DPOSERVICE

by EPS Enterprise Process Solutions srl

ORDINE DEI FARMACISTI DELLA PROVINCIA DI ORISTANO

Ente di Diritto Pubblico non Economico

Codice Fiscale 80004570950

Regolamento interno

in applicazione del

Regolamento Generale sulla Protezione dei Dati personali

(Regolamento UE 679/2016 - di seguito indicato “RGPD”),

del Codice in materia di protezione dei dati personali 196/03 modificato dal decreto 101 del 2018

e successive modifiche, integrazioni.

Presidente e Legale Rappresentante dell’Ordine	Picciau Gianfranco
Referente per il trattamento dei dati	Melis Deborah
Responsabile della protezione dei dati (DPO)	E.P.S. Enterprise Process Solutions s.r.l. nella persona di Paolo Augusto Leveghi

Adottato nella seduta di Consiglio del 27/04/2022

Piazza Sant’Ambrogio 8, 20123 MILANO - P. IVA 04772390961 - Tel. 02 4003 1996 email: dposervice@eps-italia.com

DPOSERVICE

by EPS Enterprise Process Solutions srl

Versione Documento	2.0	Data Versione	10/03/2022
Descrizione modifiche	Aggiornamento 2022		
Motivazioni	Chiarimento ed aggiornamento		

Redatto da:	Paolo Augusto Leveghi
Validato da:	Consiglio Direttivo
Approvato da:	Consiglio Direttivo nella seduta del 27/04/2022
Conservato presso:	Ordine dei Farmacisti della Provincia di Oristano
Tipologia di documento:	Regolamento
Destinatari/Utilizzatori	Interna all'ente

L'utilizzo del presente documento è riservato

agli Ordini dei Farmacisti aderenti al servizio GDPR+DPO di STUDIOFARMA

Piazza Sant'Ambrogio 8, 20123 MILANO - P. IVA 04772390961 - Tel. 02 4003 1996 email: dposervice@eps-italia.com

Sommario

Finalità

Le presenti norme rappresentano uno strumento di sensibilizzazione, informazione e formazione di tutto il personale interno e dei collaboratori che trattano dati personali per conto del Titolare dei dati. Per estensione è applicabile alle persone ed alle aziende che trattano dati per conto del Titolare dei dati come Responsabili del Trattamento.

Il documento è stato redatto allo scopo di:

- definire comportamenti corretti, in linea con le disposizioni dell'Ordine
- rendere consapevoli coloro che operano in nome e per conto dell'Ordine di poter provocare, anche involontariamente, un illecito passibile di sanzioni rilevanti;
- confermare che l'Ordine non tollera comportamenti illeciti, di qualsiasi tipo, anche se la stessa fosse in condizione di trarne vantaggio;
- prevenire rischi, assicurare i diritti degli interessati e rispettare la normativa in argomento.

Tutto il personale interno ed i collaboratori esterni che trattano dati personali nello svolgimento delle attività di competenza sono tenuti a rispettare scrupolosamente le norme.

Il mancato rispetto o la violazione delle disposizioni in materia potranno essere perseguiti con provvedimenti disciplinari nonché con azioni civili e penali previste dalla normativa vigente.

Entrata in vigore, aggiornamento e revisione

Le presenti norme modificano e sostituiscono le precedenti comunicazioni/disposizioni in materia.

Il testo va consegnato a tutto il personale interno e dei collaboratori che trattano dati personali e resta a disposizione del personale nell'archivio dell'Ordine.

Si invita tutto il personale, dopo un'attenta lettura a restituire la scheda riportata sull'ultima pagina debitamente compilata e sottoscritta.

Il presente documento è soggetto ad aggiornamento e revisione periodica, ogni incaricato può suggerire al responsabile della protezione dei dati dell'Ordine modifiche o integrazioni al presente testo.

Definizioni

Ai fini del presente documento valgono le stesse definizioni previste nell'art 4 della normativa in argomento. Più in particolare s'intende per:

DATO PERSONALE: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

TRATTAMENTO: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

LIMITAZIONE DI TRATTAMENTO»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

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

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

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

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

RESPONSABILE DEL TRATTAMENTO»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento

RESPONSABILE INTERNO: Persona delegata dal Titolare alla gestione dei Trattamenti dati personali con delibera del Consiglio dell'Ordine. Ha autonomia gestionale e risponde al Titolare stesso.

INCARICATO: Persona delegata dal Titolare alla gestione dei Trattamenti dati personali con delibera del Consiglio dell'Ordine. Non ha autonomia gestionale e risponde al Titolare ed al Responsabile interno dei trattamenti.

RESPONSABILE ESTERNO: persona fisica o giuridica che svolge il trattamento dei dati del Titolare con parziale autonomia.

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;

INTERESSATO: la persona fisica cui si riferiscono i dati;

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

VIOLAZIONE DEI DATI PERSONALI: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

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;

CREDENZIALI DI AUTENTICAZIONE: i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;

PAROLA CHIAVE: componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica

PROFILO DI AUTENTIFICAZIONE: l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;

SISTEMA DI AUTENTIFICAZIONE: l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

Disposizioni Generali Per Il Trattamento Dei Dati Personali

Il personale incaricato del trattamento di dati personali riceve istruzioni dal Titolare, adeguata formazione con manuali operativi e regolamenti/disposizioni aziendali.

I dati personali devono essere:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che il trattamento non sia incompatibile con tali finalità;

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

d) 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»));

e) 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.

f) trattati in maniera da garantire un'adeguata sicurezza mediante misure tecniche e organizzative appropriate. («integrità, disponibilità e riservatezza»).

Per la gestione dei dati deve sussistere prima dell'inizio di ogni trattamento la presenza di almeno **una delle seguenti condizioni**:

a) l'interessato ha espresso il consenso al trattamento;

b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di attività precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

Il personale nell'espletamento del proprio lavoro deve:

- osservare il più rigoroso segreto d'ufficio;
- garantire la stretta osservanza dell'incarico ricevuto, escludendo qualsiasi trattamento o utilizzo dei dati non coerente con le disposizioni ricevute;
- non comunicare ad altri e non portare all'esterno dell'ambiente di lavoro documenti e/o supporti magnetici contenenti dati, se non in presenza di una specifica autorizzazione del Titolare o del Responsabile Interno dell'Ordine;

- raccogliere dati personali solo dopo aver fornito all'interessato adeguata informativa per i trattamenti eseguiti e ove ne ricorrano gli obblighi, aver ottenuto dallo stesso adeguato consenso al trattamento.

