MISURE DI SICUREZZA E LINEE GUIDA

AZIENDALI PER IL TRATTAMENTO DEI DATI

PERSONALI CONFORME REG. UE 679/2016

La Casa del sorriso Srl in persona del Direttore Sanitario pro tempore

Dott. Pietro Floris

09047 Selargius (SU Planu)

Centrolacasadelsorriso@pec.it

PRINCIPI GENERALI

Nel presente documento sono indicate le linee guida delle procedure di gestione raccolta trasmissione conservazione e cancellazione dei dati personali raccolti.

L'adozione in seno alla **La Casa del sorriso Srl**. in persona del legale rappresentante pro tempore con sede in Sestu, della presente disciplina ha come obiettivo quello di assicurare una corretta gestione delle procedure di trattamento dei dati personali ed il rispetto dei principi e precetti contenuti nel Reg. Ue 679/2016.

Il Responsabile del Trattamento dei Dati Personali è stato individuato ed incaricato a far data dal 23.05.2018, il quale di concerto con L'amministratore Legale pro tempore della predetta società e collaboratori incaricati, procede allo svolgimento dei compiti nei limiti delle rispettive prerogative contrattuali.

Questo documento, è stato adottato in virtù dell'autorizzazione rilasciata dal Legale rappresentante pro tempore della società **La Casa del sorriso Srl**, su proposta del Responsabile del Trattamento dei Dati Personali e del Responsabile della Protezione dei dati personali, in conformità delle disposizioni di cui al Regolamento UE 679/2016.

Sono di seguito specificate le linee guida relative alle diverse procedure di trattamento dei dati personali, al rispetto e alle quali, gli Incaricati e tutti i dipendenti collaboratori nell'espletamento delle rispettive mansioni affidate, ove risultassero soggetti attivi o passivi rispetto alle generali procedure di trattamento dei dati e previo l'ausilio ed il consenso del nominato Responsabile del Trattamento dei dati Personali (DPO), procederanno ad attuare con le sotto indicate modalità nelle diverse aree

operative, con particolare attenzione, rispetto all'adempimento di tutti i rapporti contrattuali in essere con altre e diverse società che verranno identificate.

A tal proposito, allo scopo di rappresentare agli utenti il quadro normativo di riferimento si specifica che la principale fonte normativa è rinvenibile nel Reg. Ue 679/2016 e successive integrazioni o modificazioni operate dal legislatore Italiano ed Europeo.

Copia del presente Regolamento viene pubblicata sul *sito internet aziendale* nella sezione "Privacy Policy" e consegnata a ciascun dipendente all'atto dell'assunzione ed a ciascun collaboratore ad inizio attività.

Definizione di Dato personale:

Art. 4, comma 1, lett. B Reg. Ue 679/2016, "Dato personale sensibile" è rappresentato da qualunque informazione relativa a persona fisica e giuridica, ente od associazione, siano esse, informazioni nominative (come le generalità di una persona), o una qualunque altra informazione che possa rendere identificabile l'interessato, anche indirettamente (ad esempio codice fiscale, numero di matricola del dipendente);

Art. 4, comma 1, lett. "dato sensibile" si fa riferimento ai dati idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale nonché i dati personali idonei a rivelare lo stato di salute dell'interessato;

Art. 4, comma 1, lett. e "dato giudiziario sono i dati idonei a rivelare i provvedimenti in materia inseriti nel casellario giudiziale, di quelli dell'anagrafe delle sanzioni amministrative dipendenti da reati e dei relativi carichi pendenti, la qualità di imputato o di indagato ai sensi degli artt. 60 e 61 del Codice di procedura penale.

I dati giudiziari non sono in alcun modo oggetto di trattamento in seno alla **La Casa del sorriso Srl**. in persona del legale rappresentante pro tempore.

Dati di Utilizzo

Sono le informazioni raccolte automaticamente attraverso questo i siti Web ove inserito il presente documento (anche da applicazioni di parti terze integrate in questo Sito Web), tra cui: gli indirizzi IP o i nomi a dominio dei computer utilizzati dall'Pazienteche si connette con questo Sito Web, gli indirizzi in notazione URI (Uniform Resource Identifier), l'orario della richiesta, il metodo utilizzato

nell'inoltrare la richiesta al server, la dimensione del file ottenuto in risposta, il codice numerico indicante lo stato della risposta dal server (buon fine, errore, ecc.) il paese di provenienza, le caratteristiche del browser e del sistema operativo utilizzati dal visitatore, le varie connotazioni temporali della visita (ad esempio il tempo di permanenza su ciascuna pagina) e i dettagli relativi all'itinerario seguito all'interno dell'Applicazione, con particolare riferimento alla sequenza delle pagine consultate, ai parametri del sistema operativo e all'ambiente informatico dell'Utente.

Servizio

Il Servizio fornito dai siti web in dotazione della predetta società così come definito nei relativi termini su questo sito/applicazione.

Unione Europea (o UE)

Salvo ove diversamente specificato, ogni riferimento all'Unione Europea contenuto in questo documento si intende esteso a tutti gli attuali stati membri dell'Unione Europea e dello Spazio Economico Europeo.

Cookie

Piccola porzione di dati conservata all'interno del dispositivo dell'Utente.

PREAVVERTENZE

L'inosservanza delle norme sulla privacy e del Reg. Ue 679/2016 può comportare a seguito dell'accertamento di tali violazioni, l'irrogazione di sanzioni di natura civile e penale per l'incaricato e per l'azienda, da parte dell'autorità competente

Preme preliminarmente evidenziare che qualora venissero rilevate e certificate delle prassi differenti rispetto a quelle ivi indicate l'Amministratore legale pro tempore ed il Responsabile del trattamento dei dati personali anche in assenza di un provvedimento sanzionatorio e previa analisi degli elementi in loro possesso, si riservano la facoltà di promuovere idonee azioni a tutela della sociètà e delle rispettive sfere giuridico soggettive.

