TE.RI. SRL

Modello Organizzativo Privacy

REV. 2 DEL 03.06.2020

TE.RI. TERAPIA RIABILITATIVA SRL

1. SCOPO E AMBITO DI APPLICAZIONE

Il presente Modello Organizzativo Privacy (*breviter* M.O.P.) già redatto in base alle precedenti disposizioni di cui al D.lgs. 196/2003 (già DPS – documento programmatico per la sicurezza) è stato adottato dalla TE.RI. – Terapia Riabilitativa Srl – sino all'anno 2013 in ossequio alle procedure di invio a mezzo posta presso gli Uffici del Garante Italiano per la Privacy, e successivamente mantenuto in vigore ed aggiornato secondo le esigenze aziendali.

Gli aggiornamenti del M.O.P. di TE.RI. srl potranno essere soggetti a modifiche ed integrazioni connesse al perdurare ed all'evolversi dell'emergenza epidemiologica ancora in atto nonché in osservanza delle ulteriori evoluzioni di carattere tecnico – scientifico che si dovessero rendere necessarie ai fini del contenimento del Virus Sars-Cov.2 anche ai fini della tracciabilità eventuale di soggetti interessati (sintomatici ed asintomatici) che potrebbero mettere in pericolo la salvaguardia della salute del personale operante presso il Centro nonché presso il domicilio dei pazienti dallo stesso Centro assistiti. Ogni eventuale ulteriore modifica ed integrazione del presente manuale, nonché ogni integrazione di carattere legislativo e/o tecnico-scientifico che dovesse essere imposta alla struttura da norme Comunitarie, Nazionali o Regionali o dalla struttura poste in essere ai fini della salvaguardia del bene superiore della salute pel proprio personale e della propria utenza sarà tempestivamente comunicata a cura del a cura del Titolare e/o del Responsabile del Trattamento.

Stante l'entrata in vigore del Regolamento Europeo sulla Protezione dei Dati Personali n. 679/2016, (*breviter* gdpr) il presente modello viene integrato e modificato al fine di definire le politiche di sicurezza in materia di trattamento di dati personali (con inclusione dei dati già *particolari*) nonché per rimarcare ed ampliare ove necessario i criteri tecnico-organizzativi per la loro attuazione.

Il modello inoltre, fornisce idonee informazioni relative alla tipologia di dati trattati ed all'analisi dei rischi connessi all'utilizzo degli strumenti mediante i quali viene effettuato il trattamento.

Gli allegati al presente modello ne costituiscono parte integrante.

Nel presente modello e nei relativi allegati i termini *Trattamento, Dato personale, Dati identificativi, Dati sensibili, Dati giudiziari, Titolare, Responsabile, Autorizzato (già incaricato), Interessato, Diffusione, Banca dati* e tutti gli altri termini sono usati in conformità alle definizioni già elencate nel D. Lgs n. 196 del 30 giugno 2003 e contemporaneamente nel Reg. UE 2016/679 e nel D.lgs 101/2018.

In dettaglio il Modello fornisce informazioni relative a:

a. l'elenco dei trattamenti di dati personali;
b. la distribuzione dei compiti e delle responsabilità nell'ambito delle aree preposte al trattamento dei dati;
c. l'analisi dei rischi che incombono sui dati;
d. le misure adottate e da adottare per garantire l'integrità e la disponibilità dei dati, nonché le procedure da seguire per controllare l'accesso ai locali nei quali vengono conservati i dati oggetto del trattamento o l'accesso agli stessi per via telematica;
e. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a cancellazione o danneggiamento garantendone la disponibilità in tempi certi compatibili con i diritti degli interessati;
f. la predisposizione di un piano di formazione per rendere edotti gli autorizzati del trattamento dei rischi che incombono sui dati e dei modi per prevenire i danni nonché delle responsabilità che ne derivano e delle modalità di aggiornamento delle misure (già misure *minime*) adottate dal Titolare o sull'introduzione di nuovi strumenti utilizzati per il trattamento dei dati personali;

g. la descrizione dei criteri adottati e da adottare per garantire l'attivazione delle misure di sicurezza in caso di trattamento dati personali affidati all'esterno della struttura del titolare;

h. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato (per gli organismi sanitari e gli esercenti le professioni sanitarie).

La lettera *h)* del presente manuale è stata aggiornata secondo le indicazioni dell'European Data Protection Board del 19.03.2020 nonché agli atti successivi del Presidente del Garante per la Protezione dei Dati Personali relativamente alle misure atte alla prevenzione ed al contenimento dell'emergenza epidemiologica di Covid- 19, le cui indicazioni sono state riportate in informativa sul trattamento dei dati personali fornita all'utenza del Centro, al personale dipendente ed a collaborazione, e ritualmente pubblicata sul sito internet aziendale.

