ORDINE
INGEGNERI
CAGLIARI

REGOLAMENTO

PER IL CORRETTO TRATTAMENTO DEI DATI PERSONALI ED ISTRUZIONI ALLE PERSONE AUTORIZZATE AL TRATTAMENTO

Regolamento aziendale per il corretto trattamento dei dati personali ed istruzioni alle persone autorizzate al trattamento

OBIETTIVI DEL DOCUMENTO

Il presente documento fornisce le istruzioni per il corretto trattamento dei dati personali di cui l'OIC - Ordine degli Ingegneri della Provincia di Cagliari è Titolare e si applica al trattamento di dati personali tramite strumenti informatici o supporti cartacei.

Premesso che i comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro, tra ì quali rientrano l'utilìzzo delle risorse informatiche e telematiche, devono sempre ispirarsi al principio di diligenza e correttezza, l'OIC ha adottato il presente Regolamento diretto ad evitare che condotte inconsapevoli possano innescare problemi o minacce alla Sicurezza dei dati o delle attrezzature aziendali e utilizzare in modo conforme la postaelettronica aziendale e la navigazione in internet.

Si raccomanda di prestare la massima attenzione nella lettura delle disposizioni di seguito riportate in quanto il rispetto di tali istruzioni, che potranno essere integrate ed aggiornate, è obbligatorio e l'ìnosservanza delle norme sulla privacy può comportare sanzioni di natura civile e penale.

CAMPO DI APPLICAZIONE

Le presenti Istruzioni si applicano:

- a tutti ì lavoratori dipendenti e a tutti i collaboratori, a prescindere dal rapporto contrattuale con la stessa intrattenuto che si trovino ad operare sui dati personali di cui OIC stessa sia Titolare;

- a tutte le attività o comportamenti comunque connessi al trattamento di dati personali eseguiti tramite strumenti informatici, internet e posta elettronica, e cartacei, mediante strumentazione aziendale o di terze partì autorizzate all'uso dell'infrastruttura aziendale.

NORMATIVA DI RIFERIMENTO

Il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 <<relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE>> (di seguito Pagina 1GDPR), ha imposto la previsione ed il rispetto di requisiti, adempimenti formali e misure di sicurezza volti a garantire la tutela dei diritti dell'interessato. Tale Regolamento, definitivamente vincolante a partire dal 25 maggio 2016, uniforma la normativa in tutti gli Stati Membri e protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.

DEFINIZIONI - ART. 4 DEL GDPR

Dato personale: qualsiasi informazione riguardante una persona fisica identificata 0 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.

Particolari categorie di dati: dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati bìometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orìentamento sessuale della persona (art. 9 del GDPR). Dati genetici: i dati personali relativi alle caratteristiche genetiche eredìtarie o acquisite diuna 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 bìometrici: 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.

Dati personali relativi a condanne penali e reati: dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza (art. 10 del GDPR).

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con 0 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 0 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'utilízzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare 0 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 ì dati personali non possano più essere attribuiti a un interessato specifico senza l'utilìzzo 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, decentralízzato o ripartito in modo funzionale o geografico;

Titolare: 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;

DPO - Data Protection Officer: persona designata dal Titolare o dal Responsabile come centro di competenza per il corretto trattamento dei dati personali.

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio 0 altro organismo che tratti dati personali per conto del titolare del trattamento.

Persone autorizzate al trattamento: le persone fisiche autorizzate, in base a specifiche istruzioni, a compiere operazioni di trattamento dal titolare o dal responsabile. Tali operazioni possono essere effettuate solo da incaricati che operino sotto la diretta autorità del Titolare o del Responsabile, attenendosi alle istruzioni impartite.

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

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.

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 0 del responsabile.

Comunicazione: il dare conoscenza dei dati personali a uno 0 più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione consultazione.

Diffusione: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

Strumenti elettronici: gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

Violazione dei dati personali - Data breach: Violazione di sicurezza che comporti accidentalmente in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Autorità di controllo: l'autorità pubblica indipendente istituita da uno Stato membro.

PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI PERSONALI

Ai sensi dell'art. 5 del GDPR, i dati personali oggetto di trattamento sono: I trattati in modo lecito e secondo correttezza (Liceità, correttezza e trasparenza); I raccolti e registrati unicamente per finalità aziendali o istituzionali, esplicite e legittime, e successivamente trattati in modo tale che il trattamento non sia incompatibile con talifinalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali ("limitazione della finalità");

I adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati ("minimizzazione dei dati"); I esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati ("esattezza");

I conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi

più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica storica a fini statistici, fatta salva l'attuazione di misure tecniche e organizzative adeguate a tutela dei diritti e delle libertà dell'ìnteressato ("limitazione della conservazione"); I trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione 0 dal danno accidentali ("integrità e riservatezza").