Chiunque dovesse ricevere una richiesta scritta da un interessato, che intende far valere i propri diritti relativamente al trattamento dei dati che lo riguardano, previsti dagli artt. 15-21 del RGPD (ad esempio: conferma di quanto eseguito, richiesta di rettifica, cancellazione, opposizione e/o limitazione del trattamento), **deve informare tempestivamente il Titolare od il Responsabile Interno dei Trattamenti**, che provvederà se del caso, a coinvolgere il Consiglio ed il Responsabile della protezione dei dati (c.d. DPO) dell'Ordine**.**

Politiche generali per l'utilizzo di dispositivi e strumenti informatici

Titolarità, autorizzazione e finalità di utilizzo dei dispositivi e degli strumenti informatici

L'Ordine è proprietario dei dispositivi e degli strumenti informatici che vengono messi a disposizione del personale ai fini dell'esecuzione dell'attività lavorativa nonché di tutte le informazioni, le registrazioni ed i dati inerenti all'esercizio della propria attività che siano contenuti e/o trattati mediante utilizzo di tecnologie informatiche.

Ad ogni dipendente e/o collaboratore (da qui in poi denominato anche UTENTE) può essere assegnato uno o più dispositivi e strumenti informatici (personal computer, laptop, palmare, cellulare, etc.), tramite cui è possibile accedere ad una serie di risorse che possono essere fisicamente ubicate all'interno dei locali dell'Ordine o all'esterno della stessa.

L'autorizzazione all'utilizzo dei dispositivi e degli strumenti informatici, quali a titolo esemplificativo e non esaustivo l'accesso alle risorse della rete dell'Ordine, alla posta elettronica e ad Internet, concessa al dipendente al momento dell'assunzione o all'inizio del rapporto con il collaboratore, può essere revocata in qualsiasi momento da parte dell'Ordine.

L'utilizzo degli strumenti e delle risorse informative dell'Ordine deve essere strettamente vincolato all'esercizio delle attività lavorative, rispettando le normative interne e in ottemperanza alle disposizioni legislative vigenti. È proibito l'impiego delle risorse dell'Ordine per scopi personali o di terzi.

In particolare, si fa divieto esplicito di:

- Utilizzare le risorse per profitto personale;
- Impiegare le risorse per finalità diverse da quelle per le quali sono state progettate o utilizzare i sistemi informativi per compiere azioni illecite nei confronti di altri sistemi, sia interni che esterni, all'organizzazione;
- Recare volontariamente danni alle risorse dell'Ordine, ai sistemi informatici di pubblica utilità, agli strumenti di supporto, ai locali ed in generale ai dispositivi informatici utilizzati dall'organizzazione.

Ogni strumento o risorsa, concessa ai fini esclusivamente lavorativi, deve essere correttamente custodito e mantenuto in buono stato dall'utente che deve contribuire, in rapporto alle proprie responsabilità, alla protezione del patrimonio dell'Ordine.

Postazioni di lavoro

La Postazione di Lavoro (di seguito postazione) è costituita dall'insieme di componenti hardware e software forniti all'utente o di proprietà dell'utente ed autorizzate dal rispettivo ente; essa consente l'accesso al complesso dei sistemi e servizi resi disponibili.

L'utente è consapevole e accetta di restituire la totalità delle risorse utilizzate nel momento in cui cessa il rapporto con ciascun ente. Ogni utente, di norma, è assegnatario o autorizzato all'uso di una sola postazione, fissa o mobile; è responsabile della medesima e deve custodirla con diligenza (sia all'interno dell'edificio dell'Ordine, sia al di fuori), nonché segnalare eventuali furti, danneggiamenti o smarrimenti.

Inoltre, è tenuto a prestare la massima collaborazione sia alle attività di censimento ed inventario delle risorse hardware e software, sia alle attività di aggiornamento di tali risorse.

Utilizzo del Personal Computer

Il Personal Computer (PC) installato presso la Postazione di Lavoro o fornito all'Utente è configurato in modo ottimale, tenuto conto delle necessità professionali e lavorative.

Il PC affidato al dipendente o collaboratore è uno strumento di lavoro; non ne è pertanto consentita l'utilizzazione non inerente all'attività lavorativa. A tale scopo l'utente potrà utilizzare le risorse disponibili sul proprio PC e dovrà salvare, se necessario, ogni appunto creato sulla memoria di massa del PC stesso (disco locale).

Il PC deve essere custodito con cura evitando ogni possibile forma di uso non autorizzato o di danneggiamento.

Il PC che viene consegnato all'Utente contiene tutti i software necessari a svolgere gli incarichi affidati. Alla cessazione del rapporto intercorso con l'utente, il Personal Computer dovrà essere restituito nella sua interezza, comprese eventuali periferiche interne ed esterne.

Non è consentito l'uso di programmi diversi da quelli ufficialmente installati dalla società, né viene consentito agli utenti di installare autonomamente programmi di qualsivoglia natura, sussistendo infatti il grave pericolo di introdurre Virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione espone l'Ordine a gravi responsabilità civili; si evidenzia, inoltre, che le violazioni della normativa a tutela dei diritti d'autore sul software che impone la presenza nel sistema di software regolarmente licenziato, o comunque libero e quindi non protetto dal diritto d'autore vengono sanzionate anche penalmente.

Salvo preventiva espressa autorizzazione dell'Ordine, non è consentito all'Utente modificare le caratteristiche impostate sul proprio PC, né procedere ad installare dispositivi di memorizzazione, comunicazione o altro, come ad esempio masterizzatori, modem, ecc.