Eventuali ulteriori integrazioni e modifiche del presente documento e degli allegati a corredo, saranno previste di volta in volta secondo quanto disposto dalla normativa Nazionale, Regionale ed eventualmente Comunitaria, al fine di meglio ossequiare la legislazione vigente in materia di trattamento dei dati personali nel contrasto della pandemia e garantire la facile ricognizione del/dei soggetto/i potenzialmente pericoloso/i, benchè essi stessi inconsapevoli di essere portatori asintomatici del Virus Sars. Cov. 2.

A tal fine, le misure di sicurezza poste in essere dalla struttura, come meglio si dirà in seguito, rappresentano un'adeguata risposta per la tutela della salvaguardia della salute del personale operante presso la struttura nonchè presso il domicilio dell'utenza.

Il Modello è divulgato ed illustrato a tutti gli autorizzati nominati con apposite lettere di incarico custodite insieme al presente modello dal Responsabile del trattamento.

Il Titolare ha provveduto e periodicamente provvede ad idonea formazione di tutto il personale operante sia all'interno che all'esterno nonché del personale operante per conto della Struttura sulla materia in questione.

Nel corso dell'anno 2019 la struttura ha infatti organizzato a propria cura e spese, corso di formazione con riconoscimento di crediti ECM in favore del personale dipendente ed a collaborazione sulla materia specifica del trattamento dei dati personali in ambito sanitario.

L'organizzazione del corso è stata seguita in collaborazione con la Società Pre.Sic. srl.

Il materiale didattico risulta essere stato ritualmente distribuito ai partecipanti.

All'interno del Sistema di Gestione della Qualità Aziendale è presente nella sezione "formazione" ogni riferimento al corso di cui al paragrafo che precede.

Il Modello è e sarà oggetto di revisione/i periodiche di volta in volta che le stesse si renderanno necessarie.

Le sedi e i locali nei quali avviene il trattamento dei dati sono dettagliati nell'allegato A01.

Le modalità di trattamento dei dati con l'ausilio di strumenti elettronici avvengono secondo i dettami della normativa con le modalità di accesso previste e con le ulteriori specifiche descritte nell'allegato A08.

Le modalità di trattamento dati senza l'ausilio di strumenti elettronici vengono dettagliate nell'allegato A12 redatto dal Responsabile del trattamento o, in mancanza, dal Titolare.

Il presente Modello è valido per un anno a far data dal giorno 24.05.2018. Trascorso tale termine, e non oltre il 31 dicembre di ogni anno, sarà oggetto ove necessario, di opportune revisioni per adeguarlo ad eventuali modifiche normative, al mutato livello di rischio a cui sono soggetti i dati trattati, ad eventuali assegnazioni o revoche di incarichi, all'utilizzo di nuovi strumenti informatici o in generale a un mutato assetto organizzativo.

ELENCO DEI TRATTAMENTI DI DATI PERSONALI

Al Titolare del Trattamento è affidato il compito di redigere e di aggiornare l'elenco dei trattamenti effettuati sui dati personali.

Il gdpr 2016/679 ha ad oggetto la disciplina dell'attività di trattamento dei dati personali.

In particolare:

- per "*trattamento*" si intende *"qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali, con 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"*;

- per "*dato personale*" si intende *"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".*
- Sono due le categorie fondamentali di dati personali:

1) *dati particolari*: si intendono i dati che *"rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona";*
2) *dati comuni*: le informazioni riferite a persone fisiche identificate o comunque identificabili, che non siano idonee a rivelare gli stati, i fatti e le qualità, di cui all'art. 9 del GDPR, per i quali è vietato il trattamento, salvo che non ricorrano i presupposti di liceità e di legittimazione, previsti dal comma 2 dell'articolo ivi considerato.

In allegato separato è riportato il registro dei trattamenti di dati personali, costituente la base per l'analisi e la valutazione dei rischi e per il conferimento degli incarichi e la formalizzazione delle autorizzazioni e delle istruzioni.

Il documento in parola è mantenuto aggiornato, ove necessario, almeno una volta l'anno. L'evidenza dell'aggiornamento periodico del registro del trattamento è riportata sul verbale di riesame del sistema privacy oltre alla data, al timbro e alla firma del Titolare riportato su di esso.