LINEE GUIDA GENERALI

Autorizzazione e liceità del trattamento. Di seguito vengono descritte le norme a cui le persone autorizzate al trattamento devono attenersi nell'esecuzione dei compiti che implicano un trattamento di dati personali. Al fine di evitare che soggetti estranei possano venire a conoscenza dei dati personali, la persona autorizzata deve osservare le seguenti regole di ordinaria diligenza, nonché tutte le altre ulteriori misure ritenute necessarie per garantire il rispetto di quanto disposto dalla normativa in ambito privacy:

i dati personali cui è consentito accedere sono quelli la cui conoscenza è strettamente necessaria per adempiere ai compiti affidati, indispensabili per l'esecuzione della prestazione. Ogni variazione ai diritti di accesso al momento detenuti, sarà opportunamente comunicata di volta in volta.

Le persone autorizzate possono effettuare esclusivamente i trattamenti di dati personali definiti in base al ruolo ricoperto e comunicati all'atto della designazione, con la conseguente possibilità di accesso ed utilizzo della documentazione cartacea, degli strumenti informatici, e delle banche dati aziendali che contengono i predetti dati personali.

Non devono essere eseguite operazioni di trattamento per finalità non previste tra i compiti afferenti la propria mansione organizzativa o assegnati dal diretto responsabile; senza la preventiva autorizzazione del Titolare, del Responsabile del trattamento o del Data Protection Officer, non è permesso realizzare nuove ed autonome banche dati contenenti dati personali, secondo criteri organizzativi e/0 per finalità diverse da quelle già previste.

Qualora per esigenze legate alla sua mansione ritenga necessario effettuare un trattamento diverso rispetto a quelli riportati nell'informativa agli interessati, sotto il profilo dei dati trattati, delle finalità, dell'ambito di comunicazione o diffusione, dovrà consultare preventivamente il Titolare del trattamento o il Data Protection Officer al fine di individuare la necessità del trattamento medesimo e degli obblighi conseguenti.

All'atto della raccolta dei dati, il personale autorizzato al trattamento deve fornire all'interessato l'informatìva sul trattamento dei dati personali, avendo cura di raccogliere il suo consenso ove applicabile.

Devono essere svolte le sole operazioni di trattamento necessarie per le finalità per le quali ì dati sono stati raccolti e comunicate agli interessati.

SICUREZZA E RISERVATEZZA

Occorre prestare molta attenzione alla riservatezza delle informazioni scambiate e alla custodia dei dati al fine di garantirne l'integrità, la disponibilità e la riservatezza.

Nessuna informazione riservata, in particolare quelle contenenti dati personali, può essere condivisa con personale non autorizzato, interno o esterno.

Tutte le operazioni di trattamento devono essere effettuate in modo tale da garantire il rispetto delle misure di sicurezza delle informazioni di cui si viene in possesso considerando tutti i dati confidenziali e, di norma, soggetti al segreto d'ufficio;

Il vincolo di riservatezza è valido anche una volta terminato il trattamento dei dati personali.

Operare con la massima attenzione in tutte le fasi di trattamento, dalla esatta acquisizione dei dati, al loro aggiornamento, alla conservazione ed eventuale d'istruzione.

Le singole fasi di lavoro e la condotta da osservare devono consentire di evitare che i dati siano soggetti a rischi di perdita o distruzione, che vi possano accedere persone non autorizzate, che vengano svolte operazioni di trattamento non consentite o non conformi ai fini per i quali i dati stessi sono stati raccolti;

deve essere costantemente verificata l'esattezza dei dati trattati e la pertinenza rispetto alle finalità perseguite nei singoli casi.

Una volta terminato il trattamento (per motivi organizzativi, istituzionali o per conclusione del rapporto di lavoro) tutte le copie non ufficiali generate e i dati salvati o riprodotti sul proprio computer o su qualsiasi altro tipo di supporto magnetico devono essere distrutti.

ISTRUZIONI COMPORTAMENTALI E MISURE DI SICUREZZA

Comunicazione di dati personali e trasmissione di documenti.

I dati personali potranno circolare regolarmente tra tutti i dipendenti che ne abbiano necessità per esigenze di lavoro e che siano già stati autorizzati al trattamento dei dati personali.

Peraltro qualsiasi dato personale a cui Lei ha accesso non potrà essere trasmesso a terzi, se non per finalità aziendali o istituzionali e previa autorizzazione del Titolare o del Responsabile del Trattamento se designato, o del Data Protection Officer.

Circolazione e conservazione di documenti cartacei

Nel caso di accesso e trattamento di dati personali su supporti di tipo cartaceo, la persona autorizzata è tenuta a custodirli con diligenza, non disperderli, e riporli negli appositi contenitori dopo l'uso, avendo cura di chiuderli a chiave. È tenuto a custodirli fino alla restituzione, in modo da evitare l'accesso agli stessi dati da parte di persone prive di autorizzazione.

I In caso di trattamento di dati particolarmente sensibili (condizione di salute, dati giudiziari, ecc.), tutta la documentazione cartacea deve essere conservata in armadi/cassetti chiusi a chiave o stanze chiuse a chiave e le chiavi devono essere custodite con cura. L'accesso a tutti ì locali aziendali deve essere consentito solo a personale preventivamente autorizzato dal Titolare.

