini di ottenere report utili per la verifica dello stato di avanzamento delle varie attività e delle commesse. Tali interrogazioni non entrano nel merito del contenuto dei messaggi di posta elettronica scambiati. Tale attività viene effettuata attraverso il portale di amministrazione Microsoft Exchange.

In caso di cessazione del rapporto di lavoro tra l'Azienda e l'incaricato è vietato a quest'ultimo di cancellare i messaggi di mail inviati e/o ricevuti tramite l'account assegnatogli, essendo quei messaggi un patrimonio aziendale.

In caso di cessazione del rapporto di lavoro tra l'Azienda e l'incaricato la casella mail assegnata potrà essere mantenuta attiva per un periodo massimo pari a 1 mese o dismessa, anche prima di 1 mese, in base alle necessità aziendali. Se mantenuta attiva potrà essere assegnata ad altro personale aziendale oppure le mail ricevute potranno essere inviate ad altra mail aziendale e ricevute e lette da altro personale aziendale.

L'azienda potrà predisporre un messaggio di risposta automatica per avvisare il mittente che il destinatario non lavora più in azienda. Il contenuto della mail (inviato o ricevuto) resta di proprietà dell'Azienda che potrà decidere se conservarlo e archiviarlo (mantenimento dei back up) oppure eliminarlo definitivamente.

Utilizzo dei telefoni cellulari (e degli altri dispositivi quali smarphone e tablet)

Anche i telefonini, smartphone e tablet che l'azienda assegna ai dipendenti o le Sim necessarie per il loro funzionamento, sono strumenti di lavoro. In generale questi dispositivi non possono essere ceduti né fatti utilizzare a terzi.

La Direzione può disporre dei dispositivi assegnati secondo necessità, sostituendo, aggiornando, rimuovendo o adeguando in tutto o in parte le componenti hardware e/o software di cui essi si compongono, senza necessità di preavviso e di richiesta di consenso da parte dell'utilizzatore.

La Direzione è l'unico che può provvedere o autorizzare l'installazione, l'aggiornamento e la configurazione di dispositivi hardware e/o software sui programmi in uso, sui telefoni e più in generale sull'intero sistema telefonico. In particolare, in modo non esaustivo, si intende stigmatizzare i comportamenti relativi ai seguenti divieti:

- Non è consentito modificare le caratteristiche hardware e software impostate sul telefono o sugli altri dispositivi
- Non è consentita l'installazione di programmi diversi da quelli autorizzati.
- Non è consentita la riproduzione, la duplicazione, il salvataggio o lo scarico (download o file sharing) di programmi o file di ogni tipo (testo, immagini, video, audio, eseguibili) in violazione delle norme sul diritto d'autore, ai sensi delle Legge n. 128 del 21 maggio 2004.
- Non è consentita l'installazione di ulteriori dispositivi rispetto a quelli in dotazione.
- Non è consentito l'uso di qualsiasi dispositivo esterno collegabile al telefono (o allo smartphone o al tablet), se non quelli aziendali o quelli autorizzati.
- L'utilizzatore che abbia necessità di apportare modifiche software o hardware al dispositivo in dotazione, installando nuovi programmi o dispositivi, deve farne preventiva richiesta alla Direzione. Quanto memorizzato sui supporti interni al dispositivo potrebbe essere oggetto di analisi, controllo e duplicazione da parte della Direzione o da personale tecnico autorizzato, per migliorare l'affidabilità, la disponibilità e l'efficienza del dispositivo. Qualora fossero individuate componenti hardware e/o software (programmi, documenti, dispositivi esterni, ecc.) non corrispondenti ai criteri di sicurezza e di operatività individuati dalla Direzione e non esplicitamente autorizzati, tali componenti potrebbero essere rimossi e l'utilizzatore potrebbe essere coinvolto negli accertamenti e nelle verifiche del caso.

L'utilizzatore è responsabile dell'utilizzo e della custodia del dispositivo, In particolare l'utente deve garantire la riservatezza, l'integrità e la disponibilità dei dati contenuti al suo interno rispettando le seguenti best practices:

- Attivare la richiesta di autenticazione per lo sblocco preferendo l'inserimento e la gestione della password in conformità a quanto indicato nel presente regolamento;
- Impostare il blocco schermo automatico dopo 5 minuti di inutilizzo;
- Installare e mantenere attivo e aggiornato un sistema Antivirus;
- Evitare di salvare dati aziendali all'interno dello smartphone;
- Nel caso in cui sia necessario salvare dati aziendali sullo smartphone è opportuno proteggere tali informazioni con password adeguata adottando uno dei seguenti procedimenti:
    - criptare i singoli file;
    - criptare il disco in cui vengono salvati;
    - salvare i dati all'interno della cassaforte del dispositivo.