In ogni caso, all'utente non è consentito:

- modificare le configurazioni già impostate sul PC consegnato;
- modificare impostazioni di sistema che abbiano un impatto sulla sicurezza o la funzionalità del sistema;
- impedire in qualsiasi modo (personal firewall, cambio di diritti di accesso, rimozione delle condivisioni di sistema, ecc.) l'accesso al software installato sul proprio PC e ai documenti ivi registrati;
- utilizzare programmi e/o sistemi di crittografia senza la preventiva autorizzazione scritta dell'Ordine;
- installare alcun software né alcuna versione diversa, anche più recente, rispetto alle applicazioni o al sistema operativo presenti sul PC consegnato, senza l'espressa autorizzazione dell'Ordine;
- fare copia del software installato al fine di farne un uso personale;

- fare copia dei documenti dell'Ordine in modo diverso dalla copia di back-up prevista dalle procedure interne;
- caricare alcun documento, file musicale o audiovisivo o immagine diversi da quelli necessari allo svolgimento delle mansioni affidate;
- aggiungere o collegare dispositivi hardware (hard disk, drive, PMC, USB, seriale, firewall ecc.) o periferiche (telecamere, macchine fotografiche ecc.) diversi da quelli consegnati, senza l'autorizzazione espressa dell'Ordine;
- creare o diffondere programmi idonei a danneggiare il sistema informatico dell'Ordine, quali per esempio virus, trojan horses, ecc.;
- impostare connessioni private ad Internet o ad altre reti, ovvero connessioni private di comunicazione verso dispositivi mobili (telefoni cellulari e palmari) (ad es. Bluetooth);
- rimuovere la protezione automatica all'accesso al PC, ovvero lo screensaver a tempo (max 10 minuti);
- utilizzare il PC per scopi privati e comunque non inerenti all'attività lavorativa, salvo quanto specificato riguardo le modalità di utilizzo di Internet e della posta elettronica di seguito riportate

Al fine di ridurre al minimo i rischi sopra evidenziati, non vengono concessi diritti di Amministratore del sistema operativo e, in caso di necessità, possono essere automaticamente forzate alcune impostazioni di sicurezza (ad esempio lo screensaver con password).

I dischi fissi locali del PC sono gestiti sotto la responsabilità dell'utente che deve preoccuparsi di salvare, cancellare e proteggere le informazioni ivi presenti. Al momento della cessazione del rapporto di lavoro, non è consentito effettuare copie dei dati presenti nel PC.

Ogni utente è tenuto ad operare, con la necessaria diligenza, la custodia dei dati salvati sul proprio PC e non in rete. Considerato che i dati potrebbero accidentalmente essere perduti o danneggiati, l'utente deve valutare se conservare copia dei files presenti registrati sul disco fisso del proprio PC. Se l'eventuale copia fosse effettuata su supporti informatici (dispositivi USB, CD-ROM, DVD, Memory Card, Cellulari ecc.) gli stessi dovranno essere custoditi in modo adeguato al tipo di informazioni contenute e dovranno essere distrutti o cancellati quando le suddette informazioni non saranno più utili.

Nell'utilizzo della postazione di lavoro è opportuno non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

È opportuno terminare la sessione di lavoro svolta tramite utilizzo di un personal computer, ogni volta che ci si deve allontanare, anche solo per un breve periodo, effettuando il "log out" dell'account utente o mettendo in atto accorgimenti tali per cui il PC non resti:

- incustodito: può essere sufficiente, a titolo esemplificativo, che un collega rimanga nella stanza durante l'assenza di chi sta utilizzando il PC anche se la stanza rimane aperta;
- accessibile: può essere sufficiente chiudere a chiave la stanza all'interno della quale è situato lo strumento elettronico.

Non devono mai verificarsi situazioni in cui un Personal Computer venga lasciato attivo, durante una sessione di trattamento, senza che sia controllato da un incaricato al trattamento o senza che la stanza in cui è ubicato venga chiusa a chiave.

È possibile predisporre strumenti software specifici (es.: screen saver) che, trascorso un breve periodo di tempo predeterminato in cui l'elaboratore resta inutilizzato, non consente più l'accesso all'elaboratore se non previo inserimento di credenziali di accesso (es.: password, ecc.).

L'utente è tenuto a dare tempestiva segnalazione ai referenti IT di eventuali anomalie o irregolarità nel funzionamento del PC, al fine di prevenire la perdita totale o parziale della riservatezza, integrità e/o disponibilità delle informazioni in esso contenute nonché di prevenire eventuali guasti all'intero sistema. All'utente non è consentito stampare un documento elettronico, contenente informazioni riservate, trasformandolo in un documento cartaceo, se non solo ed esclusivamente per esigenze di lavoro. In tale ipotesi, il grado di riservatezza e segretezza delle informazioni contenute nel documento cartaceo dovrà ritenersi esattamente equivalente a quello delle medesime informazioni contenute nel documento elettronico trasformato mediante stampa. L'utente dovrà assicurare alle informazioni riservate contenute nel documento cartaceo una protezione adeguata ed equivalente a quella richiesta per i documenti elettronici corrispondenti.

Per ogni necessità interna, il personale espressamente incaricato ed autorizzato dalla società quale Amministratore di Sistema potrà accedere alla memoria di massa locale del PC e ai server nonché, previa comunicazione all'utente, accedere al PC di quest'ultimo anche in modalità "da remoto".

Al personale espressamente incaricato dalla società quale Amministratore di Sistema è riconosciuta la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato esclusivamente su chiamata dell'utente o, in caso di oggettiva necessità, a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso.

Inoltre, dal momento che la violazione delle regole di cui sopra potrebbe esporre la società al rischio di danneggiamento del sistema informatico, il loro rispetto potrebbe essere oggetto di controllo attraverso periodiche verifiche del contenuto della memoria di massa dei server oltre che del PC consegnato all'Utente.

Utilizzo di dispositivi rimovibili

La postazione e gli eventuali supporti di memoria rimovibili (CD, chiavi USB, memory card ecc.) devono essere conservati in luoghi protetti; è sempre necessario verificare il contenuto informativo dei supporti di memoria, prima della loro consegna a terzi e prima della loro eliminazione / distruzione.

L'utente non è autorizzato ad accedere, né a tentare l'accesso alle informazioni per le quali non ha alcun privilegio; è altresì vietato tentare di guadagnare privilegi non concessi dal proprietario del dato.