Tutto il materiale cartaceo contenente dati personali non deve essere lasciato incustodito sulle scrivanie e, a fine lavoro o durante le pause prolungate, deve essere riposto in un luogo sicuro. Inoltre, occorre usare la medesima perizia nello svolgimento delle normali quotidiane operazioni di lavoro, per evitare che il materiale risulti facilmente visibile a persone terze o, comunque, ai non autorizzati al trattamento.

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

All'interno delle bacheche aziendali potranno essere affissi solamente documenti contenenti dati personali minimi in realzione alle finalità perseguite (no indicazioni di assenza per malattia, indisposizione, permessi particolari inclusi quelli sindacali, anagrafiche e indirizzi di contatto in caso di concorsi, etc).

Telefoni, stampanti, fotocopiatore, fax

In caso di trasmissione o comunicazione di documenti contenenti dati personali necessaria per lo svolgimento dei suoi compiti, al fine di prevenire eventuali accessi ai dati aziendali da parte di soggetti terzi non autorizzati, occorre adottare le seguenti cautele:

Quando le informazioni devono essere trasmesse telefonicamente occorre essere assolutamente certi dell'identità dell'interlocutore e verificare che esso sia legittimato ad ottenere quanto domandato. In particolare, nel caso di richieste da parte di terzi può essere necessario, a seconda della natura dei dati richiesti, procedere nel seguente modo:

- chiedere il nome del chiamante e la motivazione della richiesta;

- richiedere il numero di telefono da cui l'interlocutore sta effettuando la chiamata;

- verificare che il numero dichiarato corrisponda a quello del chiamante;

- procedere immediatamente a richiamare la persona che ha richiesto l'ínformazione, con ciò accertandosí della identità dichiarata in precedenza;

- non lasciare nella memoria della segreteria telefonica messaggi relativi a dati personali.

Quando il dato deve essere inviato a mezzo fax occorre:

- prestare la massima attenzione affinché il numero telefonico o l'indirizzo e-mail immessi siano corretti;

- verificare che non vi siano inceppamenti di carta o che dalla macchina non siano presi più fogli e attendere sempre il rapporto di trasmissione per un ulteriore verifica del numero del destinatario e della quantità di pagine inviate;

- in caso di trasmissione di dati particolarmente delicati è opportuno anticipare l'invìo chiamando il destinatario della comunicazione al fine di assicurare il ricevimento nelle mani del medesimo, evitando che terzi estranei o non autorizzati conoscano il contenuto della documentazione inviata.

Non è consentito effettuare stampe 0 fotocopie di documenti contenenti dati personali se non necessario. Nel caso sia necessario effettuare una stampa, utilizzare apparecchiature collocate in aree controllate. Quando non disponibili, presidiarle in fase di stampa.

Tutti coloro che provvedono alla duplicazione di documenti con stampanti, macchine fotocopiatrici o altre apparecchiature, in caso di copia erronea o non leggibile correttamente, da cui potrebbero essere desunti dati personali, sono tenuti a distruggere il documento mediante apposita macchina "distruggi documenti" o con qualunque altro mezzo che ne renda impossibile la ricostruzione in modo da escludere qualunque possibilità da parte di estranei di venire a conoscenza dei dati medesimi.

Procedere in ogni caso alla cancellazione/distruzione secondo le modalità sopra descritte delle copie di dati appena non siano più necessarie, al fine di evitare la proliferazione incontrollata di archivi contenenti dati personali.

Non lasciare incustoditi i documenti contenenti dati personali nella fotocopiatrice, sul fax, nella stampante.

Attività al computer.

Hanno diritto all'utílizzo degli strumenti e ai relativi accessi solo i dipendenti e collaboratori che per funzioni lavorative ne abbiano un effettivo e concreto bisogno. Il computer in dotazione al dipendente è uno strumento di lavoro e contiene tutti i software necessari a svolgere le attività affidate: come tale deve essere utilizzata solo per scopi legati alla propria attività lavorativa, in modo esclusivo da un solo utente, protetta, evitando che terzi possano accedere ai dati che si stanno trattando.

Ogni utilizzo non inerente all'attívità lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto minacce alla sicurezza. L'utilizzo del computer deve prevedere quindi precisi accorgimenti al fine di impedire accessi alle informazioni da parte di persone non autorizzate.