2. ELENCO CARICHE

Titolare del trattamento

Il *"Titolare"* del trattamento dei dati personali 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, compreso il profilo della sicurezza.

Il Titolare del trattamento dei dati personali, ai sensi e per gli effetti della vigente normativa sulla privacy, è la società TE.RI. – TERAPIA RIABILITATIVA S.r.l., in persona del legale rappresentante pro tempore, Sig.ra Mara Villani sedente per la carica in Roma alla Via Renato Simoni, 29/31 – pec: terisrl@legalmail.it.

Il Titolare, avvalendosi della supervisione e collaborazione del *Data Protection Officer* aziendale, provvede:

1. A richiedere al Garante per la protezione dei dati personali l'eventuale autorizzazione al trattamento dei dati personali, nei casi previsti dalla vigente normativa e ad assolvere all'eventuale obbligo di notificazione e comunicazione;
2. A nominare con atto deliberativo i *Responsabili del trattamento dei dati personali,* impartendo ad essi, per la corretta gestione e tutela dei dati personali, i compiti e le necessarie istruzioni, in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato previsti dagli articoli da 15 a 22 del gdpr 2016/679, all'adozione delle misure di sicurezza per la conservazione, protezione e sicurezza dei dati;
3. A nominare il Data Protection Officer, come stabilito dall'articolo 37 del Regolamento UE;
4. A disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati;
5. A mettere in atto misure tecniche e organizzative adeguate per garantire che il trattamento dei dati sia effettuato conformemente al presente gdpr.

Il Titolare del trattamento provvede ad agevolare l'accesso ai dati personali da parte dell'interessato, a fornirgli le informazioni richieste ed a ridurre i tempi per il riscontro del richiedente.

DPO (Data Protection Officer o Responsabile della protezione dei dati)

Il Regolamento (UE) 2016/679 del parlamento Europeo e del Consiglio del 27 aprile 2016 *"relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)"* GDPR, introduce la figura del Responsabile dei dati personali (RDP) o DPO, ex artt. 37,38,39 GDPR 2016/679.

Le predette disposizioni prevedono che il DPO nel rispetto di quanto previsto dall'art. 39 par. 1 del GDPR 2016/679 è dunque incaricato di svolgere in piena autonomia ed indipendenza, i seguenti compiti e funzioni:

- Informare e fornire consulenza al Titolare del trattamento o al Responsabile del trattamento nonché ai dipendenti che seguono il trattamento in merito agli obblighi derivanti dal GDPR 2016/679, nonché da altre disposizioni nazionali o dell'Unione Europea relative alla protezione dei dati;
- Sorvegliare sull'osservanza del GDPR, di altre disposizioni nazionali o dell'Unione Europea relative alla protezione dei dati nonché delle politiche del Titolare o del Responsabile del trattamento in materia di protezione dei dati personali, compresa l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
- Fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'art. 35 del GDPR 2016/679;
- Cooperare con il Garante per la protezione dei dati personali;
- Fungere da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del GDPR 2016/679 ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;

La nomina avviene per iscritto e nella lettera di incarico vengono dettagliati i compiti assegnati;

Il Responsabile per la protezione dei dati (Data Protection Officer) è: Avv. Andrea Bernardini contattabile, ai fini dell'esercizio agli artt. 15 - 22 del gdpr 2016/679, al seguente indirizzo e-mail: dpo@centroteri.com.

Autorizzati del trattamento

Qualora la gestione delle banche dati richieda l'intervento operativo di altri soggetti, il Titolare può nominare uno o più Autorizzati al trattamento con apposita comunicazione scritta. Sempre per iscritto devono essere specificati i compiti loro assegnati.

La lettera di incarico deve essere sottoscritta dal soggetto interessato e sarà cura del Titolare custodire copia della lettera in luogo sicuro.

Compito degli autorizzati è quello di svolgere gli incarichi assegnati, dettagliatamente specificati nella lettera di incarico, sempre nel pieno rispetto del presente Modello.

In caso di incidenti o di conoscenza di circostanze che possano far venir meno i requisiti di sicurezza, gli Autorizzati devono comunicare tempestivamente tale circostanza al Titolare.

Se non diversamente previsto nella lettera di incarico, gli Autorizzati del trattamento vengono nominati a tempo indeterminato e decadono per dimissioni o per revoca.

Nomina degli Amministratori di sistema

Il Titolare conferisce a uno o più autorizzati ovvero a responsabili esterni (in outsourcing) le mansioni di gestione delle soluzioni informatiche sia hardware che software adottate per la gestione e la tenuta in sicurezza delle banche dati.