Utilizzo del proprio device personale per finalità aziendali (BYOD)

L'azienda autorizza, in presenza di determinate condizioni da valutare preventivamente a cura dell'**Ufficio IT**, l'utilizzo dello smartphone personale del dipendente o del collaboratore per finalità aziendali (come ad esempio per accedere alla posta elettronica aziendale o per comunicare attraverso strumenti di messaggistica istantanea).

Il dipendente o il collaboratore che intenda avvalersi del proprio smartphone o, in generale, di un proprio dispositivo personale, dovrà farne preventiva richiesta all'Ufficio IT che consentirà l'utilizzo del dispositivo personale qualora sussistano determinate condizioni, definendo con il dipendente o il collaboratore interessato, misure da porre in essere prima del trattamento ivi comprese le opportune considerazioni in caso di coinvolgimento di cloud providers in una o più operazioni di trattamento.

Sulla base del **principio di trasparenza** l'Ufficio IT provvederà, per conto del Titolare del Trattamento o del Responsabile, a rendere edotti gli interessati al fine di ridurre i rischi di compromissione dei dati e, contemporaneamente, per garantire la privacy.

Al fine di garantire lo scambio sicuro dei dati tra la infrastruttura IT ed il device del dipendente è vietato l'utilizzo di strumenti non approvati quali a titolo esemplificativo e non esaustivo whatsapp, etc. L'azienda si è dotata di strumenti quali **Microsoft Teams** che il dipendente o il collaboratore potrà utilizzare su proprio dispositivo personale. Per la sua attivazione il dipendente dovrà rivolgersi all'Ufficio IT

Non è ammesso l'utilizzo di tool gratuiti di backup online da parte del dipendente/collaboratore.

Il dipendente o il collaboratore che intenda avvalersi di propri device dovrà impegnarsi a garantire la riservatezza, l'integrità e la disponibilità dei dati aziendali contenuti nel proprio dispositivo personale rispettando le seguenti best practices:

- Attivare la richiesta di autenticazione per lo sblocco preferendo l'inserimento e la gestione della password in conformità a quanto indicato nel presente regolamento;
- Impostare il blocco schermo automatico dopo 5 minuti di inutilizzo;
- Installare e mantenere attivo e aggiornato un sistema Antivirus;
- Evitare di salvare dati aziendali all'interno dello smartphone;
- Nel caso in cui sia necessario salvare dati aziendali sullo smartphone è opportuno proteggere tali informazioni con password adeguata adottando uno dei seguenti procedimenti:
    - criptare i singoli file;
    - criptare il disco in cui vengono salvati;
    - salvare i dati all'interno della cassaforte del dispositivo.

Nel caso di coinvolgimento del proprio dispositivo personale in un **Data Breach** (violazione dei dati) il dipendente o il collaboratore dovrà applicare le policy aziendali in materia, descritte all'interno del presente regolamento in apposita sezione.

Nel caso di **perdita o furto del proprio device** il dipendente o il collaboratore dovrà immediatamente attivare la procedura prevista all'interno del presente regolamento in apposita sezione.

Al momento della interruzione del rapporto di lavoro o di collaborazione l'azienda provvederà immediatamente a rimuovere ogni accesso presente sul dispositivo personale ed il dipendente o collaboratore dovrà garantire la cancellazione immediata di eventuali dati aziendali presenti all'interno del dispositivo stesso

Il Dipendente/collaboratore può portare il tuo Notebook/Device personale in ufficio ma non può connetterlo a nessuna rete della azienda, sia cablata che wifi. Se il dipendente/collaboratore ha necessità di connettere il dispositivo personale dovrà chiedere preventiva autorizzazione all'Ufficio IT. In nessun caso è possibile utilizzare la condivisione delle password delle reti wifi concesse in uso.

Smart Working

Nello svolgimento delle attività in smart working valgono le stesse regole per il trattamento dei dati personali all'interno dell'azienda. In particolare, il dipendente/utente dovrà adottare i seguenti comportamenti al fine di garantire una modalità sicura di gestione e utilizzo dei dati:

- Al fine di garantire un'efficace ed efficiente interazione, nonché un ottimale svolgimento della prestazione lavorativa, tutto il personale quando presta la propria opera al di fuori dei locali di YACHTLINE 1618 SPA dovrà garantire il collegamento telefonico e via mail come se fosse all'interno dei locali aziendali.
- Il collegamento alla rete aziendale avverrà mediante una VPN (Virtual Private Network) di tipo (client2site) con credenziali rilasciate dalla Direzione (in collaborazione con l'Ufficio IT) e consentirà l'utilizzo di tutti gli applicativi aziendali necessari alla prestazione lavorativa. Il dipendente/collaboratore dovrà impedire l'accesso a dati e asset aziendali ai soggetti non autorizzati (es.: coniuge, familiari ecc.).
- L'utente dovrà utilizzare, per rendere la prestazione lavorativa, soltanto gli eventuali strumenti tecnologici "aziendali" (computer, smartphone, ecc.) che l'azienda ha concesso in uso anche al di fuori della struttura.
- L'utente non dovrà mai utilizzare dispositivi esterni di memorizzazione di cui non ne conosce la provenienza (es.: chiavetta USB, hard disk esterni ecc.).
- Qualora la prestazione lavorativa fosse al di fuori dell'abitazione, es. spazi pubblici, spazi di coworking, locali, mezzi di trasporto etc., ogni utente dovrà assicurarsi che lo schermo sia protetto dall'osservazione indesiderata da parte di terzi (ad esempio applicando al proprio schermo il "privacy film").
- Le credenziali di accesso devono essere conservate con diligenza e riservatezza onde evitarne la conoscibilità da parte di soggetti non autorizzati e vanno inserite ogni volta che si effettua l'accesso al sistema. Non è possibile memorizzarle per effettuare il login automatico.
- La casella mail aziendale deve essere utilizzata dal solo utente autorizzato rispettando i criteri di riservatezza e diligenza indicati al punto precedente.
- Nei casi in cui il dipendente sia stato autorizzato a detenere presso la sede scelta per lo svolgimento del proprio lavoro, documentazione cartacea indispensabile per la propria attività, la stessa dovrà essere raccolta in un porta documenti avente al suo interno un indice completo e riportante il nome del dipendente ed un suo recapito telefonico.
- In caso di rischio di violazione di dati, il dipendente è tenuto a darne immediata comunicazione, segnalando tempestivamente qualunque evento concernente una possibile violazione al Titolare del Trattamento (YACHTLINE 1618 SPA) secondo quanto stabilito nella sezione Data Breach nonché sulla base degli obblighi derivanti dal Regolamento Europeo 2016/679.

MODALITÀ PER ELABORARE E CUSTODIRE LE PASSWORD

Le credenziali di autenticazione sono assolutamente personali e non cedibili, per nessuna ragione.

Se si è in possesso di più credenziali di autenticazione, fare attenzione ad accedere ai dati unicamente con la credenziale relativa al trattamento in oggetto.

Rispettare l'ambito di competenza (i dati cui poter accedere) ed il profilo di autorizzazione (tipi di trattamento consentito) indicate nella propria Nomina a Persona autorizzata.

Nel caso in cui sia prevista la figura del custode delle copie credenziali, è necessario trascrivere una copia della propria parola chiave e consegnarla in busta chiusa (meglio se sigillata) alla Persona autorizzata od al responsabile incaricato alla loro custodia. Fare riferimento al Titolare od al Responsabile per i dettagli operativi della procedura.

Elaborare le password seguendo le istruzioni sotto riportate.

SCELTA DELLE PASSWORD

Il più semplice metodo per l'accesso illecito a un sistema consiste nell'indovinare la password dell'utente legittimo. In molti casi sono stati procurati seri danni al sistema informativo a causa di un accesso protetto da password "deboli". La scelta di password "forti" è, quindi, parte essenziale della sicurezza informatica.

COSA NON FARE

- NON dica a nessuno la sua password. Ricordi che lo scopo principale per cui usa una password è assicurare che nessun altro possa utilizzare le sue risorse o possa farlo a suo nome.
- NON scriva la password in nessun posto in cui che possa essere letta facilmente, soprattutto vicino al computer.
- Quando immette la password NON faccia sbirciare a nessuno quello che sta battendo sulla tastiera.
- NON scelga password che si possano trovare in un dizionario. Su alcuni sistemi è possibile "provare" tutte le password contenute in un dizionario per vedere quale sia quella giusta.
- NON creda che usare parole straniere renderà più difficile il lavoro di scoperta, infatti chi vuole scoprire una password è dotato di molti dizionari delle più svariate lingue.
- NON usi il suo nome utente. È la password più semplice da indovinare.
- NON usi password che possano in qualche modo essere legate a lei come, ad esempio, il suo nome, quello di sua moglie/marito, dei figli, del cane, date di nascita, numeri di telefono etc.

COSA FARE OBBLIGATORIAMENTE

- la password deve essere composta da almeno otto caratteri o, se il sistema non l'accetta, da un numero di caratteri pari a quello consentito dal sistema; è buona norma che, di questi caratteri, da un quarto alla metà siano di natura numerica;
- la Persona autorizzata deve provvedere a modificare la password immediatamente, non appena la riceve per la prima volta, da chi amministra il sistema;
- la password deve essere modificata dalla Persona autorizzata almeno ogni 6 mesi;
- se il trattamento riguarda dati sensibili o giudiziari la password deve essere modificata almeno ogni tre mesi;

COSA FARE PRATICAMENTE

Utilizzare più di una parola e creare password lunghe

A volte è più semplice ricordare una frase completa di senso compiuto piuttosto che una parola complicata, e questa tecnica oltre a facilitare la memorizzazione migliora la sicurezza stessa della parola chiave: la lunghezza influisce sulle difficoltà di individuazione e ci consente di utilizzare lo "spazio" tra una parola e l'altra come ulteriore elemento da intercettare.