Nello specifico sono richieste le seguenti misure: non utilizzare risorse informatiche private (PC, periferiche, token, ecc..); non installare alcun software non autorizzato; non lasciare sulla scrivania informazioni riservate su qualunque supporto esse siano archiviate (carta, CD, dischetti, ecc.); non lasciare il computer portatile incustodito sul posto di lavoro (al termine dell'orario lavorativo, durante le pause di lavoro o durante riunioni lontane dalla propria postazione) in caso di allontanamento, anche temporaneo, dalla propria postazione di lavoro si devono porre in essere tutte le misure necessarie assicurandosi della attivazione della funzione Lock Workstation in caso di abbandono momentaneo del proprio PC; non lasciare incustoditi cellulari e palmari; utilizzare solo ed esclusivamente le aree di memoria della Rete ed ivi creare e registrare file e software o archivi dati, senza pertanto creare altri files fuori dalle unità di Rete; mantenere sul computer esclusivamente i dispositivi di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, ecc), autorizzati; spegnere il terminale a fine lavoro o mettere in modalità "Standby"; non rimuovere o aggiungere alcuna apparecchiatura o componente della stazione di lavoro, salvo specifica autorizzazione; non modificare ove tecnicamente fattibile le configurazioni già impostate sul personal computer; non utilizzare programmi e/o sistemi di criptazione senza la preventiva autorizzazione scritta; non installare alcun software di cui non si possieda la licenza, né installare alcuna versione diversa, anche più recente, rispetto alle applicazioni o al sistema operativo presenti sul personal computer consegnato, senza espressa autorizzazione. Né è, peraltro, consentito fare copia del software installato al fine di farne un uso personale; non caricare sul disco fisso del computer alcun documento, gioco, file musicale audiovisivo, immagine diversi da quelli necessari allo svolgimento delle mansioni affidate; non aggiungere collegare dispositivi hardware (ad esempio hard disk, driver, PCMCIA,ecc.) periferiche (telecamere, macchine fotografiche, chiavi USB ecc.) diversi da quelli consegnati, senza espressa autorizzazione; non creare o diffondere, intenzionalmente o per negligenza, programmi idonei a danneggiare il sistema informatico aziendale, quali per esempio virus, trojan horses

ecc.; non accedere, rivelare o utilizzare informazioni non autorizzate o comunque non necessarie per le mansioni svolte; non copiare dati sensibili sulla propria stazione di lavoro, se non previamente autorizzato.

Protezione dei PC portatili e cellulari

Nel caso in cui vengano concessi in uso il computer portatile e il cellulare, il personale autorizzato è responsabile dei dispositivi elettronici assegnatigli e deve custodirli con diligenza sia durante gli spostamenti che durante l'utilìzzo nel luogo di lavoro.

Un computer portatile presenta maggiori vulnerabilità rispetto ad una postazione di lavoro fissa. Fatte salve tutte le disposizioni dei paragrafi precedenti, di seguito vengono illustrate le ulteriori precauzioni da adottare nell'uso dei dispositivi portatili: conservare lo strumento in un luogo sicuro alla fine della giornata lavorativa; non lasciare mai incustodito l'elaboratore in caso di utilizzo in ambito esterno all'azienda; avvertire tempestivamente l'Area IT, che darà le opportune indicazioni, in caso di furto di un PC portatile o di un cellulare; essere sempre ben consapevole delle informazioni archiviate sul portatile o sul cellulare aziendale,

che sono maggiormente soggetti a furto e smarrimento rispetto alla postazione fissa; operare sempre nella massima riservatezza quando si utilizza il PC portatile o il cellulare in pubblico: i dati, ed in particolare le password, potrebbero essere intercettati da osservatori indiscreti.

Al dipendente non è permesso svolgere la sua attività su cellulari, PC fissi o portatili personali.

Utenza e password.

L'accesso all'elaboratore è protetto da password che deve essere custodita dalla persona autorizzata al trattamento con la massima diligenza e non divulgata. In particolare quest'ultima deve gestire la propria utenza d'accesso ai sistemi e la propria password rispettando le seguenti regole:

L'utenza e la password devono essere utilizzate in maniera individuale, strettamente personale e riservata, senza condividerle con altre persone. È vietato permettere ad altri utenti (es. colleghi) di operare con il proprio identificativo utente.

L'utenza è personale ed univoca nel tempo. Deve essere revocata in caso di interruzione del rapporto di lavoro, nel caso in cui venga meno la necessità di accedere al sistema e disattivata in caso di inattività per oltre 6 mesi.

La password rilasciata in maniera provvisoria per permettere di accedere per la prima volta al sistema deve essere modificata immediatamente al primo utilizzo.

Successivamente, ove non sia già imposto da sistema, la password deve essere gestita secondo le seguenti regole:

Deve contenere sia lettere che numeri e almeno un carattere maiuscolo, essere lunga almeno 8 caratteri o, nel caso in cui lo strumento elettronico non lo consenta, un numero di caratteri pari al massimo consentito.

La presenza di un carattere speciale (es. !%&@) aumenta ulteriormente la robustezza della parola chiave.

Deve essere diversa almeno dalle 3 utilizzate in precedenza 0 in numero superiore in funzione della criticità dei sistemi.

Deve essere difficilmente riconducibile all'utente (ad es. non utilizzare il nome, il cognome etc..) e non deve essere ovvia (ad es. non il nome dell'ufficio, dei figli, etc.).

Deve essere conservata, se memorizzata, in luoghi non visibili (ad es. evitare "memo" attaccati al video, al calendario o alla lavagna dell'ufficio, etc.), non ovvi (ad es. nonnell'agenda, nel primo cassetto etc.) e non deve mai essere memorizzata sul proprio PC.