In conformità ai principi e alle normative vigenti in materia; i soggetti parte del procedimento di trattamento dei dati personali, potranno essere oggetto di procedimento disciplinare nel caso d'inadempimento delle prerogative ivi indicate ed affidate, salvo che nel contraddittorio tra le parti, questi dimostrino che l'evento dannoso "non gli è in alcun modo imputabile" (ex art. 82, paragrafo 1 e 3 Reg. 679/2016);

Sì raccomanda dunque di prestare la massima attenzione nella lettura delle disposizioni e nell'adozione delle linee guida e disposizioni sotto specificate.

II) CAMPO DI APPLICAZIONE MISURE SICUREZZA

Le presenti Istruzioni sono adottate nello svolgimento delle mansioni dei soggetti sotto elencati ed in particolare nelle attività o comportamenti comunque connessi all'utilizzo della rete Internet e della posta elettronica, mediante strumentazione aziendale o di terze parti autorizzate all'uso dell'infrastruttura aziendale e dei processi operativi propri della società stessa e comunque in seno ai processi sotto descritti di Trattamento dei dati Personali, ed in tutte le sede operative e amministrative della Società presenti nel territorio Italiano.

I soggetti parte del procedimento sono:

a) Responsabile del Trattamento dei Dati Personali;
b) Sub responsabili del Trattamento dei Dati Personali;
c) Sub Responsabili del Monitoraggio del Trattamento dei Dati Personali;
d) Incaricati, lavoratori dipendenti assimilati od equiparati, ai quali per le diverse ragioni organizzative, vengono affidate anche saltuariamente delle attività in seno al predetto processo di trattamento dei dati.

III) RIFERIMENTI NORMATIVE E DEFINIZIONI

Il procedimento prevede l'indispensabile sottoscrizione e manifestazione del consenso previa sottoscrizione in duplice copia dell'apposito modulo di autorizzazione.

Reg.UE 679/2016 ex art 7-21-22-29 "Linee guida individuate sui principi di liceità del trattamento dei dati.

In particolare, le operazioni di trattamento dei dati personali sono supervisionate nella sede amministrativa e presso le sedi operative dal Dpo incaricato e dai Sub responsabili la cui nomina è stata ratificata dal Legale rappresentante Pro tempore della **La Casa del sorriso Srl** ex art 28 pgf.4 Reg Ue 679/2016.

Sono state svolte, tempestivamente delle attività di formazione per il personale dipendente e per i collaboratori, al fine di consentire una concreta e corretta attuazione delle indicate modalità di trattamento dei dati conformemente al Reg Ue 679/2016, che hanno permesso al personale l'acquisizione delle indispensabili nozioni normative e delle linee guida dei processi de quo.

Le predette competenze acquisite di concerto con la preventiva analisi delle attitudini del personale sono state le matrici determinanti per il conferimento dei specifici incarichi all'interno del procedimento.

Quanto allo svolgimento degli Audit delle attività di trattamento e di protezione dei dati personali, preme evidenziare come questi si svolgano sotto la supervisione e direttive del DPO e attraverso l'ausilio di altri Consulenti e Collaboratori individuati nominati dal Responsabile del Trattamento dei dati personali di concerto con il Responsabile della protezione dei dati personali.

Conformemente ai principi ed alle normative vigenti in materia si suole rilevare come i dipendenti potrebbero essere oggetto di procedimento disciplinare in caso d'inadempimento delle prerogative ivi indicate ed affidate, salvo che nel contraddittorio tra le parti questi dimostrino che l'evento dannoso "non gli è in alcun modo imputabile" (ex art. 82, paragrafo 1 e paragrafo 3 Reg. 679/2016);

Il presente regolamento definisce invero le responsabilità soggettive proprie del responsabile del trattamento dei dati personali e del responsabile della protezione dei dati personali e degli ulteriori incaricati vigenti ai sensi del Reg. UE 679/2016.

Pur non prevedendo espressamente la figura dell'incaricato" del trattamento (ex art. 30 Codice), infatti regolamento non ne esclude la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile" (ex art. 4, n. 10, Reg. ue 679/2016), che operano sotto la diretta autorità del Titolare o del Responsabile, attenendosi alle istruzioni impartite.

La designazione è stata effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito.

Ai fini della corretta classificazione dei dati vengono definiti rispettivamente con il termine:

a) "trattamento"

('art. 4, comma 1, lett. A del Reg. Ue 679/2016) una qualunque operazione effettuata sui dati, svolta con o senza l'ausilio di mezzi automatizzati, che abbia quella oggetto la raccolta, registrazione, consultazione, elaborazione, modifica, diffusione, estrazione, distruzione di dati, anche se non registrati in una banca dati;

b) dato personale (art. 4, comma 1, lett. b) una qualunque informazione relativa a persona fisica e giuridica, ente od associazione, siano esse informazioni nominative (come le generalità di

una persona), o una qualunque altra informazione che possa rendere identificabile l'interessato, anche indirettamente (ad esempio codice fiscale, numero di matricola del dipendente);

c) dato sensibile (art. 4, comma 1, lett. d) una qualsiasi dato idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale nonché i dati personali idonei a rivelare lo stato di salute dell'interessato;

d) dato sensibile avente natura medica: sono tutti quei dati idonei a rivelare lo stato di salute appartengono i dati raccolti in riferimento a malattie anche professionali, invalidità, infermità, gravidanza, puerperio o allattamento, ad infortuni, ad esposizioni a fattori di rischio, all'idoneità psico-fisica a svolgere determinate mansioni o all'appartenenza a categorie protette. Sono significativi i riferimenti ai permessi per festività religiose, alle diete per motivi.