Tutti i supporti magnetici rimovibili (CD, DVD riscrivibili, supporti USB, memory card, cellulari ecc.), contenenti dati "sensibili" nonché informazioni costituenti patrimonio dell'Ordine, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati "sensibili", ogni utente dovrà contattare il personale IT dell'Ordine e seguire le istruzioni da questo impartite. In ogni caso, i supporti magnetici contenenti dati sensibili devono essere adeguatamente custoditi dagli utenti in armadi chiusi. L'utente è responsabile della custodia dei supporti e dei dati in essi contenuti.

Sistemi di protezione dei dati

Credenziali di autenticazione

Le credenziali di autenticazione ai sistemi informatici, generalmente composte da un "identificativo utente" (c.d. username o user) al quale è associata una specifica "password", sono informazioni di carattere assolutamente personale e non cedibili, per nessuna ragione.

Se si è in possesso di più credenziali di autenticazione, è necessario fare attenzione ad accedere ai dati unicamente con le credenziali relative al trattamento in oggetto. Nell'utilizzo delle credenziali di autenticazione l'utente è tenuto a rispettare:

- l'ambito di competenza assegnato;
- le base dati a cui poter accedere;
- il profilo di autorizzazione assegnato;
- le tipologie di trattamento consentito;

segnalando tempestivamente eventuali anomalie e/o malfunzionamenti riscontrati.

Scelta della password

Elaborare le password seguendo le istruzioni sotto riportate.

Di norma 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.

L'utente 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 dall'utente con una frequenza di almeno 6 mesi o nel caso in cui il sistema lo preveda, alle scadenze proposte dal sistema stesso.

Se il trattamento riguarda categorie particolari di dati o dati di natura giudiziaria, la password deve essere modificata con frequenza maggiore (es.: ogni 3 mesi).

Di seguito sono riportate alcune indicazioni "utili" per la scelta di una password

Cose da fare

- Creare password lunghe e/o utilizzare più di una parola (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);

- È utile sapere che la maggior parte degli “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);
- 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: Es.: a, b, c,
  - Caratteri maiuscoli: Es.: A, B, C,
  - Caratteri numerici: Es.: 0,1,2,3,4,5,6,7,8,9
  - Caratteri non alfanumerici: Es.: < > ` ~! $ % ^ ; * - + = | \ { @ # } [/] : ; " '?
- Non inserire i “caratteri speciali” alla fine di una parola nota (ad esempio la password “computer987" 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);
- 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", "$"al posto di "S", zero (0) o la doppia parentesi () al posto di "O", e "3" al posto di "E"). Si tratta di trovare delle analogie che ci rendano familiare la sostituzione di lettere con simboli e numeri (con alcune sostituzioni si possono creare password riconoscibili per l'utente, ad esempio "Ve$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 sopra riportata.
-

Cose da NON fare

- NON divulgare la propria password: lo scopo principale per cui si usa una password è assicurare che nessun altro possa utilizzare le risorse o possa farlo per conto dell’utente;
- NON scrivere la password in nessun posto in cui possa essere letta facilmente, soprattutto vicino al PC;
- In fase di immissione della password assicurarsi di non essere osservato;
- NON scegliere password che siano contenute all’interno di un dizionario: su alcuni sistemi è possibile "provare" tutte le password contenute in un dizionario per individuare quale giusta (l’utilizzo di parole straniere non consente di aggirare tale problema);
- NON è opportuno utilizzare il “nome utente” quale password (è la password più semplice da indovinare);

- NON è opportuno utilizzare password che possano in qualche modo essere facilmente collegate all'utente (Es.: nome, nome della moglie / marito, nome dei figli, del cane, date di nascita, numeri di telefono, ecc.).
-

Antivirus

Ogni utente deve accertarsi che, sulla propria postazione di lavoro, il software antivirus sia sempre aggiornato e funzionante, secondo quanto definito dalla società.

Non è consentito agli utenti disabilitare o inibire il corretto funzionamento del software antivirus eventualmente installato sulla propria Postazione di Lavoro, o modificarne la configurazione, disabilitando o disattivando i meccanismi di notifica automatica degli eventi e di segnalazione degli allarmi.

Qualora per la propria postazione di lavoro non esista un software antivirus rispondente alle norme, o non sia possibile installare correttamente il software antivirus, l'utente dovrà informare immediatamente il proprio Responsabile.

Nel caso in cui il software antivirus rilevi la presenza di un virus che non è riuscito ad eliminare, l'utente deve immediatamente sospendere ogni elaborazione in corso, senza spegnere il computer e segnalare l'accaduto ai referenti IT dell'Ordine.

Non è consentito agli utenti rimuovere virus con azioni personali, ma è necessario avvalersi dell'assistenza necessaria, attenendosi alle modalità stabilite dalle eventuali procedure di "gestione degli incidenti"; ad operazione ultimata, gli utenti devono accertarsi dell'eliminazione del virus e della riusabilità della Postazione di Lavoro.

Sistemi di backup

Per ogni applicazione utilizzata dalla società devono essere previste attività di backup periodico per le quali sono definiti i seguenti aspetti:

- la frequenza di esecuzione dell'attività;
- le modalità di effettuazione;
- il numero di copie da produrre;
- il periodo di conservazione dei dati.

I servizi di backup devono essere adeguati in relazione alla tipologia di dati contenuti all'interno delle diverse applicazioni e devono essere volti a garantire che tutte le informazioni essenziali e il software possano essere recuperati a seguito di un guasto o di un disastro.

i backup devono essere memorizzati in una posizione remota (con protezione ambientale e fisica), ad una distanza sufficiente per sfuggire ai danni eventualmente provocati da un disastro al luogo principale;

supporti di backup devono essere testati regolarmente per garantire che possano essere effettivamente utilizzati in caso di emergenza.

Operatività su banche dati

È raccomandabile, laddove possibile, che l'estrazione, la copia, il salvataggio e la stampa su qualunque supporto d'informazioni contenute in banche dati sia precluso, mediante adozione di idonei dispositivi tecnologici e strumenti organizzativi, a tutti gli utenti con la sola esclusione di quelli a ciò specificamente autorizzati per ragioni tecniche. Tale previsione non risulta applicabile alle banche dati funzionali al raggiungimento delle finalità istituzionali dell'Ordine e utilizzate per lo svolgimento dei propri servizi, ovvero che siano prodotte e commercializzate con espressa concessione di tali facoltà in virtù della loro natura di strumenti di diffusione di determinati contenuti informativi.