Deve essere cambiata al massimo ogni 6 mesi (3 mesi nell'eventualità di accesso a dati sensibili) ed immediatamente nel caso in cui sorga il minimo dubbio circa la sua conoscenza da parte di altri utenti.

Non deve mai essere comunicata per telefono e tantomeno via posta elettronica, salvo gravi necessità.

Protezione dai virus informatici

I Personal Computer (PC) in dotazione, pur protetti contro gli attacchi dei virus informatici mediante appositi programmi, rimangono potenzialmente esposti ad aggressioni di virus informatici non conosciuti. Alcuni di questi consentono di estrapolare informazioni dal proprio computer (es. utenze e password); per ridurre le probabilità del verificarsi di tali attacchi è necessario che vengano osservate le seguenti regole:

Ove tecnicamente fattibile, non disinstallare né modificare il software antivirus; verificare che il programma antivirus installato sia attivo ed aggiornato, in caso contrario segnalare la necessità di aggiornamento; chiudere correttamente i programmi in uso; non utilizzare CD-Rom o altri supporti elettronici di provenienza incerta e verificare con l'ausilio del programma antivirus in dotazione ogni supporto magnetico contenente dati (floppy disk o CD-Rom), prima dell'esecuzione dei file in esso contenuti; assicurarsi, prima dell'accensione o di un riavvio del sistema operativo, che nessun supporto magnetico (floppy, CD-Rom, ecc.) sia inserito nell'apposìta unità; non operare modifiche alla configurazione degli strumenti informatici in dotazione senza l'autorizzazione del personale preposto. È vietato modificare le caratteristiche impostate sulle dotazioni od installare dispositivi di memorizzazione, comunicazione o altro (ad esempio masterizzatori, modem, wi-fi o connect card), collegare alla rete aziendale qualsiasi apparecchiatura (ad es. switch, hub, apparati di memorizzazione di rete, ecc), effettuare collegamenti verso l'esterno di qualsiasi tipo (ad es. tramite modem connect card ecc.) utilizzando un pc che sia contemporaneamente collegato alla rete aziendale (creando così un collegamento tra la rete aziendale interna e la rete esterna). Non aprire, se si lavora in rete, files sospetti e di dubbia provenienza e non installare applicazioni o software non autorizzato; porre la necessaria attenzione sui risultati delle elaborazioni effettuate e sulle eventuali segnalazioni anomale inviate dal PC e nel caso in cui il sistema rilevi la presenza di un virus sulla stazione di lavoro contattare immediatamente il personale di competenza. Backup.

I dati inseriti nei sistemi devono essere salvati con frequenza al più settimanale o comunque commisurata alla frequenza di aggiornamento degli stessi.

Avvalersi del salvataggio centralizzato in tutti i casi in cui è garantito nel caso in cui si renda necessario provvisoriamente lavorare sul proprio disco fisso, provvedere al salvataggio dei dati con frequenza commisurata alla loro frequenza di aggiornamento.

In ogni caso deve essere garantito il recupero dei dati in caso di guasto (es. rottura del disco locale).

I comunicare all'amminístratore di sistema ogni esigenza relativa al salvataggio dei propri dati di lavoro.

Utilizzo di Internet.

Gli strumenti di comunicazione telematica (Internet e Posta elettronica) devono essereutilizzati solo ed esclusivamente per finalità lavorative, consapevoli del fatto che si tratti di veicoli per l'introduzione sulla propria macchina (e quindi in azienda) di potenziali virus e altri elementi dannosi.

Sono vietati comportamenti che possano arrecare danno all'organizzazione. La navigazione deve essere effettuata in modo etico e solo al fine di migliorare la propria produttività. In particolare, è necessario osservare le seguenti regole:

È consentita la navigazione internet solo in siti attinenti e necessari per lo svolgimento delle mansioni assegnate.

È fatto divieto di accedere a siti internet che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico, rilevante ai fini della realizzazione di una fattispecie di reato o che siano in qualche modo dìscriminatori sulla base della razza, dell'orìgine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, degli handicap.

È consentito solo l'utilìzzo dei programmi ufficialmente installati dall'Area IT, mentre è assolutamente vietato sia scaricare software gratuiti (freeware o shareware) prelevati da siti Internet che installare autonomamente programmi, per ovviare al grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle

applicazioni software esistenti e/o di violare la legge sul diritto d'autore, non disponendo delle apposite licenze d'uso acquistate dall'Azienda.

È vietata ogni forma di registrazione a siti in nome del Titolare, la partecipazione a Forum non professionali, l'utilìzzo di chat line, di bacheche elettroniche i cui contenuti non siano legati all'attívità lavorativa.

Non è consentito l'utilìzzo funzioni di instant messaging a meno che non siano state autorizzate dall'Area IT.

Salva esplicita autorizzazione in tal senso, è vietata la comunicazione di dati personali attraverso l'uso di telefoni cellulari, smatphone, tablet e pc personali. È vietata la diffusione sui social network di immagini del luogo nel quale si svolge l'attività lavorativa o di informazioni riguardanti il Titolare e il personale (es. colleghi).

