# GDPR

# *- General Data Protection Regulation -*

***(secondo quanto disposto dal Regolamento UE 2016/679)***

**Sicurezza sul trattamento dei dati personali**

Data di emissione: 05/06/2023

MEDICAL TI S.R.L.
Via Ruilio, 18
95126 Catania (CT)
P.iva 02313980878
e-mail: medicalti@medicalti.it

# Sommario

## Premessa

Scopo del presente documento è stabilire le misure di sicurezza organizzative, fisiche e logiche da adottare affinché siano rispettati gli obblighi, in materia di sicurezza del trattamento dei dati personali effettuato da MEDICAL TI S.R.L., secondo quanto previsto dal Regolamento UE 2016/679.

Il presente documento è stato redatto dal Titolare del Trattamento MEDICAL TI S.R.L., in collaborazione con HQ Network Consulting Soc Coop, che provvede a firmarlo in calce.

## Normativa di riferimento

Regolamento UE 2016/679

## Il GDPR - General Data Protection Regulation

Il General Data Protection Regulation è uno strumento per fare fronte all'obbligo, secondo il Regolamento UE 2016/679, relativamente alla sicurezza dei dati personali, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, mediante l'adozione di idonee e preventive misure di sicurezza in modo da ridurre al minimo i rischi di:

a) distruzione o perdita, anche accidentale, dei dati personali (causati ad es. da comandi applicativi/operativi errati, software pericolosi, malfunzionamento dell'hardware, eventi disastrosi);
b) accesso non autorizzato (nel caso in cui i dati siano consultati ad opera di soggetti diversi da quelli preposti oppure siano oggetto di comunicazione/diffusione non consentita);
c) trattamento non consentito o non conforme alle finalità della raccolta (quando il trattamento viene effettuato in violazione delle normative vigenti).

Il Titolare consapevole dell'importanza della sicurezza del sistema informativo, considera il presente Documento uno strumento utile per:

a) formalizzare, razionalizzare e finalizzare le strategie aziendali in materia di sicurezza dei dati;
b) definire opportune strategie per l'informazione e la formazione degli utenti aziendali sugli aspetti della sicurezza dei dati.

Conformemente a quanto previsto dal Regolamento, i dati personali oggetto di trattamento devono essere:

a) trattati in modo lecito e secondo correttezza;
b) raccolti e registrati per scopi determinati, espliciti e legittimi ed utilizzati in altre operazioni del trattamento in termini non incompatibili con tali scopi;
c) esatti e, se necessario, aggiornati;

d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono stati raccolti o successivamente trattati;
e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo definito, necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati. A tal fine, anche con verifiche periodiche, sarà compito del Responsabile del trattamento controllare costantemente la stretta pertinenza e la non eccedenza dei dati rispetto alle esigenze operative e gestionali della prestazione e degli incarichi in corso, da instaurare o cessati.

## Descrizione attività e struttura organizzativa

La MEDICAL TI S.R.L. con Sede Legale in Via Ruilio, 18 Catania (CT) si occupa di commercio all'ingrosso di presidi medico-chirurgici, medicamenti elettromedicali, accessoristica ospedaliera, strumentari, filati, parafarmaceutici, materiali di consumo. L'esecuzione di tutte le operazioni svolte all'interno dell'azienda viene regolata da procedure interne (SOP) redatte in conformità alla Norma UNI EN ISO 9001:2015.

## Elenco dei trattamenti dei dati

Nella tabella di seguito riportata vengono riepilogate tutte le informazioni raccolte dall'organizzazione ed il loro reale utilizzo:

| *TRATTAMENTO* | *NATURA DEI DATI* | *UTILIZZO* |
|---|---|---|
| Dati personale dipendente | Dati comuni | Fini previdenziali |
| Clienti | Dati comuni | Gestione Contabile e Amministrativa |
| Fornitori | Dati comuni | Gestione Contabile e Amministrativa |

Questi dati costituiscono il patrimonio informativo della MEDICAL TI S.R.L.
Le informazioni, di cui si possiede apposita informativa attraverso con la quale l'utente fornisce consenso scritto, vengono trattate e archiviate in apposito sia con l'ausilio di strumenti cartacei sia con strumenti informatici. E' diritto di ogni utente, come disciplinato dal Regolamento UE 679/16, di ottenere dal titolare del trattamento la cancellazione dei dati personali (quando non sono più necessari rispetto alle finalità per le quali sono stati raccolti o trattati). Questo può avvenire in sede di raccolta non concedendo consenso al trattamento dei dati personali, o, anche successivamente attraverso revoca del consenso che deve pervenire per iscritto all'organizzazione.
Al fine di proteggere e migliorare la sicurezza delle informazioni raccolte, che l'utente dichiara espressamente che vengano archiviate per un periodo non superiore ad anni 10 dalla cessazione del rapporto, l'organizzazione ha predisposto un'analisi dei rischi, riportata nella sezione successiva.
Lo scopo di quest'ultima è quantificare e qualificare il rischio associato ad una situazione ben definita o ad una minaccia conosciuta (pericolo), e di rendere il personale coinvolto pronto ad intervenire per l'adozione di una azione correttiva.