La nomina dell'Amministratore di Sistema avviene per iscritto e nella lettera d'incarico vengono dettagliati i compiti assegnati, compreso quello di approntare i mezzi necessari per effettuare le copie di sicurezza dei dati e il loro ripristino in caso di accidentale distruzione.

L'Amministratore di sistema ha anche l'onere di valutare periodicamente lo stato di efficienza delle soluzioni informatiche adottate e provvedere alla loro modifica o integrazione in base all'esperienza acquisita e al progresso tecnologico.

Qualora non fosse già stato incaricato un altro soggetto, l'Amministratore di sistema può essere nominato come custode delle credenziali di autenticazione (codici identificativi, User ID, Password, ecc.) eventualmente assegnate ad ogni soggetto autorizzato.

Nel caso in cui non venisse nominato alcun Amministratore di sistema, le relative mansioni saranno svolte dal Titolare.

Nel caso di specie, la struttura ha ritenuto opportuno che il ruolo in parola sia svolto (in outsourcing) dal Sig. Marcello Cianchetta, residente in Anguillara Sabazia (RM) alla Via Santo Stefano, 18 reperibile ai recapiti: 06.9995641 – 328.7386392 – marccianc@libero.it il quale è tenuto a:

- Sovraintendere alle risorse dei sistemi operativi, degli elaborati, delle banche elettroniche e dell'intero sistema operativo dell'azienda;
- Impostare un sistema di autenticazione informatica e di gestione delle credenziali di autenticazione, nonché adottare un efficace sistema di autorizzazione (costituito dall'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 attribuito all'utente);
- Impostare e gestire un adeguato sistema di autenticazione informatica per i trattamenti di dati personali effettuati con strumenti elettronici;
- Impostare e gestire procedure atte a proteggere gli elaborati dal rischio di intrusione e dal rischio di virus mediante idonei programmi antivirus ed appositi dispositivi (firewall ed altri strumenti) che garantiscano, anche in relazione alle conoscenze acquisite in base al progresso tecnico, la sicurezza del trattamento dei dati personali, secondo i criteri stabiliti dalla normativa vigente;
- Controllare periodicamente il servizio di assistenza informatica effettuato, in particolare nella verifica della validità ed efficienza dei sistemi tecnici/informatici;
- Promuovere tutti i provvedimenti necessari per evitare la perdita e la distruzione dei dati e provvedere al ricovero periodico degli stessi (copie di back – up);
- Provvedere a tenere aggiornato l'elenco degli incaricati a cui è assegnato un profilo utente ed un criterio di autorizzazione;
- Attivare ed aggiornare, con cadenza almeno semestrale, o secondo eventuali e più adeguate misure individuate aziendalmente, idonei strumenti atti a proteggere i dati trattati contro il rischio di intrusione e contro l'azione di virus informatici facendosi supportare nell'operazione dall'Amministratore di Rete che in questa sede è individuato nella persona del Sig. Stefano Bertoni, residente in Mazzano Romano alla Via Meterano, 7/a e reperibile ai seguenti recapiti: 06.9049176 – 329.4192469 – s.bertoni@studiosb.it;

- Organizzare i flussi di rete, la gestione dei supporti di memorizzazione, la verifica di eventuali tentativi di accesso non autorizzati al sistema provenienti da soggetti terzi quali accesso abusivo al sistema informatico o telematico, frode informatica, danneggiamento di informazioni, dati e programmi informatici, danneggiamento di sistemi informatici e telematici.

La nomina avviene per iscritto e nella lettera di incarico nella quale vengono dettagliati i compiti assegnati.

L'amministratore, nello svolgere questo incarico, si attiene a quanto previsto nel presente modello come Custode delle credenziali di autenticazione.

Nel caso in cui non venisse nominato alcun Amministratore di sistema, le relative mansioni saranno svolte dal Responsabile del trattamento o, in mancanza, dal Titolare.

Nomina del custode delle credenziali di autenticazione

Il Responsabile del trattamento, in concerto con il Titolare, può nominare uno o più custodi delle credenziali di autenticazione per l'accesso ai sistemi di elaborazione dati.

L'incarico viene assegnato per iscritto e la lettera deve essere conservata in un luogo sicuro da parte del soggetto che conferisce l'incarico.

Il *Custode delle credenziali* prende visione di tutte le credenziali di accesso da custodire.

Le credenziali non devono essere divulgate e dovranno essere custodite in luogo sicuro.

Spetta al custode definire le modalità di utilizzo delle credenziali di autenticazione in caso di impedimenti o prolungata assenza dell'autorizzato alle quali sono state assegnate.