È vietata la memorizzazione di documenti informatici di natura oltraggiosa, diffamatoria e/o discriminatoría per sesso, lingua, religione, razza, origine etnica, opinione e appartenenza sindacale e/o politica.

È vietato al lavoratore di promuovere utile o guadagno personale attraverso l'uso di

Internet o della posta elettronica aziendale. È vietato creare siti web personali sul sistemi aziendali nonché acquistare beni o servizi su Internet a meno che l'articolo acquistato non sia stato approvato a titolo di spesa professionale. È vietato accedere ad alcuni siti internet mediante azione ínibenti dei filtri, sabotando comunque superando o tentando di superare o disabilitando, ove tecnicamente fattibile, i sistemi adottati per bloccare accessi non conformi all'attívità lavorativa. In ogni caso è vietato utilizzare siti o altri strumenti che realizzino tale fine. Le persone autorizzate al trattamento sono tenute al rispetto della regolamentazione del copyright (es. legge 22 aprile 1941, n. 633 e successive modificazioni, d.lgs. 6 maggio 1999, n. 169 e legge 18 agosto 2000, n. 248) anche per i programmi freeware e shareware scaricati dalla rete; ciò deve valere anche per lo scarico di materiale mediatico (es. immagini, mp3, ...).

Non devono essere messi a disposizione materiali a carattere inappropriato od offensivo, cui comunque vietato accedervi. Non devono essere messe a disposizione di terzi informazioni a carattere riservato o

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

Posta elettronica.

La posta elettronica è uno strumento a disposizione per l'attività lavorativa e deve essere utilizzato nel rispetto dell'etica e dell'immagine del Titolare. La posta elettronica e qualsiasi altro strumento di connessione telematica deve essere utilizzato nel rispetto delle norme civili e penali vigenti e per scopi compatibili con le attività aziendali.

Alle persone autorizzate al trattamento viene assegnato un indirizzo nominativo di posta elettronica salvo specifiche e determinate eccezioni (indirizzi istituzionali). Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

Prestare attenzione ai messaggi di posta elettronica ed ai file, programmi e oggetti allegati, ricevuti da mittenti sconosciuti, con testo del messaggio non comprensibile o comunque avulso dal proprio contesto lavorativo. In tali casi le persone autorizzate al trattamento devono in particolare:

- visualizzare preventivamente il contenuto tramite utilizzo della funzione "Riquadro di lettura" (o preview) e, nel caso si riscontri un contenuto sospetto, non aprire il messaggio,

- una volta aperto il messaggio, evitare di aprire gli allegati 0 cliccare sui "link" eventualmente presenti,

- cancellare il messaggio e svuotare il "cestino" della posta,

- segnalare l'accaduto all'Amministratore di Sistema.

Non è consentito rispondere a messaggi provenienti da un mittente sconosciuto o di dubbio contenuto in quanto tale atto assicura al mittente l'esistenza del destinatario.

Evitare di cliccare sui collegamenti ipertestuali dubbi presenti nei messaggi di posta: in caso di necessità, accedere ai siti segnalati digitando il nome del sito da visitare direttamente nella barra degli indirizzi nei consueti strumenti di navigazione.

Al fine di ottimizzare le risorse a disposizione della posta elettronica aziendale e migliorare le prestazioni del sistema si evidenzia che la casella di posta deve essere “tenuta in ordine” cancellando periodicamente o comunque se sono superati i limiti di spazio concessi, documenti inutili o allegati ingombranti.

Particolari cautele nella predisposizione dei messaggi di posta elettronica.

Nell'utìlizzo della posta elettronica ogni persona autorizzata al trattamento deve tenere in debito conto che i soggetti esterni possono attribuire carattere istituzionale alla corrispondenza ricevuta da dipendenti aziendali. Pertanto si deve prestare particolare attenzione agli eventuali impegni contrattuali e precontrattuali contenuti nei messaggi e rispettare le seguenti prescrizioni in proposito:

È vietato l'utilìzzo della posta elettronica per comunicare informazioni riservate, dati personali dati critici, senza garantirne l'opportuna protezione.

Occorre sempre accertarsi che i destinatari della corrispondenza per posta elettronica siano autorizzati ad entrare in possesso dei dati che ci si appresta ad inviare.

In caso di errore nella spedizione o ricezione, contattare rispettivamente il destinatario cui è stata trasmessa per errore la comunicazione o il mittente che, per errore, l'ha spedita, eliminando quanto ricevuto (compresi allegati) senza effettuare copia.

Utilizzare il seguente disclaimer:

«Il presente messaggio e gli eventuali allegati sono di natura aziendale e prevalentemente confidenziale: qualora vi fosse pervenuto per errore, vi preghiamo di cancellarlo dal vostro sistema. La risposta o l'eventuale invio spontaneo da parte vostra di e-mail al nostro indirizzo potrebbero non assicurare

la confidenzialità potendo essere viste da soggetti appartenenti alla nostra Organizzazione per finalità di sicurezza informatica, amministrative e allo scopo del continuo svolgimento del/'attività aziendale”.