## Analisi dei Rischi

L'analisi dei rischi consente di acquisire consapevolezza e visibilità sul livello di esposizione al rischio del proprio patrimonio informativo e avere una mappa preliminare dell'insieme delle possibili contromisure di sicurezza da realizzare.

L'analisi dei rischi consiste nella:

1. individuazione di tutte le risorse del patrimonio informativo;
2. identificazione delle minacce a cui tali risorse sono sottoposte;
3. identificazione delle vulnerabilità;
4. definizione delle relative contromisure.

I dati personali trattati sono:

a) Dati comuni (qualsiasi informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale);
b) Dati idonei a rivelare lo stato di salute.

Il GDPR si applica al trattamento di tutti i dati personali effettuato a mezzo di:

1. Strumenti elettronici di elaborazione;
2. altri strumenti di elaborazione (cartacei).

L'analisi è stata effettuata mediante l'implementazione di una **Matrice dei rischi,** al fine di individuare
- la minaccia: evento che potrebbe compromettere la sicurezza del dato trattato;
- la vulnerabilità: falla che può consentire la riduzione del livello di sicurezza dei dati trattati;
- il danno: conseguenza derivante dalla realizzazione della minaccia;
- le contromisure: provvedimento diretto a prevenire o neutralizzare azioni o situazioni dannose o comunque pericolose.

| *MATRICE DEI RISCHI PER I TRATTAMENTI INFORMATICI E CARTACEI* | | | |
|---|---|---|---|
| **MINACCIA** | **VULNERABILITÀ** | **DANNO** | **CONTROMISURE** |
| Furto di credenziali di autenticazione | Personale non formato<br>Strumenti non conformi | Accesso o trattamento da parte di soggetti non autorizzati; perdita totale o parziale dei dati; alterazione delle informazioni | Formazione del personale<br>Adeguamento periodico parco macchine<br>Aggiornamento dei sistemi operativi |
| Carenza di consapevolezza, disattenzione o incuria | Personale non formato | Accesso o trattamento da parte di soggetti non autorizzati | Formazione del personale sulle regole relative al trattamento e alla protezione dei dati |
| Comportamenti sleali o fraudolenti | Accesso indesiderato alle postazioni o ai server, fisicamente o per mezzo della rete | Perdita totale o parziale dei dati; accesso o trattamento da parte di soggetti non autorizzati; asportazione o blocco operativo, perdita dell'integrità, decadimento delle prestazioni del sistema | Formazione del personale sulle regole relative al trattamento e alla protezione dei dati |
| Errore Materiale | Personale non formato;<br>Software non certificato;<br>Assenza di backup;<br>Strumenti non conformi | Perdita totale o parziale dei dati; alterazione delle informazioni; accesso o trattamento da parte di soggetti non autorizzati | Formazione del personale sulle regole relative al trattamento e alla protezione dei dati<br>Verifica Backup |
| Azione di virus informatici | Antivirus non aggiornato<br>Comportamenti scorretti | Perdita totale o parziale dei dati; accesso o trattamento da parte di soggetti non autorizzati | Formazione del personale<br>Aggiornamento dei sistemi operativi e antivirus |
| Spamming o altre tecniche di sabotaggio | Antivirus non aggiornato.<br>Comportamenti scorretti | Perdita totale o parziale dei dati; accesso o trattamento da parte di soggetti non autorizzati | Formazione del personale<br>Aggiornamento dei sistemi operativi e antivirus |
| Malfunzionamento, indisponibilità o degrado degli strumenti | Risorse obsolete, strumenti non conformi, impianti elettrici non a norma. | Perdita totale o parziale dei dati; blocco operativo e perdita dell'integrità della banca dati | Adeguamento periodico parco macchine<br>Verifica Impianti<br>Aggiornamento dei sistemi operativi |