In mancanza di un custode delle credenziali di autenticazione, le mansioni sopra riportate saranno svolte dall'Amministratore del Sistema o, in mancanza, dal soggetto che ha conferito l'incarico (Responsabile o Titolare del trattamento).

Nel caso di specie il custode delle credenziali è l'Amministratore di Sistema già in precedenza generalizzato.

ANALISI DEI RISCHI – Valutazione di Impatto

L'analisi dei rischi ai quali sono soggetti i dati trattati è dettagliata nell'allegato A.11.

In tale allegato è compilata un'apposita lista dei rischi incombenti sui dati da parte del sistema di elaborazione, dal Sistema operativo, dagli Applicativi.

La predetta lista viene di volta in volta aggiornata a seconda degli interventi normativi (nazionali o comunitari) ed a seconda delle decisioni aziendali sull'implementazione delle misure di sicurezza.

Nello stesso allegato sono proposte le azioni correttive o preventive.

L'analisi dei rischi è redatta in relazione al progresso tecnologico, alla sostituzione, integrazione e sostituzione di hardware, agli aggiornamenti o alla sostituzione di sistemi operativi e\o programmi applicativi.

3. MISURE DI SICUREZZA E CONTROLLO ACCESSO AI LOCALI

In ottemperanza agli articoli 32 e ss del gdpr 2016/679 (*ex* agli artt. 31, 32, 33, 34, 35 e 36 del D. Lgs 30/06/2003 n. 196), il presente modello prevede idonee misure di sicurezza (già) adottate e volte a garantire la sicurezza dei dati.

La sicurezza dei dati si esplica nella loro diligente custodia al fine di prevenirne alterazioni, distruzione, cancellazione, diffusioni non autorizzate o trattamenti non conformi alle finalità della raccolta.

Il Responsabile del trattamento o, in mancanza, il Titolare approntano ed appronteranno ove necessario tutti i mezzi necessari per il perseguimento dei fini legati alla sicurezza dei dati, sfruttando anche le conoscenze acquisite in base al progresso tecnico e tecnologico.

Sono previste specifiche misure di sicurezza sia per quanto riguarda la custodia di archivi elettronici e non, che l'accesso ai locali ove i dati oggetto del trattamento fisicamente sono conservati.

La procedura di preservazione dal rischio di perdita dei dati trattati con mezzi informatici o dalla divulgazione non autorizzata si esplica nella previsione di un piano basato su:

Copie periodiche di Backup.

Tale procedura, che il Responsabile del trattamento o il Titolare hanno stilato in concerto con l'amministratore di sistema, fornisce istruzioni e modalità in merito al tipo di supporto utilizzato, all'impiego di specifici software per salvataggi automatizzati, alla nomina degli Autorizzati al trattamento che eventualmente eseguiranno le copie di Backup, alla custodia dei supporti nei quali sono stati memorizzati i dati, alla distruzione dei supporti dopo un determinato lasso di tempo e comunque alla cancellazione dei dati dai supporti di Backup in maniera tale da impedirne ogni possibile consultazione.

La procedura di salvataggio prevede anche il monitoraggio di tutte le operazioni affinché il Responsabile o il Titolare del trattamento possano individuare periodicamente circostanze che impongano l'adozione di un diverso piano di Backup o il suo aggiornamento.

Il salvataggio dei dati avviene con cadenza almeno settimanale.

La procedura di Backup è dettagliata nell'allegato A.10.

a) Protezione da virus informatici o intrusioni non autorizzate nella propria rete informatica.

Il Responsabile del trattamento o il Titolare hanno incaricato l'Amministratore del Sistema e l'Amministratore di Rete ad approntare tutte le misure di sicurezza idonee a prevenire e ridurre infezioni da Virus informatici o da intrusioni non autorizzate nel sistema.

In dettaglio nell'allegato A09 vi sono tutte le misure adottate compresi l'utilizzo di appositi programmi Antivirus, Firewall e qualsiasi ulteriore soluzione informatica ritenuta opportuna ed idonea allo scopo di diminuire la vulnerabilità del sistema.

E' compito dell'amministratore di sistema in concerto con l'amministratore di rete pianificare il lavoro relativo all'installazione degli aggiornamenti messi a disposizione delle case produttrici di software per correggere eventuali difetti dei programmi o dei sistemi operativi utilizzati ed adattarli, in sicurezza, alla realtà aziendale.

Gli amministratori di sistema e di rete possono prevedere anche che il periodico aggiornamento dei programmi utilizzati per garantire che la sicurezza informatica avvenga in un arco di tempo inferiore a quanto previsto dal gdpr 2016/679 (*ex* all.B D. Lgs 30/06/2003 n. 196).