Inoltre è bene sapere che diversi strumenti di intercettazione presumono che le password non siano formate da più di 14 caratteri, e quindi, anche senza complessità, le password molto lunghe (da 14 a 128 caratteri) possono rappresentare un'ottima protezione contro possibili violazioni. Non tutti i software sono tuttavia in grado di accettare password superiori a 14 caratteri: ad esempio i sistemi operativi Windows 95 98 e Me non oltrepassano questo limite.

Utilizzare numeri e simboli al posto di caratteri

Non limitarsi alle sole lettere ma, dove possibile, utilizzare l'ampia gamma di minuscole/maiuscole, numeri e simboli a disposizione sulla propria tastiera:

- Caratteri minuscoli: a, b, c,...
- Caratteri maiuscoli: A, B, C,...
- Caratteri numerici: 0,1,2,3,4,5,6,7,8,9
- Caratteri non alfanumerici: (< > , .) ` ~ ! $ % ^ ; * - + = | \ { @ # } [/] : ; " '?

Non inserirli alla fine di una parola nota come ad es.:"computer987". In questo caso la password può essere identificata abbastanza facilmente: la parola "computer" è inclusa in molti dizionari contenenti nomi comuni e quindi dopo aver scoperto il nome restano solo 3 caratteri da identificare. Al contrario, è sufficiente sostituire una o più lettere all'interno della parola con simboli che possono essere ricordati facilmente. Ad esempio si può provare a

utilizzare "@"al posto di "A", "$"al posto di "S", zero (0) o la doppia parentesi () al posto di "O", e "3"al posto di "E": si tratta di trovare delle analogie che ci rendano familiare la sostituzione di lettere con simboli e numeri. Con alcune sostituzioni si possono creare password riconoscibili per l'utente, ad esempio (es.: "Ve$tit0 di Mari0"), già sufficientemente lunghe e estremamente difficili da identificare o decifrare.

Cercare di realizzare password utilizzando caratteri appartenenti a tutti i quattro gruppi rappresentati nella lista.

OBBLIGO DI NON LASCIARE INCUSTODITI E ACCESSIBILI GLI STRUMENTI ELETTRONICI, MENTRE È IN CORSO UNA SESSIONE DI LAVORO

Non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento. È necessario terminare la sessione di lavoro, al computer, ogni volta che ci si deve allontanare, anche solo per cinque minuti effettuando un log out o mettendo in atto accorgimenti tali, per cui anche in quei cinque minuti il computer non resti:

- incustodito: può essere sufficiente che un collega rimanga nella stanza, durante l'assenza di chi sta lavorando con lo strumento elettronico, anche se la stanza rimane aperta;
- accessibile: può essere sufficiente chiudere a chiave la stanza, dove è situato lo strumento elettronico, durante l'assenza, anche se nella stessa non rimane nessuno.

Non si devono invece mai verificare situazioni in cui lo strumento elettronico venga lasciato attivo, durante una sessione di trattamento, senza che sia controllato da una Persona autorizzata al trattamento o senza che la stanza in cui è ubicato venga chiusa a chiave.

Sono installati strumenti software specifici (es.: screen saver) che, trascorso un breve periodo di tempo predeterminato dall'utente in cui l'elaboratore resta inutilizzato, non consente più l'accesso all'elaboratore se non previa imputazione di password. Verifichi con i Responsabili o con il Titolare le possibilità di abilitazione dello strumento.

PROCEDURE E MODALITÀ DI UTILIZZO DEGLI STRUMENTI E DEI PROGRAMMI ATTI A PROTEGGERE I SISTEMI INFORMATIVI

Di seguito alcune indicazioni e linee guida tese a garantire la protezione dei sistemi informativi e dei dati aziendali

FATTORI DI INCREMENTO DEL RISCHIO E COMPORTAMENTI DA EVITARE

- uso di software gratuito (trial, freeware o shareware) prelevato da siti Internet o in allegato a riviste o libri;
- collegamento in Internet con download di file eseguibili o documenti di testo da siti web o da siti FTP;
- collegamento in Internet e attivazione degli applets di Java o altri contenuti attivi;
- file attached di posta elettronica;
- accertare l'attendibilità del mittente della mail

LINEE GUIDA PER LA PREVENZIONE DEI MALWARE, TROJAN, VIRUS

Un virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi. Alcuni virus si limitano a riprodursi senza ulteriori effetti, altri si limitano alla semplice visualizzazione di messaggi sul video, i più dannosi arrivano a distruggere tutto il contenuto del disco rigido.

Gli stessi possono arrivare dalla navigazione internet, dalla posta elettronica, dagli allegati della posta elettronica, da fonti esterne quali chiavette USB ed affini, da smartphone.