Servizi di rete

Nell'utilizzo della rete interna (se presente) gli utenti devono tenere un comportamento corretto e diligente. A tal riguardo, l'utente non deve effettuare nessun tipo di attività volta ad eludere o compromettere i meccanismi di protezione dei sistemi informatici.

Utilizzo di internet

Il servizio di connessione ad Internet dell'Ordine è uno strumento operativo che viene reso disponibile agli utenti che ne abbiano effettiva necessità.

L'accesso ad Internet è fornito allo scopo di ottenere informazioni necessarie allo svolgimento dell'attività lavorativa. Essendo uno strumento di lavoro di proprietà dell'Ordine, gli Utenti cui la società attribuisce l'accesso sono responsabili del suo corretto utilizzo.

Esso costituisce una risorsa ed un'opportunità di sviluppo dell'Ordine, ma rappresenta anche una potenziale minaccia alla sicurezza dei sistemi e delle informazioni. L'uso incauto può essere una fonte di rischio per la sicurezza, oltre che un costo rilevante per gli enti.

La società qualora lo ritenga necessario ha la facoltà di revocare l'accesso ad Internet dei singoli utenti e di installare software atti a filtrare / bloccare in automatico l'accesso a siti che non sono ritenuti di interesse dell'Ordine o attinenti ad attività lavorative. L'utente che accede ad un sito Internet deve prendere visione se specificato nel sito stesso, dei termini e le condizioni che ne regolano l'utilizzo e operare in conformità delle stesse.

L'uso di Internet attraverso le apparecchiature dell'Ordine è consentito solo per motivi di lavoro e nell'interesse esclusivo dell'Ordine. La connessione ad Internet dai computer (inclusi portatili e palmari) e ogni accesso alla rete Internet potrebbero essere registrati nel proxy Server dell'Ordine.

L'accesso ad Internet deve avvenire solo attraverso le infrastrutture tecnologiche poste in essere dalla società e deve essere configurato dal personale IT specializzato. Non è autorizzato pertanto l'accesso a Internet utilizzando collegamenti via modem o altri mezzi di collegamento personali.

L'utente si impegna, nei confronti dell'Ordine cui appartiene, a non utilizzare il servizio di connessione ad Internet per scopi illegali o che comunque possano recare danno o pregiudizio alla medesima o a terzi, assumendosi ogni responsabilità derivante dall'uso improprio del servizio ed

esonerando contestualmente la società da ogni pretesa o azione che dovesse essere rivolta alla medesima da qualunque soggetto, in conseguenza di tale uso improprio.

L'utente, inoltre, non può utilizzare la connessione a Internet in modo da danneggiare, disattivare, sovraccaricare, pregiudicare o interferire con l'utilizzo e il godimento della stessa da parte di altri Utenti. In ogni caso al dipendente o collaboratore non è consentito:

- accedere ai siti Internet assoggettati a restrizione da parte dell'Ordine, forzando i sistemi di sicurezza dalla medesima predisposti ed in ogni caso utilizzare siti o altri strumenti (es. Cracking Programs) che realizzino tale fine;
- effettuare il download di software, ancorché gratuito (freeware), o messo a disposizione in rete per essere provato (shareware, demo), e comunque il download di qualsiasi software nonché di file multimediali (come file musicali o video) senza l'espressa autorizzazione dell'Ordine;
- modificare la configurazione del browser o del PC in modo da diminuirne il livello di protezione Internet;
- effettuare qualsiasi genere di attività personale di guadagno economico, nonché di transazione finanziaria in rete, ivi compresi gli acquisti on line e le operazioni di remote banking per scopi estranei allo svolgimento dell'attività lavorativa;
- accedere a siti Internet che abbiano un contenuto contrario a norme di legge e a norme a tutela dell'ordine pubblico;
- utilizzare Internet per effettuare attività considerate illegali e, comunque, accedere a siti contenenti:
    - materiale teso alla promozione di comportamenti criminali o violenti;
    - materiale discriminante o lesivo in relazione a razza, sesso, religione, ecc.;
    - materiale che violi la legge in materia di protezione dati personali;
    - contenuti o materiali che violino i diritti di proprietà di terzi;
    - materiale pornografico o simile, in particolare in violazione della legge n.269 del 1998 "Norme contro lo sfruttamento sessuale dei minori degli anni 18";
    - altri contenuti inappropriati o contrari alla legge;
- accedere, attraverso le apparecchiature dell'Ordine, a qualsivoglia gruppo di discussione o conferenza in rete (chat lines o altro) o banche dati esterne, con la sola esclusione di quelli espressamente autorizzati;
- utilizzare identificativi altrui al fine di effettuare la connessione a Internet;
- utilizzare l'accesso ad Internet in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore.

Qualunque attività eseguita in Internet deve tenere conto, in qualunque momento, dell'integrità dei dati dell'Ordine, per esempio: non si devono divulgare informazioni tecniche quali IP address, password o identificativi utenti.

La società potrebbe utilizzare prodotti di content filtering per selezionare il traffico di Internet e si potrebbe dotare di apposite procedure per la gestione dei profili di accesso al servizio, che regolamentano e limitano l'accesso al servizio e ad alcuni siti.

Il dipendente è tenuto a dare tempestiva segnalazione di eventuali anomalie o irregolarità nel funzionamento dell'accesso a Internet, al fine di prevenire eventuali guasti all'intero sistema.

Dal momento che la violazione delle regole sopra riportate potrebbe esporre la società al rischio di danneggiamento o mal funzionamento del sistema informatico, il rispetto di tali regole potrà essere oggetto di controllo anche mediante accesso in remoto, attraverso periodiche verifiche del contenuto della memoria di massa dei server di accesso a Internet (proxy), dei PC e dei sistemi di "content filtering", nonché mediante esame dei file di log della navigazione svolta.