§ Finalità del Trattamento dei Dati raccolti

I dati dell'pazientesono raccolti per consentire al Titolare di fornire i propri Servizi di fornitura e vendita del prodotto, così come per le seguenti finalità: Statistica, Visualizzazione di contenuti da piattaforme esterne, Protezione dallo SPAM, Contattare l'Utente, Gestione contatti.

IV Sistema e procedura per il Trattamento dei dati personali:

Il sistema di trattamento adottato comprende i seguenti capitoli del procedimento:

1) Raccolta del dato personale previa sottoscrizione dell'idonea informativa;
2) Inserimento nell'idoneo sistema informativo;
3) Classificazione;
4) Conservazione;
5) Monitoraggio;
6) Distruzione e/o cancellazione.

Nei sopra citati ed individuati capitoli (1-6) vengono ricomprese operazioni di utilizzo interno (organizzazione, conservazione, raffronto, ecc.) ed esterno (comunicazione, diffusione, interconnessione ad altre banche dati), e prescindendo sia dall'eventuale uso di strumenti informatici, sia dalla circostanza che il dato venga divulgato o elaborato nel senso stretto del termine.

Con il termine " trattamento" ci si riferisce tanto al procedimento elettronico automatizzati, quanto procedimento che richiede un supporto umano.

V) MISURE MINIME DI SICUREZZA

Nella stesura delle linee guida de quo è stata prestata particolare attenzione alla preventiva analisi dei rischi incombenti sui dati, e sull'analisi dei rischi per i diritti e le libertà delle persone fisiche.

Il procedimento invero è stato strutturato e progettato a margine di un'analisi dei predetti rischi e modificato successivamente sulla base delle linee guida indicate dalle autorità del sottore.

L'articolo 35 del Regolamento n. 2016/679/UE (GDPR) è stato strutturato sulla matrice giuridico-umanistica prevalente in Giurisprudenza che ha portato prima ad una precisa estrinsecazione del diritto alla riservatezza, concretizzandosi ed evolvendosi previa una puntuale indicazione e previsione normativa in seno alla Convenzione di Nizza del diritto alla riservatezza e del diritto all'obblio.

In ragione di quanto sopra l'analisi del regolamento Ue 679/2016 alla luce dell'evoluzione normativa di matrice Europea che vede una rafforzata tutela dei diritti sopra citati nelle proprie e diverse estrinsecazioni degli stessi.

Giammai dunque sarà sufficiente individuare una mera valutazione dei rischi di "violazione dei dati" che ciascun trattamento può eventualmente presentare, ma risulterà indispensabile una progettazione ed analisi costante delle criticità a margine ed in seno al trattamento del dato personale e sensibile.

In tal senso il registro di classificazione risulta elemento utile per la verifica della presenza dei fattori di rischio ma la cui efficienza è comunque vincolata allo svolgimento di audit di controllo previo tracciamento dei dati personali e sensibili.

Il significato del termine "protezione dei dati personali", non equivale a "sicurezza dei dati personali" ma bensì si suole indicare la necessaria tutela di qual si voglia elemento essenziale dell'essere umano, cioè va inteso – e così è palesemente inteso dal legislatore europeo sin dai Trattati – come diritto fondamentale strumentale alla tutela di altri diritti e libertà fondamentali. (Carta di Nizza)

È indispensabile dunque come che una Valutazione d'Impatto ex art. 35 GDPR, dopo avere smarcato la due diligence di conformità normativa dello specifico trattamento, comprenda due fasi di analisi:

1. Una prima fase, nella quale si si ricercano i possibili rischi "patologici" incombenti sui dati personali oggetto di trattamento, cioè in sostanza i gradi di severità e di probabilità che si verifichino "violazioni dei dati" come definite all'art. 4 GDPR *("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");

2. Una seconda fase, in cui valutare i rischi per i diritti e le libertà delle persone fisiche comportati:

a) dal trattamento in sé, implicitamente anche in assenza di violazioni dei dati (situazione fisiologica);

b) dalla violazione dei dati (situazione patologica).

Solo a valle di questa duplice valutazione operata nella seconda fase, e comprendente non solo la casistica patologica di data breach ma anche e soprattutto, per la ratio dell'art. 35, la carica intrinseca di potenziale impatto negativo sui diritti e le libertà delle persone di quel trattamento in sé, sarà possibile andare a individuare misure di mitigazione più o meno mirate ed efficaci.

Nella prima fase è stata quindi verificata la probabilità e severità di possibili problemi patologici (analisi dei rischi di violazione dei dati).

Nella seconda fase di analisi, trattamento che in sé può comportare rischi elevati per i diritti e le libertà delle persone fisiche.

(Art.7-11-35) Se necessario, il Titolare del Trattamento previo l'ausilio delle competenze degli incaricati procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.

MISURE DI PREVENZIONE

TRATTAMENTI DEI DATI PREVIO UTILIZZO DI STRUMENTI ELETTRONICI

Il processo di trattamento di dati personali viene effettuato con strumenti elettronici ed in presenza delle misure preventive sotto indicate:

A) autenticazione informatica;

B) adozione di procedure di gestione delle credenziali di autenticazione;

C) utilizzazione di un sistema di autorizzazione;

D) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici.

E) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non

consentiti e a determinati programmi informatici coadiuvato dal sistema di monitoraggio da remoto nella disponibilità del Dpo e dei Sub responsabili.