Come prevenire i virus:

1. Usi soltanto programmi provenienti da fonti fidate

Ogni programma deve essere autorizzato preventivamente dall'azienda e dall'Ufficio IT e sottoposto alla scansione prima di essere installato. Non è possibile utilizzare programmi non autorizzati

2. Assicurarsi che il proprio dispositivo sia monitorato dall'antivirus

Si assicuri che il suo dispositivo sia sotto corretta protezione antivirus: se sul dispositivo compaiono "pop-up" o notifiche relative all'antivirus, dovrà essere fatto immediatamente presente all'Ufficio IT.

3. Non diffonda messaggi di provenienza dubbia

Se riceve messaggi che avvisano di un nuovo virus pericolosissimo, lo ignori: le mail di questo tipo sono dette con terminologia anglosassone hoax (termine spesso tradotto in italiano con "bufala"), l'equivalente delle "leggende metropolitane" della rete. Questo è vero anche se il messaggio proviene dal suo migliore amico, dal suo capo o da un tecnico informatico. È vero anche e soprattutto se si fa riferimento a "una notizia proveniente dalla Microsoft" oppure dall'IBM (sono gli hoax più diffusi).

4. Non partecipi a "catene di S. Antonio" o simili

Analogamente, tutti i messaggi che vi invitano a "diffondere la notizia quanto più possibile" sono hoax. Anche se parlano della fame nel mondo, della situazione delle donne negli stati arabi, di una bambina in fin di vita, se promettono guadagni miracolosi o grande fortuna; sono tutti hoax aventi spesso scopi molto simili a quelli dei virus, cioè utilizzare indebitamente le risorse informatiche. Queste attività sono vietate dagli standard di Internet e contribuire alla loro diffusione può portare alla terminazione del proprio accesso.

5. Non utilizzare memorie di massa esterne con dati personali nelle stazioni di lavoro

Non si deve utilizzare memorie di massa contenenti Dati Personali su altro computer aziendale.

OBBLIGO DI RISERVATEZZA E CAUTELA NELLA COMUNICAZIONE A TERZI DI DATI E INFORMAZIONI

Anche informazioni di normale quotidianità aziendale o ritenute non riservate all'interno dell'interscambio tra Persone autorizzate, assumono diversa importanza, e quindi necessitano di una maggiore tutela, se comunicate all'esterno a soggetti terzi. La salvaguardia delle informazioni e dei dati oltre ad essere un requisito fondamentale per la sicurezza del patrimonio informativo aziendale, è anche un espresso obbligo di legge nei confronti di qualsiasi soggetto definito "interessato". A fronte di tali motivazioni è importante ribadire la necessità di osservare ogni cautela nel trasferire all'esterno qualsiasi informazione proporzionalmente al loro contenuto e all'attendibilità dell'interlocutore.

SOCIAL ENGINEERING

Il social engineering è l'insieme delle tecniche psicologiche usate da chi vuole indurci ai propri scopi presentandosi personalmente presso di noi o contattandoci dall'esterno a mezzo telefono o posta elettronica. Gli obiettivi possono andare dalla raccolta di informazioni apparentemente innocue riguardanti l'azienda o la sua organizzazione e il personale che vi lavora, ma possono arrivare a raggiungere dati anche molto riservati.

Con l'ausilio di messaggi studiati o abili tecniche di persuasione l'aggressore può anche renderci complici inconsapevoli di azioni che andranno a suo beneficio come, ad esempio, l'acquisizione di informazioni o l'ottenimento della fiducia del personale, l'apertura di allegati infetti o la visita di un sito che contiene dialer o altro materiale

pericoloso. Rispetto al social engineering via e-mail, uno dei principali problemi degli autori di virus è che molti utenti utilizzano strumenti di difesa aggiornati che non consentono l'esecuzione in automatico di applicativi e quindi non consentono l'attivazione di programmi dannosi. Per scavalcare queste precauzioni e quindi lanciare il virus, c'è un modo molto semplice: indurre la vittima, tramite espedienti psicologici a fidarsi dell'allegato e quindi eseguirlo, o fidarsi del collegamento ad un sito web contenuto nel messaggio e quindi raggiungerlo. In questo senso l'aggressore potrebbe essere capace di sfruttare i nostri punti di debolezza redigendo abili messaggi che, inducendo fiducia o curiosità, riescono ad arrivare allo scopo.

E-MAIL PHISHING

Un altro scopo degli aggressori è indurre l'utente a fidarsi dell'intero contenuto di un messaggio di posta elettronica e quindi ottenere una fedele esecuzione delle istruzioni contenute: ad esempio, vengono inviate false comunicazioni e-mail aventi grafica, forma, autorevolezza e loghi ufficiali di enti noti, banche, intermediari finanziari, assicurazioni, etc., chiedendo informazioni attraverso moduli o link a pagine web debitamente camuffate. In questa modalità vengono richieste ad esempio password, numeri di carta di credito o altre informazioni riservate senza che in realtà la raccolta dati abbia nulla a che vedere con l'organismo ufficiale imitato. La vittima crede di comunicare con essi ma in realtà sta trasmettendo informazioni riservate all'aggressore.