La formulazione dei messaggi deve prevedere l'uso di un linguaggio appropriato, corretto e rispettoso, che tuteli la dignità delle persone, l'immagine e la reputazione dell'Azienda.

Devono essere conservate le comunicazioni inviate o ricevute, in particolare quelle dalle quali si possano desumere impegni e/o indicazioni operative provenienti dalla Committenza pubblica.

È vietato utilizzare l'indirizzo di posta elettronica contenente il dominio aziendale per iscriversi in qualsivoglia sito per motivi non attinenti all'attívità lavorativa, senza espressa autorizzazione scritta del Titolare nonché utilizzare il dominio aziendale per scopi personali.

In caso di iscrizione a servizi informativi accessibili via internet ovvero a servizi di editoria on line necessari per lo svolgimento dell'attività professionale, veicolati attraverso lo strumento di posta elettronica:

- adoperare estrema cautela ed essere selettivi nella scelta della società che fornisce il servizio (in particolare, l'adesione dovrà avvenire in funzione dell'attinenza del servizio con la propria attività lavorativa);

- utilizzare il servizio solo per acquisire informazioni inerenti finalità aziendali, facendo attenzione alle informazioni fornite a terzi in modo da prevenire attacchi di social engineering.

Evitare di predisporre messaggi che contengano materiali in violazione della legge sul diritto d'autore, o altri diritti di proprietà intellettuale o industriale.

Non è permesso lo scambio di messaggi in conflitto con l'etica professionale con gli interessi aziendali.

È vietato creare, archiviare o spedire, anche solo all'interno della rete aziendale, messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) non connessi con lo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto, catene di Sant'Antonio in genere a pubblici dibattiti utilizzando l'indirizzo aziendale.

È vietato utilizzare il servizio di posta elettronica per trasmettere a soggetti esterni all'azíenda informazioni riservate o comunque documenti aziendali, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte. È vietato inviare messaggi di posta elettronica, anche all'ìnterno della rete aziendale, che abbiano contenuti contrari a norme di legge ed a norme di tutela dell'ordine pubblico, rilevanti ai fini della realizzazione di una fattispecie di reato, o che siano in qualche modo dìscriminatori della razza, dell'orìgine etnica, del colore della pelle, della fede religiosa, dell'età, del sesso, della cittadinanza, dello stato civile, dello stato di salute. Qualora il dipendente riceva messaggi aventi tale contenuto, è tenuto a cancellarli immediatamente e a darne comunicazione alla Direzione. Il collaboratore ha l'obbligo di attivare il servizio di risposta automatica (Auto-reply), in caso di assenze programmate e non programmata. In tale ultimo caso qualora il collaboratore non possa attivare il servizio ha l'obbligo di segnalarne la necessità.

Accesso ordinario ai dati da parte dell'Amministratore di Sistema.

L'Amministratore di Sistema può accedere ai dati trattati tramite posta elettronica onavigazione in rete esclusivamente per motivi di sicurezza e protezione del sistema informatico (ad es., contrasto virus, malware, intrusioni telematiche, fenomeni quali spamming, phishing, spyware, etc.), ovvero per motivi tecnici e/o manutentivì e/o di regolare svolgimento dell'attività lavorativa (ad esempio aggiornamento/sostituzione/ìmplementazione di programmi, manutenzione hardware).

Fatta eccezione per gli interventi urgenti che si rendano necessari per affrontare situazioni di emergenza e massima sicurezza, il personale incaricato accederà ai dati su richiesta della persona autorizzata al trattamento e/o previo avviso al medesimo. Ove sia necessario per garantire la sicurezza, l'assistenza tecnica e la normale attività operativa, l'amministratore avrà anche la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni previo avviso al personale. Lo stesso Amministratore di Sistema può, nei casi suindicati, procedere a tutte le operazioni di configurazione e gestione necessarie a garantire la corretta funzionalità del sistema informatico aziendale (ad es. rimozione di file o applicazioni pericolosi).

L'Amministratore di Sistema, in caso di assenza improvvisa o prolungata del dipendente comunque non programmata e per improrogabili necessità di sicurezza o di operatività del sistema è abilitato ad accedere alla sua posta elettronica per le strette necessità operative. Di tale avvenuto accesso dovrà comunque essere data tempestiva comunicazione.

L'Amministratore di Sistema è altresì abilitato ad accedere ai dati contenuti negli strumenti informatici restituiti dal dipendente 0 collaboratore all'azíenda per cessazione del rapporto, sostituzione delle apparecchiature, etc.

Sarà cura dell'utente la cancellazione preventiva di tutti gli eventuali dati personali eventualmente ivi contenuti.

Modalità di controllo e verifica.

Il Titolare promuove ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri e, comunque, a minimizzare l'uso di dati riferibili ai lavoratori e allo scopo può adottare ogni possibile strumento tecnico, organizzativo e fisico, volto a tutela la sicurezza dei dati e prevenire trattamenti illeciti sui dati trattati con strumenti informatici.