F) L’adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi:

I trattamenti dei dati personali effettuati per finalità amministrativo-contabili risultano, in seno alla predetta struttura organizzativa, connessi allo svolgimento delle attività di natura organizzativa, amministrativa, finanziaria e contabile, ed operativa a prescindere dalla classificazione operata dei dati sensibili e dunque oggetto di analisi preventiva delle possibili criticità presenti in seno al procedimento.

Questi dunque sono trattati nelle modalità sopra esposte ed effettuati per quanto di competenza nella sede organizzativa centrale e nelle diverse aree di coordinamento e/o operative presenti nei punti vendita e nei magazzini.

Oggetto di analisi e verifica risultano infine gli assetti organizzativi posti a presidio e alla salva guardia dei procedimento di trattamento dei dati personali e/o sensibili , e le diverse attività organizzative interne, quelle funzionali all'adempimento di obblighi contrattuali e precontrattuali, alla gestione del rapporto di lavoro in tutte le sue fasi, alla tenuta della contabilità e all'applicazione delle norme in materia fiscale, sindacale, previdenziale-assistenziale, di salute, igiene e sicurezza sul lavoro.

TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;

b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;

c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

ATTUAZIONE DELLE MISURE MINIME DI SICUREZZA

In conformità con il Disciplinare, si riportano di seguito le prescrizioni al fine di dare attuazione nell'ambito aziendale alle "misure minime di sicurezza" nel trattamento dei dati personali di cui al predetto Regolamento UE 679/2016.

SISTEMA DI AUTENTICAZIONE INFORMATICA

E

MISURE CAUTELARI PRELIMINARI

Ciascun incaricato del trattamento dei dati personali :

a) viene dotato, all'atto di presa del servizio, di proprie credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa ai trattamenti che dovrà effettuare. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo.
b) è tenuto ad adottare le necessarie cautele individuate nei rispettivi mansionari a questi forniti per assicurare la segretezza della componente riservata della credenziale, che non dovrà essere divulgata né resa pubblica.
c) La parola chiave dovrà essere composta da almeno otto caratteri.
d) Essa non dovrà contenere riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi.
e) In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
f) Le credenziali di autenticazione non utilizzate da almeno sei mesi vengono disattivate da remoto dai sub responsabili, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
g) Le credenziali verranno disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
h) ha il dovere non lasciare accessibile o incustodita la propria postazione di lavoro informatica, in caso di allontanamento, anche temporaneo.
i) deve fornire copia delle credenziali di accesso all'Amministratore di Sistema onde assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento

dell'incaricato stesso in presenza di circostanze che rendano indispensabile e indifferibile l'intervento per esclusive necessità di operatività e di sicurezza del sistema.

SISTEMI DI AUTORIZZAZIONE

Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso, è utilizzato un sistema di autorizzazione per l'accesso ai dati da trattare.

All'inizio del trattamento il Responsabile per il trattamento dei dati definisce il profilo di autorizzazione per ciascun incaricato, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

La definizione dei profili viene effettuata per iscritto nell'atto di conferimento di incarico al trattamento dati e revisionata con cadenza mensile entro il 24 del mese successivo.

Qualsiasi modifica andrà comunicata per iscritto da parte del Responsabile.

Con cadenza annuale, il Responsabile per il trattamento dei dati verifica la sussistenza delle condizioni per la conservazione dei profili di autorizzazione nei confronti di ciascun incaricato, dando evidenza delle modifiche in apposito verbale.

ALTRE MISURE DI SICUREZZA

I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici (Antivirus) che verranno aggiornati con cadenza almeno semestrale. Vedasi comunque più avanti al paragrafo 5.3.

Ciascuna postazione di lavoro è sottoposta ad aggiornamento almeno annuale allo scopo di verificarne la piena funzionalità ed allo scopo di prevenirne la vulnerabilità da attacchi esterni e consentire la correzione di difetti.

L'Amministratore di Sistema procederà, in ogni caso, a disporre il salvataggio dei dati con frequenza giornaliera (v. più avanti, paragrafo 5.4).

Ulteriori Misure In Caso Di Trattamento dei Dati Sensibili

I dati sensibili e/o giudiziari sottoposti a trattamento sono protetti contro l'accesso abusivo, di cui all'art.615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici che verranno aggiornati con cadenza almeno semestrale. Vedasi comunque più avanti al paragrafo 5.3.

Ciascuna postazione di lavoro di incaricati al trattamento dei dati sensibili e/o giudiziari verrà sottoposta ad aggiornamento almeno semestrale allo scopo di verificarne la piena funzionalità ed allo scopo di prevenirne la vulnerabilità da attacchi esterni e consentire la correzione di difetti.

Il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, verrà effettuato dall'Amministratore di Sistema entro il termine sette giorni.

Misure di tutela e garanzia

Laddove la società **La Casa del sorriso Srl** dovesse ricorrere a soggetti terzi per la messa in opera od esecuzione delle misure minime di sicurezza di cui sopra, il Responsabile per il trattamento dei dati dovrà esigere dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del Disciplinare.

Procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi

La procedura di backup utilizzata da **La Casa del sorriso Srl** è effettuata ogni settimana su un sistema esterno e presso i Server interni con un ripristino potenziale in tempo reale rispetto alla data di conoscenza della perdita dei dati.

TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Il Responsabile per il Trattamento dei dati personale, all'atto del conferimento, impartisce istruzioni scritte agli incaricati finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Quando gli atti e i documenti contenenti dati personali sensibili, riportanti documentazione medica o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate. Vedasi anche più avanti, ai paragrafi 5.7e 5.8.