Spesso queste tecniche sono abbinate tra loro e applicate più volte nel tempo sulla stessa vittima.

COSA FARE

- non fornire informazioni confidenziali al telefono o di persona a interlocutori non conosciuti;
- limitatevi a fornire informazioni a interlocutori noti e operanti con voi per disposizione aziendale, nei limiti dei contenuti afferenti all'ambito lavorativo a voi assegnato;
- diffidate di messaggi provenienti da fonte non conosciuta;
- non aprite messaggi provenienti da fonte non conosciuta contenenti allegati;
- non aprite messaggi contenenti allegati sospetti;
- non utilizzare mai link contenuti nel testo del messaggio perché possono essere facilmente falsificati; in questi casi si deve andare direttamente sul sito citato digitandone da capo il nome;
- non trasmettere mai alcuna informazione in risposta ad una richiesta proveniente da fonte sconosciuta;
- non trasmettere mai alcuna informazione in risposta ad una richiesta proveniente da fonti istituzionali o apparentemente conosciute (ad es.: banche) in quanto tali strutture non richiedono mai dati utilizzando questa modalità;
- in caso di dubbio è sempre preferibile verificare l'attendibilità delle richieste con il Responsabile o il Titolare.

PROCEDURE PER IL SALVATAGGIO DEI DATI

L'azienda ha definito procedure automatiche e schedulate di backup giornalieri. Tali backup riguardano i server ed i documenti in essi contenuti.

Qualsiasi documento, progetto, dato deve dunque essere conservato sui server al fine di garantirne un adeguata storicità.

Smarrimento o Furto

In caso di furto o smarrimento di eventuali device il dipendente deve:

- Inviare mail (entro 3h) al responsabile della sicurezza Simone Lucchesi; s.lucchesi@yachtline1618.com e in copia all'ufficio IT itdepartment@yachtline1618.com con OGGETTO: FURTO dispositivo aziendale.
- Il responabile della sicurezza provvederà a recarsi presso il più vicino comando di Forze di Polizia ed effettuare la denuncia di furto o smarrimento all'autorità giudiziaria.
- Qualora sia l'interessato a provvedere dovrà spedire denuncia a s.lucchesi@yachtline1618.com e per conoscenza itdepartment@yachtline1618.com a entro e non oltre 48 ore dall'evento.

Restituzione e distruzione dei device

A seguito di una cessazione del rapporto lavorativo o di consulenza dell'Incaricato con l'Azienda o, comunque, al venir meno, ad insindacabile giudizio dell'Azienda, della permanenza dei presupposti per l'utilizzo dei device aziendali, gli incaricati hanno i seguenti obblighi:

- procedere immediatamente alla restituzione dei device in uso nello stato in cui si trova;
- divieto assoluto di cancellare o formattare o alterare o manomettere o distruggere i device assegnati o rendere inintelligibili i dati in essi contenuti tramite qualsiasi processo, compresa la cifratura dei dati.

Nel caso in cui il collaboratore dimissionario sia in possesso di una SIM aziendale esso può procedere immediatamente alla restituzione oppure richiedere la migrazione del numero.

Nel periodo di preavviso antecedente alla cessazione del rapporto di lavoro l'Azienda può attuare controlli specifici per verificare che non vengano effettuate copie o estrazioni non autorizzate di informazioni riservate.

Ogni Device ed ogni memoria esterna affidati agli incaricati (computer, notebook, tablet, SIM, smartphone, memory card, chiavi usb, hard disk, dvd, cd-rom, ecc.) riconsegnati verranno distrutti o ricondizionati dall'azienda seguendo le norme di legge in vigore al momento della riconsegna. In particolare l'Azienda provvederà a cancellare o a rendere inintelligibili i dati negli stessi memorizzati. Possono essere utilizzate le seguenti procedure:

- Distruzione fisica del supporto.
- Cancellazione Logica (Wiping).
- Smagnetizzazione (Degauss).

Accesso ai dati trattati dall'utente

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 dell'azienda, direttamente a cura della Direzione o dell''Ufficio IT, 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.

Sistemi di controlli graduali

In caso di anomalie, il personale incaricato effettuerà controlli anonimi che si concluderanno con un 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 interessati ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite. Controlli su base individuale potranno essere computi solo in caso di successive ulteriori anomalie

In alcun caso verranno compiuti controlli prolungati, costanti o indiscriminati.

ISTRUZIONI RELATIVE ALLA GESTIONE DI UN DATA BREACH

Definizioni

L'art 4 p.12 del GDPR afferma che per "Violazione di dati" (Data Breach) si intende 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".
Si possono distinguere tre tipi di violazioni:

- **violazione di riservatezza**, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale;
- **violazione di integrità,** ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale;
- **violazione di disponibilità,** ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali;

In generale ogni violazione rispetto della normativa di riferimento in vigore, ovvero quando si configura un'evidente trasgressione delle regole interne o delle normative in vigore.