| | | | |
|---|---|---|---|
| Accessi esterni non autorizzati | Accessi non controllati | Perdita totale o parziale dei dati; accesso o trattamento da parte di soggetti non autorizzati; asportazione o alterazione delle informazioni | Firewall aggiornato<br>Anti virus con aggiornamento automatico |
| Intercettazione di informazioni in rete | Accessi non controllati | Perdita totale o parziale dei dati; accesso o trattamento da parte di soggetti non autorizzati; asportazione o alterazione delle informazioni | Firewall aggiornato<br>Anti virus con aggiornamento automatico |
| Accessi non autorizzati a locali/reparti ad accesso ristretto | Accessi non controllati | Perdita totale o parziale dei dati; accesso o trattamento da parte di soggetti non autorizzati; asportazione o alterazione delle informazioni | Sistema di video sorveglianza<br>Sistemi operativi con blocco psw |
| Asportazione e furto di strumenti contenenti dati | Accessi controllati | Perdita totale o parziale dei dati; accesso o trattamento da parte di soggetti non autorizzati; asportazione o alterazione delle informazioni | Sistema di video sorveglianza<br>Sistemi operativi con blocco psw |
| Guasto ai sistemi complementari (impianto elettrico, idrico, climatizzazione, ecc.) | Mancanza manutenzione | Perdita totale o parziale dei dati | Interventi di manutenzione programmata |
| Errori umani nella gestione della sicurezza fisica | Personale non formato | Perdita totale o parziale dei dati | Formazione del personale |

Dall'analisi è emerso che le principali 'fonti' di rischio sono:

a) comportamento degli operatori;
b) eventi relativi agli strumenti;
c) eventi relativi al contesto.

Successivamente si è valutata la possibilità che il rischio evidenziato potesse avverarsi (SI/NO) e nel caso in cui vi è la possibilità di accadimento se ne è descritto l'impatto sulla sicurezza (stimato in: alta/media/bassa)
Sono state, quindi, individuate le Misure d'azione per contrastare il rischio.

| *MISURE D'INTERVENTO* | | | | |
|---|---|---|---|---|
| **FONTE DEL RISCHIO** | **RISCHI** | **SI/NO** | **DESCRIZIONE DELL'IMPATTO SULLA SICUREZZA gravità stimata: alta/media/bassa** | **Misure di Intervento** |
| Comportamento degli operatori | Uso improprio delle credenziali aziendali | SI | Medio | Blocco account |
| | Carenza di consapevolezza, disattenzione o incuria | SI | Medio | Richiamo |
| | Comportamenti sleali o fraudolenti | SI | Medio | Allontanamento |
| | Errore Materiale | SI | Bassa | Recupero da backup dati persi |
| Eventi relativi agli strumenti | Azione di virus informatici | SI | Medio | Antivirus aggiornato |
| | Spamming o altre tecniche di sabotaggio | SI | Bassa | Strumenti di controllo e correzione |
| | Malfunzionamento, indisponibilità o degrado degli strumenti | SI | Bassa | Interventi di supporto/manutenzione e sostituzione attrezzatura |
| | Accessi esterni non autorizzati | SI | Bassa | Firewall aziendale |
| | Intercettazione di informazioni in rete | SI | Bassa | Antivirus aggiornato |
| Eventi relativi al contesto | Accessi non autorizzati a locali/reparti ad accesso ristretto | SI | Medio | Sistemi di videosorveglianza e blocco sistemi con user e psw |
| | Asportazione e furto di strumenti contenenti dati | SI | Basso | Sistemi di videosorveglianza e blocco sistemi con user e psw |
| | Guasto ai sistemi complementari (impianto elettrico, idrico, ecc.) | SI | Medio | Interventi di supporto/manutenzione e sostituzione attrezzatura |
| | Errori umani nella gestione della sicurezza dati | SI | Medio | Personale formato |

L'analisi svolta da consapevolezza di quelle che sono le minacce rilevate e quelle che sono le misure di intervento da adottare, riportate nel prossimo paragrafo. Sarà compito del responsabile al trattamento vigilare sull'effettiva adozione di queste misure.

## Individuazione delle misure d'intervento

Si tratta di azioni che si propongono il fine di annullare o di limitare le vulnerabilità e di contrastare le minacce, esse sono classificabili nelle seguenti tre categorie:

- misure di carattere fisico;
- misure di carattere procedurale;
- misure di carattere elettronico/informatico.