L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato attraverso il procedimento di monitoraggio in adozione sin dal 24.04.2018.

Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate.

Le persone che accedono ai suddetti archivi vanno preventivamente autorizzate dal Responsabile del trattamento dei dati personali.

Di seguito vengono descritte le norme a cui gli Incaricati devono attenersi nell'esecuzione dei compiti che implicano un trattamento di dati personali riferiti sia a persone fisiche che giuridiche.

Preliminarmente va evidenziato che, al fine di evitare che soggetti estranei possano venire a conoscenza dei dati personali oggetto del trattamento, l'Incaricato 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 Reg Ue 679/2016 :

a) tutte le operazioni di trattamento devono essere effettuate in modo tale da garantire il rispetto delle misure di sicurezza, la massima riservatezza delle informazioni di cui si viene in possesso considerando tutti i dati confidenziali e, di norma, soggetti al segreto d'ufficio;
b) e 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;
c) in caso di allontanamento, anche temporaneo, dalla propria postazione di lavoro si devono porre in essere tutte le misure necessarie (es. blocco del pc) affinché soggetti terzi, anche se dipendenti, non possano accedere ai dati personali per i quali era in corso un qualunque tipo di trattamento, sia esso cartaceo che automatizzato;
d) non devono essere eseguite operazioni di trattamento per fini non previsti tra i compiti assegnati dal diretto responsabile;
e) devono essere svolte le sole operazioni di trattamento necessarie per il raggiungimento dei fini per i quali i dati sono stati raccolti;
f) deve essere costantemente verificata l'esattezza dei dati trattati e la pertinenza rispetto alle finalità perseguite nei singoli casi.

Quanto sopra descritto impone, in altri termini, di operare con la massima attenzione in tutte le fasi di trattamento, dalla esatta acquisizione dei dati, al loro aggiornamento, alla conservazione ed eventuale distruzione.

Nei successivi paragrafi si riportano le procedure di attuazione che gli Incaricati devono adottare sia che trattino dati in formato elettronico che cartaceo.

ACCESSO AI DATI DALLA POSTAZIONE DI LAVORO

La postazione di lavoro deve essere:

• utilizzata solo per scopi legati alla propria attività lavorativa;

• utilizzata in modo esclusivo da un solo utente;

• protetta, evitando che terzi possano accedere ai dati che si sta trattando.

Occorre, inoltre, evidenziare come sia dovere dell'Incaricato:

• non utilizzare in Azienda risorse informatiche private (PC, periferiche, token, ecc…);

• non installare alcun software;

• non lasciare sulla scrivania informazioni riservate su qualunque supporto esse siano archiviate (carta, CD, pen-drive);

• richiamare le funzioni di sicurezza del sistema operativo (con la sequenza dei tasti CTRL+ALT+CANC) ed assicurarsi della attivazione della funzione Lock Workstation in caso di abbandono momentaneo del proprio PC o, in alternativa, impostare lo screen saver con password in modo che si attivi dopo max. 5 minuti di inattività;

• 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);

• non lasciare incustoditi cellulari e palmari;

• non utilizzare fax e/o telefono per trasmettere informazioni riservate e personali se non si è assolutamente certi dell'identità dell'interlocutore o del destinatario e se esso non è legittimato a riceverle.

GESTIONE DELLE PASSWORD

Per una corretta gestione delle password, ciascun Incaricato deve aver cura di:

• modificare, alla prima connessione, quella che ha attribuito di default;

• cambiarla almeno ogni 60 giorni, o immediatamente nei casi in cui sia compromessa;

• comporla utilizzando almeno 8 caratteri o, nel caso in cui lo strumento elettronico non lo consenta, con un numero di caratteri pari al massimo consentito;

• usare sia lettere che numeri e almeno un carattere maiuscolo;

• non basare la scelta su informazioni facilmente deducibili quali, ad esempio, il proprio nome, il nome dei propri familiari, le date di nascita, i codici fiscali, ecc.,

• mantenerla riservata e non divulgarla a terzi;

• non permettere ad altri utenti (es. colleghi) di operare con il proprio identificativo utente;

• non trascriverla su supporti (es. fogli, post-it) facilmente accessibili a terzi, né lasciarla memorizzata sul proprio PC;

• non comunicarla mai per telefono salvo gravi necessità.

ANTIVIRUS

I Personal Computer (PC) in dotazione agli utenti, pur protetti contro gli attacchi dei virus informatici mediante appositi programmi, rimangono potenzialmente esposti ad aggressioni di virus non conosciuti.

Per ridurre le probabilità del verificarsi di tali attacchi è necessario che vengano osservate le seguenti regole:

• controllare che il programma antivirus installato sia aggiornato periodicamente e sia attivo;

• chiudere correttamente i programmi in uso;

• non aprire, se si lavora in rete, files sospetti e di dubbia provenienza;

• non scaricare o installare applicazioni/software che non siano state preventivamente approvate e autorizzate;

• 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;

• non utilizzare CD-Rom o altri supporti elettronici di provenienza incerta;

• porre la necessaria attenzione sui risultati delle elaborazioni effettuate e sulle eventuali segnalazioni anomale inviate dal PC;

• usare correttamente e solo per esigenze di lavoro i servizi di posta elettronica e di Internet;

• non modificare le configurazioni impostate sul proprio PC;

• spegnere il PC al termine della giornata di lavoro;

Alla verifica di un malfunzionamento del PC, che può far sospettare la presenza di un virus, è bene che l'Incaricato:

a. sospenda ogni operazione sul PC evitando di lavorare con il sistema infetto;

b. contatti immediatamente;

c. chiuda il sistema e le relative applicazioni.