Tutte le misure di sicurezza previste dagli amministratori di sistema e di rete sono periodicamente valutate per adattare la procedura all'evoluzione tecnologica.

L'amministratore di sistema provvede ad istruire adeguatamente eventuali incaricati al trattamento.

In caso di infezione del sistema da parte di Virus informatici, l'amministratore del sistema in concerto con l'amministratore di rete deve tempestivamente adottare tutte le misure idonee per isolare il sistema ed evitare che il danno venga esteso ad altri elaboratori; deve quindi individuare le cause di tale infezione e provvedere a rimuoverle.

b) Sistema di autenticazione informatica.

Così come previsto in gdpr 2016/679 (*ex* all.B Allegato B al D. lgs 196/2003) il trattamento dei dati personali con strumenti elettronici è consentito solo agli autorizzati dotati di credenziali che consentono il superamento di una procedura di autenticazione.

Il Responsabile del trattamento (o in mancanza, il Titolare), in accordo con l'Amministratore di sistema, definisce le modalità di assegnazione delle credenziali di autenticazione agli autorizzati del trattamento.

Le credenziali possono consistere nell'assegnazione di User ID e password o nell'utilizzo di dispositivi associati ad un codice identificativo.

Ad ogni soggetto autorizzato all'accesso alle banche dati possono essere assegnate anche più credenziali per l'autenticazione in base alle esigenze organizzative o al numero di banche dati gestite.

Se fra le credenziali di autenticazione è prevista l'assegnazione di una password, questa non deve essere di lunghezza inferiore agli otto caratteri (o al numero massimo possibile se lo strumento elettronico utilizzato non lo consente).

Al primo utilizzo delle password, l'incaricato provvederà a modificarla e successivamente la modificherà periodicamente con cadenza almeno trimestrale.

Ogni persona autorizzata al trattamento dei dati deve adottare tutte le cautele possibili per garantire la segretezza delle credenziali di autenticazione assegnatele.

Per ciò che concerne la gestione dei dati non trattati con strumenti elettronici, viene appositamente definita la modalità di trattamento e i vari supporti utilizzati. Vengono altresì definite tutte le misure di sicurezza da adottare per evitare l'accidentale perdita o danneggiamento dei dati. Tutte le modalità di trattamento dati senza l'ausilio di strumenti elettronici e della loro sicurezza sono dettagliate nell'allegato A.12.

L'allegato A.12 contiene le modalità di accesso ai locali dove fisicamente vengono gestite le banche dati, sia nel caso di dati trattati con l'ausilio di strumenti elettronici che con altri strumenti.

E' cura del Responsabile (od in mancanza del Titolare del Trattamento) redigere e tenere aggiornato tale documento.

In ogni caso è fatto divieto a qualunque soggetto di divulgare informazioni concernenti i dati oggetto del trattamento, effettuarne copie di qualsiasi natura (su supporti cartacei, informatici, audiovisivi, ecc.) distruggere, sottrarre o manipolare il contenuto delle banche dati se non espressamente autorizzato dal Responsabile o dal Titolare.

3.1 ACCESSO AI LOCALI A SEGUITO EMERGENZA EPIDEMIOLOGICA COVID-19

A seguito dell'insorgenza della pandemia e della conseguente emergenza epidemiologica di Covid-19 la struttura ha posto in essere ulteriori misure di sicurezza per l'accesso ai propri locali operativi ed amministrativi.

Nel dettaglio: l'ingresso al Centro di riabilitazione i locali sono siti in Roma alla Via Renato Simoni, 31 è sottoposto alla scansione sia del personale che dell'utenza ad apparecchio denominato "termoscanner" fornito alla struttura da parte della Società Digital Tecnologies con sede in Trezzano sul Naviglio (MI) alla Via Politi, 10.

L'apparecchio di cui sopra, il cui manuale utente è allegato al presente documento, ha come funzione principale quella del rilevamento della temperatura corporea che, secondo quanto previsto dal Piano Territoriale della Regione Lazio, non deve essere uguale o superiore ai 37,5°.

L'utenza ed il personale prima di accedere alla struttura deve obbligatoriamente sottoporsi a scansione della temperatura e contestualmente deve indossare il presidio (DPI) della mascherina chirurgica.