### Misure di carattere fisico

- le apparecchiature informatiche critiche (server di rete) e gli archivi cartacei contenenti dati personali sono situati in locali ad accesso controllato;
- i locali ad accesso sono chiusi, controllati e videosorveglianti;
- l'ingresso ai locali ad accesso controllato è possibile solo dall'interno dell'area sotto la responsabilità del'incaricato preposto;
- i locali sono provvisti di sistema di allarme e di estintore;
- sono programmati interventi periodici di manutenzione nei locali ad accesso controllato.

### Misure di carattere procedurale

- L'ingresso nei locali ad accesso controllato è consentito solo alle persone autorizzate;
- il responsabile dell'area ad accesso controllato deve mantenere un effettivo controllo sull'area di sua responsabilità;
- i visitatori occasionali delle aree ad accesso controllato sono accompagnati da un incaricato;
- è controllata l'attuazione del piano di verifica periodica sull'efficacia degli allarmi e degli estintori;
- l'ingresso in locali ad accesso controllato da parte di dipendenti o estranei per operazioni di pulizia o di manutenzione avviene se le operazioni si svolgono alla presenza dell'Incaricato del trattamento di tali dati;
- il protocollo riservato, accessibile solo al Titolare e al Responsabile del trattamento è conservato nei server aziendali e copia cartacea, presso gli uffici aziendali. E' disponibile, previa autorizzazione, a chiunque ne richieda visione.

### Misure di carattere elettronico/informatico

- Presenza di gruppi di continuità elettrica per il server;
- attivazione di un sistema di backup centralizzato e automatizzato con periodicità giornaliera;
- installazione di un sistema antivirus su tutte le postazioni di lavoro, configurato per controllare la posta in ingresso, la posta in uscita, per eseguire la procedura di aggiornamento in automatico con frequenza giornaliera e la scansione periodica dei supporti di memoria;

Per gli elaboratori che ospitano archivi (o hanno accesso tramite la rete) con dati personali sono adottate le seguenti misure:

- l'accesso agli incaricati ed agli addetti alla manutenzione è possibile solo in seguito ad autorizzazione;
- Tutti gli incaricati del trattamento dei dati personali accedono al sistema informativo per mezzo di un codice identificativo personale (in seguito indicato User-id) e password personale.
- le copie di backup realizzate su Nas che viene effettuata ogni 15 minuti;
- per evitare errori e dimenticanze, è adottato uno screensaver automatico dopo 10 minuti di non utilizzo, con ulteriore password segreta per la prosecuzione del lavoro;
- divieto di memorizzazione di archivi con dati sensibili di carattere personale dell'utente sulla propria postazione di lavoro non inerenti alla funzione svolta;
- divieto di installazione di software di qualsiasi tipo sui personal computer che contengono archivi con dati sensibili senza apposita autorizzazione scritta da parte del responsabile del trattamento dati;

Per minimizzare il rischio da virus informatici, gli utilizzatori dei PC adottano le seguenti regole:

- controllare (scansionare con un antivirus aggiornato) qualsiasi supporto di provenienza sospetta prima di operare su uno qualsiasi dei file in esso contenuti;
- evitare l'uso di programmi shareware e di pubblico dominio se non se ne conosce la provenienza, ovvero divieto di "scaricare" dalla rete internet ogni sorta di file, eseguibile e non. La decisione di "scaricare" può essere presa solo dal responsabile del trattamento;
- attivare la protezione massima per gli utenti del programma di posta Outlook Express al fine di proteggersi dal codice html di certi messaggi e-mail (buona norma è visualizzare e trasmettere messaggi in formato testo poiché alcune pagine web, per il solo fatto di essere visualizzate possono infettare il computer);
- non aprire gli allegati di posta se non si è certi della loro provenienza, e in ogni caso analizzarli con un software antivirus;
- non cliccare mai un link presente in un messaggio di posta elettronica da provenienza sconosciuta;
- avvisare l'Amministratore di sistema nel caso in cui il virus sia stato scoperto solo dopo aver subito svariati malfunzionamenti della rete o di qualche PC, ovvero in ritardo;
- La manutenzione degli elaboratori, che può eventualmente prevedere il trasferimento fisico presso un laboratorio riparazioni, è autorizzata solo a condizione che il fornitore del servizio dichiari per iscritto di avere redatto il GDPR e di aver adottato le misure minime di sicurezza previste dal disciplinare.