SALVATAGGIO DEI DATI

Tutti i dati al termine della giornata lavorativa vanno salvati sul server aziendale. A tale riguardo, qualora vi sia la necessità, l'Incaricato può richiedere la creazione sul server di una cartella a lui intestata o, in alternativa, di una cartella condivisa dal gruppo di lavoro cui fa riferimento l'Incaricato stesso.

PROTEZIONE DEI PC PORTATILI

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;

• essere sempre ben consapevole delle informazioni archiviate sul portatile il quale è maggiormente soggetto a furto e smarrimento rispetto alla postazione fissa;

• operare sempre nella massima riservatezza quando si utilizza il PC portatile in pubblico: i dati, ed in particolare le password, potrebbero essere intercettati da osservatori indiscreti.

USO DI INTERNET E POSTA ELETTRONICA

Gli strumenti di comunicazione telematica (Internet e Posta elettronica) devono essere utilizzati solo ed esclusivamente per finalità lavorative. Sono vietati comportamenti che possano arrecare danno all'Azienda.

In particolare, l'pazientedovrà osservare le seguenti regole:

- è consentita la navigazione internet solo in siti attinenti e necessari per lo svolgimento delle mansioni assegnate;
- non è consentito scaricare software gratuiti (freeware o shareware) prelevati da siti Internet;
- non è consentita la registrazione a siti internet o partecipare a Forum di discussione se questo non è strettamente necessario per lo svolgimento della propria attività lavorativa;
- non è consentito l'utilizzo funzioni di instant messaging a meno che autorizzate dall' Area IT;

- è vietato aprire e-mail e file allegati di origine sconosciuta o che presentino degli aspetti anomali (quali ad esempio, un soggetto non chiaro);
- 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;
- è vietato l'utilizzo della posta elettronica per comunicare informazioni riservate, dati personali o 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;
- occorre sempre essere consapevoli che posta elettronica e navigazione internet sono veicoli per l'introduzione sulla propria macchina (e quindi in azienda) di virus e altri elementi potenzialmente dannosi;
- è consentito solo l'utilizzo dei programmi ufficialmente installati;
- è vietato installare autonomamente programmi, sussistendo infatti il grave pericolo di introdurre virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti, di violare la legge sul diritto d'autore non disponendo delle apposite licenze d'uso acquistate dall'Azienda;
- 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 o 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);
- 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.
- va sempre prestata la massima attenzione nell'utilizzo dei supporti di origine esterna (per es. chiavi USB, dischi esterni ecc.), avvertendo immediatamente l'Amministratore di sistema nel caso in cui siano rilevati virus.

L’paziente(incaricato, collaboratore o dipendente) in caso di assenza programmata (ad esempio per ferie o attività di lavoro fuori sede) - di almeno 5 giornate lavorative - deve attivare l’apposita funzionalità di sistema (cd. “Fuori Sede”) che consente di inviare automaticamente ai mittenti un messaggio di risposta contenente le “coordinate” (anche elettroniche o telefoniche) di un altro pazienteo altre modalità utili di contatto della struttura.

L’azienda, in caso di assenza improvvisa o prolungata dell’pazienteo comunque non programmata e per improrogabili necessità di sicurezza o di operatività del sistema, si riserva, per mezzo dell’Amministratore di Sistema e Responsabile sistemi, di accedere alla casella di posta elettronica dell’pazienteassente: per i dettagli si rimanda al paragrafo 5 “Accesso ai dati dell’utente”.

PARTICOLARI CAUTELE NELLA PREDISPOSIZIONE DEI MESSAGGI DI POSTA ELETTRONICA

Nell’utilizzo della posta elettronica ciascun pazientedeve 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.

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

L’Azienda formula inoltre le seguenti regole di comportamento a cui gli utenti devono attenersi:

a) conservare le comunicazioni inviate o ricevute, in particolare quelle dalle quali si possano desumere impegni e/o indicazioni operative provenienti dalla Committenza pubblica;

b) 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 gli utenti 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 o cliccare sui “link” eventualmente presenti,
- cancellare il messaggio e svuotare il “cestino” della posta,
- segnalare l’accaduto all’Amministratore di Sistema;

c) 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;

d) in caso di iscrizione a servizi informativi accessibili via internet ovvero a servizi di editoria on line, 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,
- in caso di appesantimento dovuto ad un eccessivo traffico di messaggi scambiati attraverso la lista di distribuzione, revocare l'adesione alla stessa. Si raccomanda, in proposito, di approfondire al momento dell'iscrizione le modalità per richiederne la revoca.

e) 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;

f) evitare di predisporre messaggi che contengano materiali che violino la legge sul diritto d'autore, o altri diritti di proprietà intellettuale o industriale.

TRASMISSIONE E RIPRODUZIONE DEI DOCUMENTI

Al fine di prevenire eventuali accessi ai dati aziendali da parte di soggetti terzi non autorizzati, occorre adottare delle cautele nella trasmissione e riproduzione dei documenti contenenti dati personali.

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'informazione, con ciò accertandosi della identità dichiarata in precedenza.

Quando il dato deve essere inviato a mezzo fax, posta elettronica, SMS, ecc. e, in particolar modo, nel caso in cui vengano inviati documenti contenenti dati sensibili 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;

• nel caso di documenti inviati per posta elettronica accertarsi, prima di confermare l'invio, di avere allegato il file giusto;

• in caso di trasmissione di dati particolarmente delicati è opportuno anticipare l'invio 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.

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.

ARCHIVI CARTACEI

Tutto il materiale cartaceo contenente dati personali non deve essere lasciato incustodito sulle scrivanie e, a fine lavoro, 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.

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 in caso di allontanamento, anche temporaneo, dalla postazione di lavoro.