Qualora, come da informativa semplificata affissa e ben visibile sulla porte di accesso alla struttura, l'apparecchio rilevi una temperatura corporea inferiore ai 37,5° e la presenza di mascherina chirurgica, la porta di accesso al centro si apre automaticamente, consentendo all'operatore, al dipendente amministrativo, all'utente ed al proprio accompagnatore, di accedere presso la sala di attesa della struttura e recarsi nella zona denominata "triage" per gli ulteriori controlli necessari alla verifica delle propri condizioni di salute.

Allo stesso modo altro apparecchio termoscanner, è stato posizionato all'interno dei locali della cd "palestra fkt".

L'area entro cui il personale ivi operante è appositamente delimitata, consentendo allo stesso di posizionarsi correttamente dinanzi alla macchina per il controllo della temperatura e la verifica della presenza del DPI.

Gli aggiornamenti del M.O.P. di TE.RI. srl potranno essere soggetti a modifiche ed integrazioni connesse al perdurare ed all'evolversi dell'emergenza epidemiologica ancora in atto nonché in osservanza delle ulteriori evoluzioni di carattere tecnico – scientifico che si dovessero rendere necessarie ai fini del contenimento del Virus Sars-Cov.2 anche ai fini della tracciabilità eventuale di soggetti interessati (sintomatici ed asintomatici) che potrebbero mettere in pericolo la salvaguardia della salute del personale operante presso il Centro nonché presso il domicilio dei pazienti dallo stesso Centro assistiti. Ogni eventuale ulteriore modifica ed integrazione del presente manuale, nonché ogni integrazione di carattere legislativo e/o tecnico-scientifico che dovesse essere imposta alla struttura da norme Comunitarie, Nazionali o Regionali o dalla struttura poste in essere ai fini della salvaguardia del bene superiore della salute pel proprio personale e della propria utenza sarà tempestivamente comunicata a cura del a cura del Titolare e/o del Responsabile del Trattamento.

La procedure del sistema di gestione qualità aziendale, nonché gli addendum sul rischio biologico elaborate dal R.S.P.P.E. prevedono che il personale (dipendente ed a collaborazione) rediga sotto la propria esclusiva responsabilità un modulo denominato "triage e diario giornaliero" composto da una griglia riportante giorno per giorno le proprie condizioni di salute, confermando, dopo il passaggio al termoscanner la possibilità di accesso presso i locali di Via Renato Simoni, 31 apponendo la propria firma sotto la lettera "C" = conforme.

In ambito di compliance aziendale ed interconnessione tra i manuali: DVR – M.O.G. – ISO 9001:2015 in questa sede ci si riporta integralmente alle procedure in essi trascritte.

Allo stesso modo ulteriore apparecchio termoscanner con altrettanti moduli di triage ed autovalutazione giornaliera dello stato di salute, è stato posizionato presso i locali amministrativi della Struttura, siti in Roma alla Via Giuseppe Marcotti, 32.

In ossequio ai principi di liceità del trattamento dei dati, benchè le Direttive dell'EDPB prevedano ogni deroga possibile al trattamento dei dati di cui all'art. 9) del gdpr per tutto il perdurare dell'emergenza epidemiologica di Covid-19, la Struttura, che ha nominato la Società Digital Tecnologies srl quale Responsabile del Trattamento (accessi in struttura per il tramite di termoscanner) in assenza di una precisa indicazione degli Organi Istituzionali, ha richiesto che le apparecchiature in questione non trattengano immagini né di utenza, né di personale al momento dell'ingresso presso le proprie sedi (operativa ed amministrativa).

L'unico dato di cui la struttura rimane in possesso per un periodo non superiore a 15 giorni, è la data di accesso dell'interessato con indicazione di temperatura riscontrata dalla macchina e presenza o meno di DPI al momento dell'entrata.

4. CRITERI DI RIPRISTINO DATI DANNEGGIATI

In caso di distruzione o danneggiamento dei dati oggetto del trattamento, ogni autorizzato, in concerto con l'amministratore del sistema, provvederà a ripristinare i dati mediante utilizzo delle copie di backup realizzate in conformità a quanto descritto nell'allegato A10.

L'amministratore di sistema può anche prevedere l'utilizzo di altri strumenti in suo possesso (supporti cartacei, e-mail, registrazioni audiovisive, ecc.) per ricostruire nel modo più fedele possibile i dati distrutti o danneggiati, sia quelli trattati con l'ausilio di strumenti elettronici che quelli trattati con altri tipi di strumenti.

In caso di eventuale distruzione o danneggiamento degli strumenti utilizzati per l'accesso ai dati, l'Amministratore di sistema provvederà tempestivamente al ripristino del normale stato di utilizzo dei suddetti strumenti o alla loro sostituzione.