Tale controllo costituisce una procedura di controllo di carattere "ordinario" (o di 1° livello), rivolta principalmente in modo indistinto alla popolazione dell'Ordine, giustificata da esigenze operative,

organizzative e produttive dell'Ordine nonché dalla necessità di tutela del patrimonio informativo dell'Ordine stessa, e potrà essere eseguita anche mediante l'utilizzo di strumenti automatizzati. L'accesso ai sistemi ed alle evidenze del controllo è riservato esclusivamente al personale dell'Ordine individuato quale "Amministratore di Sistema".

Posta elettronica

La società può attribuire agli utenti un "account" o indirizzo di posta elettronica utilizzabile per inviare e ricevere e-mail.

La casella di posta elettronica assegnata all'utilizzatore, il relativo indirizzo e i messaggi in entrata ed in uscita dalla stessa, sono di proprietà dell'Ordine. Essi rappresentano uno strumento di lavoro affidato all'utente al solo fine di consentirgli di svolgere le proprie mansioni ed attività lavorativa. Le persone cui la società attribuisce l'uso di caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse. La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti. Il personale incaricato dalla società quale Amministratore di Sistema, inoltre, è autorizzato a compiere interventi nel sistema informativo dell'Ordine diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento / sostituzione / implementazione di programmi, manutenzione hardware etc.). Tali interventi, potranno anche comportare l'accesso in qualunque momento alle caselle di posta elettronica degli utenti, escludendo tuttavia che l'accesso sia finalizzato, in tali circostanze, ad attività di controllo.

Utilizzando l'indirizzo di posta elettronica dell'Ordine, l'utente è a conoscenza e consapevole che:

- un messaggio di posta elettronica si configura, da un punto di vista giuridico, come corrispondenza aperta, potendo essere letto da chiunque durante il suo percorso sulla rete Internet fino al destinatario, nonché dall'Amministratore di sistema sui server;
- l'uso dell'indirizzo di posta elettronica dell'Ordine è ammesso per motivi attinenti all'attività lavorativa: l'uso per motivi personali è consentito solo nei limiti della normalità e cioè per un limitato numero di messaggi di cortesia o inerenti rapporti parentali o amicali, sempre nel rispetto delle norme di comportamento interne e tenuto conto dell'interesse dell'Ordine;

- a tutela del proprio diritto alla privacy, relativa ai messaggi di posta elettronica in entrata ed in uscita utilizzando l'indirizzo dell'Ordine, l'accesso ai messaggi personali ivi contenuti, qualora esso si dovesse rendere necessario (es. in caso di assenza non programmata dell'utente), oppure per motivazioni di carattere lavorativo ed a giudizio dell'Ordine, può avvenire per il tramite di altro collega (fiduciario) indicato dal dipendente stesso. Sarà comunque consentito al superiore gerarchico o, sentito l'utente (qualora raggiungibile), a persona individuata dalla società, accedere alla propria casella di posta elettronica per ogni ipotesi di carattere lavorativo per cui ciò si dovesse rendere necessario. Il fiduciario, che agirà all'occorrenza in caso di assenza dell'utente, ovvero il superiore gerarchico, o la persona individuata dalla società come sopra indicato, utilizzerà una password d'ingresso creata "ad hoc" dal fiduciario (ovvero dal superiore gerarchico o persona individuata dalla società) mediante autorizzazione dell'Ordine. La password dovrà essere custodita dal fiduciario (ovvero dal superiore gerarchico o persona individuata dalla società) e dovrà essere resettata al cessare delle suddette motivazioni o al rientro del titolare. È cura dell'utente segnalare al proprio superiore gerarchico il nominativo del fiduciario prescelto;
- il messaggio di posta elettronica potrebbe essere letto da destinatari diversi da quelli a cui era diretto, e ciò potrebbe determinare danni anche gravi alla società;
- falsi o errati messaggi di posta elettronica scritti per conto e nel nome dell'Ordine potrebbero essere spediti per errore sia all'interno che all'esterno dell'Ordine;
- messaggi di posta elettronica spediti potrebbero non essere recapitati, essere distrutti o subire ritardi. In ogni caso al dipendente o collaboratore non è consentito:
- inviare un messaggio con allegato un file eseguibile (.exe);
- utilizzare l'indirizzo di posta elettronica contenente il dominio dell'Ordine per iscriversi a qualsivoglia sito per motivi non attinenti all'attività lavorativa, senza espressa autorizzazione scritta dell'Ordine, nonché per partecipare a qualunque genere di petizione, "catene di Sant'Antonio" o in generale, a qualunque pubblico dibattito su qualsivoglia tema;
- indicare liberatorie personalizzate all'interno dei messaggi;
- utilizzare il servizio di posta elettronica per trasmettere a soggetti esterni alla società informazioni riservate o comunque documenti interni, se non nel caso in cui ciò sia necessario in ragione delle mansioni svolte;
- accedere a caselle di posta elettronica personali attraverso la rete (Webmail) e le apparecchiature dell'Ordine. L'utente non potrà, peraltro, inoltrare automaticamente i messaggi ricevuti all'indirizzo di posta elettronica dell'Ordine su indirizzi personali;
- inviare o archiviare messaggi in forma crittografata senza l'espressa autorizzazione che deve essere richiesta ai referenti IT;
- inviare, tramite la posta elettronica, anche all'interno della rete dell'Ordine, alcun materiale a contenuto violento, sessuale o comunque offensivo dei principi di dignità personale, di libertà religiosa, di libertà sessuale o di manifestazione del pensiero, anche politico. Qualora il dipendente riceva messaggi aventi tale contenuto, è tenuto a darne comunicazione tempestiva al proprio responsabile;
- ricevere ed inviare messaggi con allegati diversi da quelli inerenti e connessi alla prestazione lavorativa;

- creare, archiviare o spedire, anche all'interno della rete dell'Ordine, messaggi pubblicitari o promozionali o comunque allegati (filmati, immagini, musica o altro) in nessun modo connessi con lo svolgimento della propria attività lavorativa, nonché partecipare a richieste, petizioni, mailing di massa di qualunque contenuto utilizzando l'indirizzo dell'Ordine;
- utilizzare la posta elettronica dell'Ordine in violazione delle norme in vigore nell'ordinamento giuridico italiano a tutela del diritto d'autore.

Il dipendente o il collaboratore è tenuto a dare tempestiva segnalazione di eventuali anomalie o irregolarità nel funzionamento della posta elettronica, al fine di prevenire la perdita totale o parziale della riservatezza, integrità e/o disponibilità delle informazioni in essa contenute nonché di prevenire eventuali guasti all'intero sistema.