## Data Breach

L'organizzazione, così come previsto dal Regolamento UE 679/16, comunicherà entro 72 ore eventuali violazioni dei dati personali (data breach) dei propri utenti, all'Autorità nazionale di protezione dei dati (Autorità di controllo).
Se la violazione dei dati rappresenta una minaccia grave per i diritti e le libertà delle persone, l'organizzazione dovrà informare in modo chiaro, semplice e immediato anche tutti gli interessati e offrire indicazioni/suggerimenti su come limitare eventuali conseguenze negative.

## Titolare, responsabili, incaricati

**Titolare del trattamento:** è la persona fisica, giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza. È onere del Titolare del trattamento, qualora lo ritenesse opportuno, individuare, nominare e incaricare per iscritto uno o più Responsabili del trattamento dei dati. Il titolare, a tal proposito, redigerà apposita lettera di incarico, che dovrà essere sottoscritta per accettazione dal responsabile.
È cura del titolare del trattamento vigilare sull'operato del responsabile del trattamento e verificare che le misure di sicurezza disposte vengano attuate.
Nel caso di specie, il Titolare al Trattamento è la società MEDICAL TI S.P.A. nella figura del suo Legale Rappresentante.

**Responsabile del titolare del trattamento**: la persona fisica o giuridica, l'autorità pubblica o altro organismo che tratta dati personali per conto del titolare. Secondo quanto disposto dall'art. 24 del Regolamento UE 679/16, deve mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario. L'organizzazione a seconda del tipo di trattamento e delle finalità del trattamento che viene effettuato per conto del Titolare può nominare uno o più Responsabili del trattamento.
Nel caso di specie, i Responsabili al trattamento sono:

- sig.ra Rossella Tirendi, per il trattamento dei dati costituenti il patrimonio informativo del Titolare;

## Personale interno incaricato al trattamento e norme comportamentali

Come già evidenziato in precedenza, il personale interno è autorizzato:
1. all'utilizzo degli strumenti di archiviazione, siano essi informatici o cartacei;
2. al trattamento dei dati dei propri utenti.

| *Nome e Cognome* | *Mansione* | *Strumenti Utilizzati* |
|---|---|---|
| Rossella Tirendi | Resp. Amministrativa | Pc/archivi cartacei |
| Angela Pacini | Resp. Commerciale | Pc/archivi cartacei |
| Donatella Consolo | Resp. Dati Gestionali | Pc/archivi cartacei |
| Valeria Sbarbaro | Add. Serv. Clienti | Pc/archivi cartacei |
| Antonella Rossi | Imp. Attività Comm.le | Pc/archivi cartacei |
| Grazia Trovato | Imp. Amministrativa | Pc/archivi cartacei |

| | | |
|---|---|---|
| Giovanni Zuccarello | Imp. Attività Comm.le | Pc/archivi cartacei |
| Giuseppe Zappala' | Addetto Logistica | Pc/archivi cartacei |
| Antonella Messina | Imp. Attività Comm.le | Pc/archivi cartacei |
| Eleonora Signorello | Imp. Amministrativa | Pc/archivi cartacei |
| Alessandro Trovato | Imp. Attività Comm.le | Pc/archivi cartacei |

Il personale dipendente ha l'obbligo di:

- Custodire la User/psw assegnata per gli accessi agli strumenti di archiviazione informatica;
- Divieto di copia o divulgazione a terzi di dati relativi agli utenti che costituiscono il patrimonio informativo della MEDICAL TI S.R.L.
- segnalare eventuale comportamento scorretto o fraudolento da parte di altro operatore, al responsabile del trattamento dati.

Tutti gli incaricati del trattamento dei dati devono avvisare tempestivamente il responsabile della sicurezza informatica o l'amministratore di sistema o il responsabile del trattamento dei dati, nel caso in cui constatino le seguenti anomalie:

- discrepanze nell'uso degli user-id;
- modifica e sparizione di dati;
- cattive prestazioni del sistema;
- elevate di tentativi di connessione falliti.

In caso di incidente sono considerate le seguenti priorità:

1. evitare danni diretti alle persone;
2. proteggere l'informazione sensibile o proprietaria;
3. evitare danni economici;
4. limitare i danni all'immagine dell'organizzazione.

Garantita l'incolumità fisica alle persone si procedere a:

1. isolare l'area contenente il sistema oggetto dell'incidente;
2. isolare il sistema compromesso dalla rete;
3. tentare lo spegnimento del sistema oggetto dell'incidente.

***Una volta spento il sistema oggetto dell'incidente non deve più essere riacceso se non dal personale preposto;***

4. documentare tutte le operazioni.