Cosa fare in caso di incidenti di sicurezza che coinvolgono i dati personali

Qualsiasi Incaricato dovrà comunicare al Titolare del Trattamento dati senza ingiustificato ritardo, e in ogni caso **entro 4 ore dall'avvenuta conoscenza**, ogni violazione della sicurezza che comporti anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura (Data Breach, art. 33 del Regolamento).

Considerando 85: "Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata. Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo".

La comunicazione dovrà essere effettuata all'indirizzo s.lucchesi@yachtline1618.com, privacy@yachtline1618.com e l'Ufficio IT: itdepartment@yachtline1618.com le comunicazioni di Data Breach dovranno descrivere ove possibile:

a) la natura della violazione dei dati, le categorie e il numero approssimativo di interessati coinvolti, nonché le categorie e il numero approssimativo di registrazioni dei dati personali coinvolti;
b) le probabili conseguenze della violazione;
c) le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione o attenuarne gli effetti pregiudizievoli;

Una volta appurato che l'incidente coinvolge dati personali, e che quindi si può configurare una potenziale "violazione di dati personali", il Titolare del Trattamento in collaborazione con l'Ufficio IT coadiuvato da eventuali partner tecnologici esterni svolge un'approfondita analisi, redigendo una relazione tecnica indicante la necessità di inviare:

a) notifica al Garante secondo le modalità e la modulistica messe a disposizione dal Garante, **entro 72 ore** dal momento in cui è venuto a conoscenza della violazione.
b) comunicazione, senza ingiustificato ritardo, ai singoli interessati i cui dati sono coinvolti nella violazione quando la violazione dei dati personali può comportare un rischio elevato per i diritti e le libertà delle persone fisiche.

È importante che sia dimostrabile il momento della scoperta dell'incidente, poiché da quel momento decorrono i tempi previsti per la notifica.
Si invitano pertanto i soggetti incaricati a prestare la massima attenzione al verificarsi di incidenti di sicurezza potenzialmente configurabili come data breach e a rispettare i tempi di comunicazione al Titolare del Trattamento delle violazioni rilevate.

CUSTODIA ED UTILIZZO DEI SUPPORTI RIMUOVIBILI, CONTENENTI DATI PERSONALI

Una particolare attenzione deve essere dedicata ai supporti rimovibili (es. chiavette USB), contenenti dati particolari, nei seguenti termini:

- I supporti rimovibili (es. chiavette USB), contenenti dati particolari devono essere custoditi ed utilizzati in modo tale, da impedire accessi non autorizzati (furti inclusi) e trattamenti non consentiti: è bene adottare archiviazioni in modo che vengano conservati in cassetti chiusi a chiave, durante il loro utilizzo, e successivamente formattati, quando è cessato lo scopo per cui i dati sono stati memorizzati su di essi.
- Una volta cessate le ragioni per la conservazione dei dati, i supporti non possono venire abbandonati. Si devono quindi cancellare i dati, se possibile, o arrivare addirittura a distruggere il supporto, se necessario.

DOVERE DI AGGIORNARSI, UTILIZZANDO IL MATERIALE E GLI STRUMENTI FORNITI DALL'ORGANIZZAZIONE, SULLE MISURE DI SICUREZZA

Pretendere dal titolare che vengano forniti strumenti per la formazione sulla privacy. In particolare relativamente a:

- profili della disciplina sulla protezione dei dati personali, più rilevanti in rapporto alle relative attività, e conseguenti responsabilità che ne derivano;
- rischi che incombono sui dati;
- misure disponibili per prevenire eventi dannosi;
- modalità per aggiornarsi sulle misure minime di sicurezza, adottate dal titolare.

ISTRUZIONI GENERICHE

LA PERSONA AUTORIZZATA DOVRÀ:

procedere alla raccolta di dati personali, nelle modalità previste dalle sue mansioni e indicate in apposita informativa;

consegnare agli interessati, al momento della raccolta dei dati, il modulo contenente l'informativa di cui agli artt. 13-14 del Reg.to UE 2016/679, salvo che l'informativa medesima sia stata fornita direttamente dal titolare o dal responsabile;

raccogliere, sempre al momento della raccolta dei dati, il consenso espresso, documentato per iscritto, degli interessati ai trattamenti previsti, salvo che a ciò abbiano provveduto direttamente il Titolare o il Responsabile, e salvo i casi di esonero previsti dalla stessa legge;

trattare i dati personali nella misura necessaria e sufficiente alle finalità proprie della banca dati nella quale vengono inseriti, secondo quanto espresso nell'informativa e, comunque, in modo lecito e secondo correttezza;

adottare, nel trattamento dei dati, tutte le misure di sicurezza che siano indicate dal Titolare o dal Responsabile, in particolare dovrà:

- per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su terminali altrui e/o di lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
- trattare i soli dati la cui conoscenza sia necessaria e sufficiente per lo svolgimento delle operazioni da effettuare rispettando strettamente il proprio profilo di autorizzazione;
- conservare i supporti informatici e/o cartacei contenenti i dati personali in modo da evitare che detti documenti siano accessibili a persone non autorizzate al trattamento dei dati medesimi;

- con specifico riferimento agli atti e documenti cartacei contenenti dati personali ed alle loro copie, restituire gli stessi al termine delle operazioni affidate;
- utilizzare i supporti di memorizzazione usati solamente qualora i dati in essi precedentemente contenuti non siano in alcun modo recuperabili, altrimenti etichettarli e riporli negli appositi contenitori;
- copie di dati personali su supporti rimuovibili sono permesse solo se parte del trattamento, copie di dati sensibili devono essere espressamente autorizzate dal Responsabile del trattamento o dal Titolare. In ogni caso tali supporti devono avere un'etichetta che li identifichi e non devono mai essere lasciati incustoditi;
- in caso si constati o si sospetti un incidente di sicurezza deve essere data immediata comunicazione al Responsabile del trattamento o al Titolare;
- segnalare al Titolare o al Responsabile eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- effettuare la comunicazione e la diffusione dei dati esclusivamente ai soggetti indicati dal Titolare o dal Responsabile e secondo le modalità stabilite dai medesimi e dichiarate nell'informativa;
- mantenere, salvo quanto precisato al punto precedente, la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento dell'incarico, per tutta la durata del medesimo ed anche successivamente al termine di esso;
- fornire al Titolare o al Responsabile, a semplice richiesta e secondo le modalità indicate da questi, tutte le informazioni relative all'attività svolta, al fine di consentire loro di svolgere efficacemente la propria attività di controllo;
- in generale, prestare la più ampia e completa collaborazione al Titolare ed al Responsabile al fine di compiere tutto quanto sia necessario ed opportuno per il corretto espletamento dell'incarico nel rispetto della normativa vigente.

OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY

È obbligatorio attenersi alle disposizioni in materia di Privacy e di misure minime di sicurezza, come indicate nelle procedure aziendali, nel caso di dipendenti/collaboratori con accesso ai dati personali gestiti dall'Azienda, così come indicato nella lettera di designazione di Incaricato del trattamento dei dati ai sensi del Regolamento Generale Europeo sulla Protezione dei Dati GDPR.

MANCATA OSSERVANZA DELLA NORMATIVA AZIENDALE E PROVVEDIMENTI DISCIPLINARI

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

Il datore di lavoro esercita il potere direttivo ossia detta le regole di comportamento da osservare nell'Azienda per garantire uno svolgimento ordinato ed efficiente dell'attività lavorativa. A tale potere è complementare la facoltà del datore di lavoro di adottare provvedimenti sanzionatori sia nei confronti del dipendente (in riferimento a quanto stabilito dal CCNL) che dei collaboratori esterni (es. recessione dal contratto) in caso di inosservanza delle disposizioni impartite.

Oltre alle ipotesi sopra riportate ricorre anche il provvedimento del licenziamento disciplinare. Per disciplinare si intende il licenziamento intimato per motivi connessi alla condotta del lavoratore, tali da determinare la lesione del vincolo fiduciario esistente con il datore di lavoro. In particolare la condotta del lavoratore può costituire GIUSTA CAUSA o GIUSTIFICATO MOTIVO SOGGETTIVO di licenziamento, ipotesi che si differenziano essenzialmente per l'intensità della lesione e per gli effetti che ne conseguono.

La Giusta Causa (art.2119 c.c.; art.1 L.604/66) si sostanzia in un comportamento talmente grave da non consentire la prosecuzione anche provvisoria del rapporto. Il datore di lavoro può pertanto recedere senza dare il preavviso.

Il licenziamento per Giustificato Motivo Soggettivo (art.3 L. 604/66), determinato da un notevole inadempimento degli obblighi del lavoratore, non è invece così grave da rendere impossibile la prosecuzione del rapporto di lavoro e pertanto il datore di lavoro deve dare il preavviso.

AGGIORNAMENTO E REVISIONE DEL DOCUMENTO

Tutti i dipendenti/collaboratori possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dalla Direzione.

Il presente Regolamento è soggetto a revisione quando si renda necessario aggiornarne i contenuti a seguito di nuove esigenze normative, la versione aggiornata verrà resa disponibile a tutti i dipendenti nell'area condivisa i quali riceveranno un avviso tramite email dell'aggiornamento del regolamento. E' obbligo dell'incaricato prendere visione dell'ultima versione del Regolamento Aziendale a seguito di ogni aggiornamento.

Rev del 31/01/2024