Dal momento che la violazione delle regole sopra riportate potrebbe esporre la società al rischio di danneggiamento o mal funzionamento del sistema informatico, il rispetto di tali regole potrebbe essere oggetto di controllo attraverso periodiche verifiche del contenuto della memoria di massa dei server oltre che del PC consegnato al dipendente.

Tale controllo costituisce una procedura di controllo di carattere "ordinario" (o di 1° livello), rivolta principalmente in modo indistinto alla popolazione dell'Ordine, giustificata da esigenze operative, organizzative e produttive dell'Ordine nonché dalla necessità di tutela del patrimonio informativo dell'Ordine stessa, e potrà essere eseguita anche mediante l'utilizzo di strumenti automatizzati. L'accesso ai sistemi ed alle evidenze del controllo è riservato esclusivamente al personale dell'Ordine individuato quale "Amministratore di Sistema".

Collegamento remoto

Il collegamento remoto a reti, sistemi o applicazioni dell'Ordine è consentito esclusivamente per finalità interne attraverso i punti di ingresso identificati ed autorizzati (server di posta, concentratori VPN, o altro) e per il tempo strettamente necessario all'esecuzione delle attività lavorative.

Il collegamento tramite computer non dell'Ordine è consentito esclusivamente se preventivamente autorizzato o per gravi e motivate situazioni di emergenza. In ogni caso, il computer utilizzato deve essere dotato di sistemi antivirus, attivi ed aggiornati. È vietato il collegamento da dispositivi pubblici, ad esempio Internet point.

Accesso ai sistemi

L'accesso ai sistemi, alle reti ed alle applicazioni deve essere preventivamente autorizzato e deve svolgersi con modalità conformi allo svolgimento delle attività dell'Ordine. L'Ordine attribuisce ad ogni utente delle credenziali di autentificazione (user-id e password) per l'accesso alle risorse e alla rete locale. L'accesso deve avvenire esclusivamente attraverso l'utilizzo della utenza personale (user-id) assegnata o, in casi particolari per finalità di test, assistenza o manutenzione, con altra, apposita utenza.

La mera possibilità di utilizzo di sistemi, reti o applicazioni per le quali non si sia stati preventivamente autorizzati non costituisce una implicita autorizzazione, ma al contrario è da ritenere una possibile esposizione di sicurezza da segnalare alle strutture competenti.

L'accesso ai sistemi, alle reti ed alle applicazioni è sottoposto a registrazione.

Le credenziali di accesso, costituendo la base per l'identificazione e l'autenticazione degli utenti nella fase di accesso ai sistemi informatici, devono essere custodite con la massima riservatezza e non rivelate ad alcuno (neanche ai colleghi). Qualunque accesso effettuato utilizzando le credenziali personali dell'utente è da considerare sotto la diretta responsabilità dell'utente stesso così come lo sono le conseguenti operazioni effettuate.

Analoga riservatezza deve essere osservata nei confronti delle credenziali di accesso "applicative" (cioè delle credenziali utilizzate da applicazioni, sistemi o dispositivi) di cui si venga a conoscenza. Qualora l'utente ritenga che la confidenzialità delle credenziali sia stata compromessa, deve provvedere, nel caso di password, al cambio immediato della stessa, o, nel caso di credenziali di autenticazione di altro genere (smart card, token, ecc.), all'immediata segnalazione ai referenti IT. Le credenziali di accesso rilasciate all'utente sono conservate con modalità che non ne consentono la conoscenza o la ricostruzione, neanche da parte del personale IT.

Trattamento di dati personali residenti su archivi cartacei

Gli atti e i documenti contenenti dati personali e/o sensibili (vedi definizioni seguenti) devono essere conservati in contenitori/armadi o locali con accesso limitato al personale incaricato.

I documenti cartacei, se contenenti dati personali, dovranno essere trattati in modo riservato e distrutti previa autorizzazione dell'apposita direzione dell'Archivio generale dello Stato.

È vietata la stampa e/o la riproduzione di documenti se non finalizzate all'attività lavorativa.

Politiche generali per l'utilizzo degli archivi cartacei

Tutto il materiale cartaceo contenente dati personali deve essere gestito evitando che esso risulti facilmente visibile a persone terze o, comunque, ai non autorizzati al trattamento. Non deve essere lasciato incustodito sulle scrivanie e, a fine lavoro, deve essere riposto in un luogo sicuro.

In caso di trattamento di dati particolarmente sensibili (condizioni di salute, dati giudiziari, ecc.), tutta la documentazione cartacea deve essere conservata in armadi/cassetti chiusi a chiave o stanze chiuse a chiave in caso di allontanamento, anche temporaneo, dalla postazione di lavoro.

I documenti contenenti dati "sensibili" particolari devono essere controllati e custoditi in modo che non vi accedano persone non autorizzate. La consultazione deve avvenire per il tempo strettamente necessario alla digitazione stessa e, subito dopo, i documenti devono essere archiviati.

Ogni dipendente o collaboratore ha la responsabilità dei propri documenti e in presenza di dati personali, deve:

- consentire l'accesso unicamente per finalità lavorative, a persone autorizzate e limitatamente ai dati la cui conoscenza è strettamente necessaria;
- proteggere i documenti cartacei e i dati personali in essi contenuti da perdite, distruzione, falsificazione, accesso e divulgazione non autorizzati;
- conservare gli atti e i documenti contenenti dati personali in archivi ad accesso selezionato, secondo le istruzioni del proprio responsabile;
- distruggere fisicamente i documenti cartacei che contengono dati personali prima di cestinarli;
- restituire i documenti al termine delle operazioni affidate.

Obbligo di comunicare i casi di violazione dei dati personali (data breach)

Il titolare del trattamento (per il tramite del suo Presidente, con la collaborazione del Consiglio dell'Ordine e del Responsabile Interno) deve comunicare eventuali violazioni dei dati personali all'Autorità Garante della protezione dei dati.

Se la violazione dei dati rappresenta una minaccia per i diritti e le libertà delle persone, il titolare dovrà informare in modo chiaro, semplice e immediato anche tutti gli interessati e offrire indicazioni su come intende limitare le possibili conseguenze negative.