Il Titolare garantisce la non effettuazione di alcun trattamento mediante sistemi hardware e software specificatamente preordinati al controllo a distanza, quali, a titolo esemplificativo:

lettura e registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori (log) al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;

I riproduzione ed eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;

I lettura e registrazione dei caratteri inseriti tramite la tastiera 0 analogo dispositivo.

Ogni eccezione è esplicitata all'ìnterno dell'Informativa nella quale sono esplicitate le eventuali finalità e modalità di trattamento.

Conformemente ai principi di pertinenza e non eccedenza, le verifiche sugli strumenti informatici saranno realizzati nel pieno rispetto dei diritti e delle libertà fondamentali delle persone autorizzate e del presente Regolamento.In generale i sistemi software sono programmati e configurati in modo da cancellare periodicamente ed automaticamente (eventualmente con l'intervento tecnico) i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

Un eventuale prolungamento dei tempi di conservazione viene valutato come eccezionale e deve aver luogo solo in relazione:

o ad esigenze tecniche o di sicurezza del tutto particolari; all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria; o all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria.

L'Amministratore di Sistema può procedere a controlli sulla navigazione finalizzati a garantire l'operatívità e la sicurezza del sistema, nonché il necessario svolgimento delle attività lavorative, es. mediante un sistema di controllo dei contenuti (Proxy server) o mediante "file di log" della navigazione svolta.

L'eventuale controllo sui file di log da parte dell'Amministratore di Sistema non è comunque continuativo ed è limitato ad alcune informazioni (es. Posta elettronica: l'indirizzo del mittente e del destinatario, la data e l'ora dell'invio e della ricezione e l'oggetto -Navigazione internet: il nome dell'utente, l'identificativo della postazione di lavoro, indirizzo IP, la data e ora di navigazione, il sito visitato e il totale degli accessi effettuati) ed i file stessi vengono conservati per il periodo strettamente necessario per il perseguimento delle finalità organizzative, produttive e di sicurezza dell'azienda, e comunque non oltre 12 mesi, fatti salvi in ogni caso specifici obblighi di legge.

L'eventuale sistema di registrazione dei log viene configurato in modo cancellare periodicamente ed automaticamente (attraverso procedure di sovraregistrazione) i dati personali degli utenti relativi agli accessi internet e al traffico telematico.

In caso di anomalie il Titolare, per quanto possibile, privilegerà preliminari controlli anonimi e quindi riferiti a dati aggregati nell'ambito di intere strutture lavorative o di sue aree nelle quali si è verificata l'anomalia.

Qualora nell'ambito di tali verifiche si dovesse rilevare un evento dannoso, una situazione di pericolo o qualche altra modalità non conforme all'attívità lavorativa (es. scarico di files pirata, navigazioni da cui sia derivato il download di virus informatici, ecc.) si effettuerà: o un avviso al Responsabile della struttura dell'Area aziendale interessata in cui è stato rilevato l'utilìzzo anomalo degli strumenti aziendali affinché lo stesso inviti le strutture da lui dipendenti ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite; o in caso di successive, perduranti anomalie, ovvero ravvisandone comunque la necessità, la società si riserva di effettuare verifiche anche su base individuale, comunque finalizzate esclusivamente alla individuazione di eventuali condotte illecite.

In nessun caso verranno realizzate verifiche prolungate, costanti 0 indiscriminate, fatte salve le verifiche atte a tutelare gli interessi aziendali.

Violazione dei dati personali - Data Breach

Nel caso in cui la persona autorizzata al trattamento venga a conoscenza di una violazione dei dati personali (data breach), deve provvedere ad informare senza ritardo il Titolare o il Responsabile della protezione dei dati affinché possano notificare la violazione all'autorità di controllo competente, secondo quanto previsto dall'articolo 33 del GDPR.

Responsabilità, provvedimenti disciplinari e sanzioni.

Le persone autorizzate al trattamento, i dipendenti e i collaboratori, al fine di non esporre se stessi e il Titolare a rischi sanzionatori, sono tenuti ad adottare comportamenti puntualmente conformi alla normativa vigente ed alla regolamentazione aziendale. In caso contrario, saranno ritenuti responsabili degli eventuali danni cagionati agli interessati del trattamento, al patrimonio e alla reputazione del Titolare.

Sono pertanto tenuti ad osservare e a far osservare le disposizioni contenute nel presente Regolamento, il cui mancato rispetto o la cui violazione, costituendo inadempimento contrattuale potrà comportare:

- per il personale dipendente oltre che l'adozione di provvedimenti di natura disciplinare previsti dal Contratto Collettivo Nazionale di Lavoro vigente, le azioni civili e penali stabilite dalle leggi vigenti;

- per i collaboratori esterni oltre che la risoluzione del contratto le azioni civili e penali stabilite dalle leggi vigenti.

Esercizio dei diritti dell'interessato.

Il personale interessato al trattamento dei dati può esercitare i propri diritti ai sensi degli articoli dal 15 al 22 del GDPR rivolgendosi al Titolare del trattamento o al Responsabile della protezione dei dati.