Se l'incidente è dovuto ad imperizia del personale o ad eventi accidentali, ovvero quando non vi è frode, danno, abuso e non è configurabile nessun tipo di reato, il ripristino può essere effettuato, a cura dell'amministratore di sistema, direttamente sugli hard disk originali a partire dalle ultime copie di backup ritenute valide.
Altrimenti il titolare del trattamento, il responsabile del trattamento e l'amministratore di sistema coinvolgeranno esperti e/o autorità competenti. La successiva fase di indagine e di

ripristino del sistema sarà condotta da personale esperto di incident response.

## Formazione del personale interno

Tutti i dipendenti o le figure neoassunte, concorrono alla realizzazione della sicurezza, pertanto devono proteggere le risorse loro assegnate per lo svolgimento dell'attività lavorativa, nel rispetto di quanto stabilito e pertanto hanno diritto a regolare formazione.
La MEDICAL TI S.R.L. ha predisposto un piano di formazione volto ad argomentare ed intervenire su:

- analisi dettagliata ed aggiornamenti vigenti sul regolamento UE 679/2016;
- analisi dettagliata del GDPR;
- istruzioni sul corretto utilizzo degli applicativi che consentono l'accesso ai dati e formazione tecnica specifica sugli stessi;

Coerentemente con l'evoluzione degli strumenti tecnici adottati dall'organizzazione, e/o dell'insorgere di nuove disposizioni legislative in materia, verranno istituiti nuovi incontri formativi. In ogni caso, una volta l'anno, verrà calendarizzati degli incontri formativi sull'importanza di adottare le norme di sicurezza e protezione di dati personali, e per recepire eventuali suggerimenti in materia derivanti dalla constatazione della presenza di minacce o vulnerabilità riscontrate.

## Professionisti esterni titolari del trattamento autonomo

I soggetti esterni all'azienda titolare del trattamento ai quali vengono comunicati dati personali per l'esecuzione della propria attività professionale, possono essere considerati dei titolari del trattamento autonomi.
Ogni volta che un soggetto terzo verrà incaricato con mandato professionale, dovrà trattare i dati per conto del titolare. Quest'ultimo dichiarerà il soggetto come "titolare autonomo" del trattamento, e si farà rilasciare, dal soggetto esterno, una dichiarazione che i dati affidatigli saranno trattati secondo normativa vigente ed esclusivamente per le finalità per le quali gli sono stati affidati/comunicati, senza possibilità di diffusione, mentre la comunicazione potrà essere fatta solo in forza di disposizioni di legge o di regolamento (come ad esempio nel caso del consulente del lavoro che fa l'assunzione, o del commercialista che deve comunicare i dati all'agenzia delle entrate, eccetera).

Allo stato attuale, risultano nominati i seguenti professionisti esterni:

- Dr.ssa Rosa Fantauccio per i dati relativi ai dipendenti, nella qualità di medico competente;
- Dr. Alfredo Piazza, per i dati relativi alle scritture contabili, nella qualità di commercialista;
- Sig.ra Consolo Donatella, per i dati relativi alle buste paga, nella qualità di consulente del lavoro;
- Savi srl , per i servizi Hardware e Software;
- Plus informatica, per i servizi di assistenza Software e Manutenzione sistemi informatici;

- Dr. Alessio Nastri, Revisore Unico;

## Aggiornamento del piano

Il presente piano non è soggetto a revisione ai sensi del Regolamento UE 679/2016.
Tuttavia, il piano deve essere aggiornato ogni qualvolta si verificano le seguenti condizioni:

1. Modifiche all'assetto organizzativo della ditta ed in particolare del sistema informativo (sostituzioni di hardware, software, procedure, connessioni di reti, ecc.) tali da giustificare una revisione del piano;
2. Assunzioni o licenziamenti del personale dipendente interessato al trattamento;
3. Danneggiamento o attacchi al patrimonio informativo della ditta tali da dover correggere ed aggiornare i livelli minimi di sicurezza previa analisi dell'evento e del rischio.

***Elenco Allegati costituenti parte distinta di questo documento***

- Mod. 1-2023: Privacy Dipendenti;
- Mod. 1-2023: Modello credenziali User/Psw dipendenti;
- Mod. 1-2023: Nomina Responsabile al trattamento;
- Mod. 1-2023: Lettera trattamento autonomo professionisti esterni;
- Informativa clienti.

Il presente Documento deve essere divulgato e illustrato a tutti gli incaricati.

Il Titolare del Trattamento
Medical TI s.r.l.
Amministratore Unico
Avv. Demetrio Spadaro
Timbro e Firma