Il titolare del trattamento potrà decidere di non informare gli interessati se riterrà che la violazione non comporti un rischio elevato per i loro diritti (quando non si tratti, ad esempio, di frode, furto di identità, danno di immagine); oppure, nell'eventualità in cui informare gli interessati potrebbe comportare uno sforzo sproporzionato, la comunicazione avviene sul sito web del titolare).

L'Autorità di protezione dei dati potrà comunque imporre al titolare del trattamento di informare gli interessati sulla base di una propria autonoma valutazione del rischio associato alla violazione.

Gestione dei rischi e degli incidenti

Ogni dipendente o collaboratore è tenuto a segnala~~re~~ tempestivamente al Titolare in forma tracciabile (ad esempio utilizzando le caselle di posta) eventuali violazioni nelle misure di sicurezza, smarrimento o furto di informazioni o di strumenti informatici, trattamenti illeciti o situazioni di rischio di cui sia venuto a conoscenza.

Per ogni incidente, si dovrà procedere con una prima rapida valutazione dell'accaduto e dei rischi derivanti.

In seguito, l'amministratore del sistema di riferimento dovrà:

- raccogliere la documentazione comprovante quanto accaduto;
- conservarla in modo da garantirne la disponibilità, l'integrità e per quanto possibile, evitare ogni contestazione da parte degli incaricati.

Nel caso in cui l'incidente abbia compromesso o possa compromettere la riservatezza, l'integrità o la disponibilità dei dati, dovrà essere coinvolto tempestivamente il "Responsabile della Protezione dei dati" ed il Consiglio dell'Ordine, che provvederà ad indicare:

- le contromisure da attivare;
- l'obbligo di notificazione all'Autorità Garante;
- l'obbligo di comunicazione tempestiva agli interessati coinvolti.

APPENDICE 1 – Lavoro da remoto

Nella necessità di dover lavorare senza accedere ai locali preposti dove sono presenti i sistemi dell'Ordine, devono essere approntate delle misure atte a garantire la sicurezza dell'accesso e dei trattamenti dei dati.

In particolare, vanno tenuti sotto controllo l'utilizzo di PC e device personali dell'incaricato e l'accesso da remoto ai sistemi aziendali.

Informative

Il datore di lavoro deve informare/formare il lavoratore sulle modalità di gestione e sui rischi derivanti dai trattamenti eseguiti.

E' opportuno che il datore rammenti al personale in smart working che è tenuto al rispetto delle istruzioni già rese dal titolare in tema di trattamento e protezione dei dati personali, con le "Norme e disposizioni emanate in applicazione del Regolamento Generale sulla Protezione dei Dati personali".

Istruzioni operative

E' necessario che il lavoratore individui una zona ove allestire una postazione utilizzata in modo esclusivo, per assicurare la riservatezza dei dati (trattati sia su carta - sia su video) e garantire l'integrità dei documenti e dei sistemi informatici utilizzati.

Utilizzo dispositivi aziendali:

Il computer affidato al dipendente è uno strumento di lavoro, pertanto, ne è vietato l'utilizzo per attività personali, non attinenti allo svolgimento delle proprie mansioni, a meno di autorizzazione scritta in merito.

Per l'utilizzo valgono le stesse regole descritte per l'uso in ufficio.

Utilizzo dispositivi personali

Qualora il lavoratore, per eseguire la prestazione lavorativa, non disponga di un dispositivo aziendale, previa autorizzazione dell'Ente, dovrebbe:

- utilizzare un dispositivo personale ad uso esclusivo;
- nel caso il dispositivo (pc, tablet) sia condiviso con i familiari, creare un account personale, in modo da realizzare una partizione esclusiva;
- impedire l'accesso di altre persone ai documenti e ai dispositivi aziendali;
- evitare il ricorso a credenziali conosciute e/o facilmente intuibili;

- non salvare nel browser del dispositivo le password di accesso ai programmi aziendali;
- verificare che il dispositivo sia dotato di misure di protezione aggiornate, quali: antivirus, antimalware e firewall. Il datore potrebbe, indicare e/o fornire i tool di sicurezza più adatti;
- non salvare documenti aziendali nella memoria del proprio dispositivo o in periferiche personali, laddove siano disponibili funzioni di salvataggio sui sistemi/server aziendali;
- non aprire allegati o link sospetti;
- non scaricare/istallare programmi di dubbia provenienza;
- disconnettersi accuratamente a fine lavoro dagli applicativi aziendali.

Accesso dall'esterno ai sistemi aziendali

Il Titolare e l'Amministratore di sistema devono scegliere una modalità sicura per gestire l'accesso ai sistemi aziendali, da remoto.

Sarebbe opportuno valutare/prevedere:

- canali sicuri/criptati e credenziali di accesso a doppio fattore (OTP- one-time password);
- utilizzo di V.P.N. con pass-phrase complesse;
- firewall con specifiche regole per consentire l'accesso solo dai computer conosciuti/assegnati al dipendente.

Videochiamate

La scelta dei software necessari a connettersi alle applicazioni e la scelta delle soluzioni per collaborare a distanza è fondamentale per poter operare e mantenere adeguate relazioni con i colleghi e con gli utenti.

Indipendentemente dal sistema utilizzato per il collegamento è importante:

- Assicurarsi di effettuare la chiamata da luogo segregato dove non si può essere uditi da terze parti
- Verificare che la videocamera non inquadri elementi personali
- Verificare che lo schermo del computer non sia visibile da terzi

Attestato di ricevuta del Regolamento interno per il trattamento dei dati personali"

Il sottoscritto

_____

Dichiara di aver ricevuto, letto e compreso il presente documento relativo al il trattamento dei dati personali ai sensi del Regolamento Generale per la Protezione dei Dati 679/2016, e si impegna alla scrupolosa osservanza delle norme comportamentali in esso indicate.

Data…_____/____/_____

Firma

_____

Il presente modulo deve essere restituito al Titolare del Trattamenti compilato e firmato.

Piazza Sant'Ambrogio 8, 20123 MILANO - P. IVA 04772390961 - Tel. 02 4003 1996 email: dposervice@eps-italia.com