L’accesso a tutti i locali aziendali deve essere consentito solo a personale preventivamente autorizzato dalla Titolarità.

ACCESSO AI DATI DELL’UTENTE

L’Amministratore di Sistema può accedere ai dati trattati dall’pazientetramite posta elettronica o navigazione 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 manutentivi e/o di regolare svolgimento dell’attività lavorativa (ad esempio, aggiornamento/sostituzione/implementazione 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 dell’pazientee/o previo avviso al medesimo.

Ove sia necessario per garantire la sicurezza, l’assistenza tecnica e la normale attività operativa, il personale incaricato avrà anche la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni.

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 dell’pazienteo comunque non programmata e per improrogabili necessità di sicurezza o di operatività del sistema è abilitato ad accedere alla posta elettronica dell’pazienteper le strette necessità operative. Di tale avvenuto accesso dovrà comunque essere data tempestiva comunicazione all’utente.

L’Amministratore di Sistema può procedere a controlli sulla navigazione finalizzati a garantire l’operatività 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.

Il sistema di registrazione dei log è configurato per cancellare periodicamente ed automaticamente (attraverso procedure di sovra registrazione) i dati personali degli utenti relativi agli accessi internet e al traffico telematico.

L'Amministratore di Sistema è altresì abilitato ad accedere ai dati contenuti negli strumenti informatici restituiti dall'pazienteall'azienda per cessazione del rapporto, sostituzione delle apparecchiature, etc.

Sarà cura dell'pazientela cancellazione preventiva di tutti gli eventuali dati personali eventualmente ivi

contenuti.

In ogni caso, **La Casa del sorriso Srl**. 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;

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

• lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo.

CONTROLLI DA PARTE DELLA TITOLARITA'

Con il presente capitolo portiamo all'attenzione degli incaricati la possibilità di questa Azienda di effettuare controlli sulle proprie apparecchiature tecnologiche al fine di preservare la sicurezza informatica dei dati personali in esse contenuti.

A tale proposito si sottolinea che la strumentazione tecnologica/informatica e quanto con essa creato è di proprietà dell'Azienda in quanto mezzo di lavoro. E' pertanto fatto divieto di utilizzo del mezzo tecnologico/informatico e delle trasmissioni interne ed esterne con esso effettuate per fini ed interessi non strettamente coincidenti con quelli dell'Azienda stessa.

Nel rispetto dei principi di pertinenza e non eccedenza, le verifiche sugli strumenti informatici saranno realizzati dall'Azienda nel pieno rispetto dei diritti e delle libertà fondamentali degli utenti e del presente Regolamento.

In caso di anomalie, l'Azienda, 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.

In tali casi, il controllo si concluderà con un avviso al Responsabile della struttura dell'Area aziendale interessata in cui è stato rilevato l'utilizzo anomalo degli strumenti aziendali affinché lo stesso inviti le Strutture da lui dipendenti ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

In caso di successive, perduranti anomalie, ovvero ravvisandone comunque la necessità, l'Azienda 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 o indiscriminate, fatte salve le verifiche atte a tutelare gli interessi aziendali.

RESPONSABILITÀ E SANZIONI

L'utente, al fine di non esporre sé stesso e l'Azienda a rischi sanzionatori, è tenuto ad adottare comportamenti puntualmente conformi alla normativa vigente ed alla regolamentazione aziendale.

Gli utenti sono responsabili del corretto utilizzo dei servizi di Internet e Posta Elettronica. Pertanto sono responsabili per i danni cagionati al patrimonio, alla reputazione e alla Committenza.

Tutti gli utenti sono pertanto tenuti ad osservare e a far osservare le disposizioni contenute nel presente Regolamento Disciplinare 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 tempo per tempo vigente, le azioni civili e penali stabilite dalle leggi tempo per tempo vigenti;
- per i collaboratori esterni oltre che la risoluzione del contratto le azioni civili e penali stabilite dalle leggi tempo per tempo vigenti.

Diritto legittimo- Esercizio del diritto all'obblio - opposizione al trattamento dei dati personali -

I criteri e la verifica della presenza di un diritto legittimo al trattamento dei dati personali vengono adottati puntualmente da ogni incaricato con lo standard proprio del buon professionista.

L'incaricato procede alla stampa e alla consegna del documento d'informativa sul trattamento dei dati personali e all'atto della autorizzazione liberamente prestata previa sottoscrizione dello stesso procede all'archiviazione e classificazione e conservazione dello stesso con l'ausilio degli appositi software di gestione.

Nei processi automatizzati, il " Paziente "previo esame del documento contenente l'informativa citata procede alla concessione dell'autorizzazione al trattamento dei dati propri dati personali.

Nella modulistica allegata al presente " disciplinare " vengono espressamente indicate le discipline normative in vigore ed una sintetica esposizione delle modalità d'esercizio dell'interessato a non essere sottoposto ad una decisione basata unicamente su un trattamento automatizzato dei dati che produca effetti giuridici che lo riguardano o che comunque incida significativamente sulla sua persona (tra le operazioni contemplate dalla norma campeggia la profilazione come definita dall'art. 4.1, n. 4).

Le modalità d'esercizio al "diritto all'oblio" e alla cancellazione dei dati personali forniti ed infine le modalità d'esercizio di opposizione nanti le autorità competenti sono espressamente indicate nello stesso documento teste citato.

Visualizzazione di contenuti da piattaforme esterne.

Questo tipo di servizi permette di visualizzare contenuti ospitati su piattaforme esterne direttamente dalle pagine di questo Sito Web e di interagire con essi.

Nel caso in cui sia installato un servizio di questo tipo, è possibile che, anche nel caso gli Utenti non utilizzino il servizio, lo stesso raccolga dati di traffico relativi alle pagine in cui è installato.

Google Fonts (Google Inc.)

Google Fonts è un servizio di visualizzazione di stili di carattere gestito da Google Inc. che permette a questo Sito Web di integrare tali contenuti all'interno delle proprie pagine.

Dati Personali raccolti: Dati di utilizzo e varie tipologie di Dati secondo quanto specificato dalla privacy policy del servizio.

Luogo del trattamento: Stati Uniti – Privacy Policy. Soggetto aderente al Privacy Shield.

Diritti dell'Utente

Gli Utenti possono esercitare determinati diritti con riferimento ai Dati trattati dal Titolare.

L'Pazienteha diritto ad ottenere informazioni sui Dati trattati dal Titolare, su determinati aspetti del trattamento ed a ricevere una copia dei Dati trattati.

- verificare e chiedere la rettificazione.
- verificare la correttezza dei propri Dati e richiederne l'aggiornamento o la correzione.
- ottenere la limitazione del trattamento.
- quando ricorrono determinate condizioni, l'Pazientepuò richiedere la limitazione del trattamento dei propri Dati. In tal caso il Titolare non tratterà i Dati per alcun altro scopo se non la loro conservazione.
- ottenere la cancellazione o rimozione dei propri Dati Personali. Quando ricorrono determinate condizioni, l'Pazientepuò richiedere la cancellazione dei propri Dati da parte del Titolare.
- ricevere i propri Dati o farli trasferire ad altro titolare. L'Pazienteha diritto di ricevere i propri Dati in formato strutturato, di uso comune e leggibile da dispositivo automatico e, ove tecnicamente fattibile, di ottenerne il trasferimento senza ostacoli ad un altro titolare. Questa disposizione è applicabile quando i Dati sono trattati con strumenti automatizzati ed il trattamento è basato sul consenso dell'Utente, su un contratto di cui l'Pazienteè parte o su misure contrattuali ad esso connesse.
- L'Pazientepuò proporre un reclamo all'autorità di controllo della protezione dei dati personali competente o agire in sede giudiziale.

Dettagli sul diritto di opposizione

Quando i Dati Personali sono trattati nell'interesse pubblico, nell'esercizio di pubblici poteri di cui è investito il Titolare oppure per perseguire un interesse legittimo del Titolare, gli Utenti hanno diritto ad opporsi al trattamento per motivi connessi alla loro situazione particolare.

Si fa presente agli Utenti che, ove i loro Dati fossero trattati con finalità di marketing diretto, possono opporsi al trattamento senza fornire alcuna motivazione. Per scoprire se il Titolare tratti dati con finalità di marketing diretto gli Utenti possono fare riferimento alle rispettive sezioni di questo documento.

Modalità esercizio diritti

Per esercitare i diritti dell'Utente, gli Utenti possono indirizzare una richiesta agli estremi di contatto del Titolare indicati in questo documento.

Le richieste sono depositate a titolo gratuito e evase dal Titolare nel più breve tempo possibile, in ogni caso entro 60 giorni .

Cookie Policy

Questo Sito Web fa utilizzo di Cookie. Per saperne di più e per prendere visione dell'informativa dettagliata, il Paziente può consultare la Cookie Policy.

Ulteriori informazioni sul trattamento

Difesa in giudizio

I Dati Personali del paziente possono essere utilizzati da parte del Titolare in giudizio o nelle fasi preparatorie alla sua eventuale instaurazione per la difesa da abusi nell'utilizzo di questo Sito Web o dei Servizi connessi da parte dell'utente.

Il Paziente dichiara di essere consapevole che il Titolare potrebbe essere obbligato a rivelare i Dati per ordine delle autorità pubbliche.

Informative specifiche

Su richiesta del Paziente, in aggiunta alle informazioni contenute in questa privacy policy, questo Sito Web potrebbe fornire al Paziente delle informative aggiuntive e contestuali riguardanti Servizi specifici, o la raccolta ed il trattamento di Dati Personali.

Log di sistema e manutenzione

Per necessità legate al funzionamento ed alla manutenzione, questo Sito Web e gli eventuali servizi terzi da essa utilizzati potrebbero raccogliere Log di sistema, ossia file che registrano le interazioni e che possono contenere anche Dati Personali, quali l'indirizzo IP Utente.

Informazioni non contenute in questa policy

Ulteriori informazioni in relazione al trattamento dei Dati Personali potranno essere richieste in qualsiasi momento al Titolare del Trattamento utilizzando gli estremi di contatto.

Risposta alle richieste DO Not Track"

Questo Sito Web non supporta le richieste "Do Not Track".

Per verificare se gli eventuali servizi di terze parti utilizzati le supportino, l'Pazienteè invitato a consultare le rispettive privacy policy.

Modifiche privacy policy

Il Titolare del Trattamento si riserva il diritto di apportare modifiche alla presente privacy policy in qualunque momento dandone informazione agli utenti su questa pagina e, se possibile, su questo Sito Web.

Si prega dunque di consultare regolarmente questa pagina, facendo riferimento alla data di ultima modifica indicata in fondo.

Qualora le modifiche interessassero i trattamenti la cui base giuridica è il consenso, il Titolare provvederà a raccogliere nuovamente il consenso dell'Utente, se necessario.

La presente informativa privacy è redatta sulla base di molteplici ordinamenti legislativi e del Regolamento (UE) 2016/679.

Il presente privacy policy è disponibile in ogni sede operativa e di controllo della predetta società e nelle piattaforme Informatiche utilizzata dalla stessa.

Selargius Su Planu 24 maggio 2018