La procedura di ripristino o di accesso ai dati avverrà comunque in tempi compatibili con i diritti degli interessati in conformità alle disposizioni del gdpr.

Ad ogni evento che comporti distruzione, danneggiamento o problemi di accesso ai dati dovrà essere opportunamente aggiornata l'analisi dei rischi di cui al paragrafo IV del presente Modello.

5. PIANO DI FORMAZIONE DEGLI AUTORIZZATI

Al Responsabile (o in mancanza al Titolare) spetta il compito di provvedere all'opportuna formazione di tutti gli autorizzati al trattamento dei dati al fine di:

a) garantire il massimo rispetto delle procedure elencate nel presente Modello;
b) rendere edotto il personale sui rischi che incombono sui dati;
c) informare il personale sulle responsabilità che ne derivano.

Il Responsabile (o in mancanza il Titolare) valuterà opportunamente il livello di preparazione dei singoli addetti in merito alle procedure (informatiche e non) utilizzate per il trattamento e la custodia dei dati; eventuali lacune saranno colmate con appositi interventi formativi volti a rendere i soggetti interessati idonei a svolgere gli incarichi loro assegnati.

Il Titolare o il Responsabile, con cadenza almeno annuale e con il supporto del DPO nominato, ove necessario, provvederanno a verificare le esigenze di formazione del personale in base all'esperienza acquisita, al progresso tecnologico o al cambiamento di mansioni.

Formazione da impartire	Intervento formativo
Custodia dello strumento elettronico durante una sessione di trattamento di dati personali	Corso formativo, tenuto dal Titolare del Trattamento o ove esistente dal Consulente Aziendale teso a sensibilizzare il personale autorizzato al trattamento e alla custodia dello strumento elettronico;

Rischi incombenti sui dati	Corso formativo teso ad illustrare i rischi incombenti sui dati nonché ad istruire il personale autorizzato al trattamento all'utilizzo corretto degli applicativi che consentono l'accesso ai dati;
Conoscenza delle norme e del Documento/Modello o delle parti rilevanti in relazione al trattamento dei dati ed al settore di attività aziendale	Il corso formativo organizzato dal Titolare del Trattamento con l'ausilio del Consulente Aziendale, è teso a rendere edotto il personale autorizzato dei contenuti del Documento / Modello Organizzativo per la tutela dei dati personali-particolari, nonché a fornire a tutti i soggetti elencati una copia del Dlgs 196/2003 come aggiornato con il D.lgs 101/2018, una copia del GDPR 2016/679 ed una copia del Documento/Modello.
Custodia ed uso dei supporti rimovibili contenenti dati personali, sensibili o giudiziari.	Il corso formativo è teso a fornire apposite istruzioni in merito. Durante il corso il personale autorizzato sarà istruito affinché l'autorizzato al trattamento non lasci incustoditi i supporti rimovibili contenenti dati personali, non conduca supporti rimovibili all'esterno degli uffici in cui il trattamento è effettuato.
Controllo e custodia per l'intero ciclo di trattamento di dati senza supporto di strumenti elettronici	Le procedure per il controllo, la custodia ed il trattamento di dati personali senza l'ausilio di strumenti elettronici sono descritti nel regolamento aziendale in apposita procedura

	presente in CEedC. A cura del Titolare, e/o del Consulente aziendale è organizzato apposito corso formativo che coinvolga tutti gli autorizzato in cui viene illustrato il documento sopramenzionato e chiariti ulteriori quesiti posti dagli stessi autorizzati.

6. DATI AFFIDATI ALL'ESTERNO DELLA STRUTTURA – AFFIDAMENTO IN AUTSOURCING (RESPONSABILI EX ART 28 REG. UE)

Nei casi in cui il trattamento dei dati venisse affidato in parte o *in toto* a soggetti esterni alla struttura, la nomina di tali soggetti come in precedenza avviene per iscritto mediante apposita lettera di incarico.

E' cura del Titolare conservare in luogo sicuro copia di tale lettera.

La scelta dei Responsabili del trattamento dati in esterno deve ricadere su soggetti che forniscano i requisiti di affidabilità previsti ex art. 28 Reg. Eu. 2016/679.

Tutti i soggetti esterni che effettuino operazioni di trattamento sulle banche dati dell'Azienda, per conto e nell'interesse della stessa, per finalità connesse all'esercizio delle funzioni istituzionali, sono nominati "Responsabili esterni" del trattamento.

I Responsabili ex art. 28 hanno l'obbligo:

a) di trattare i dati in modo lecito, secondo correttezza e nel pieno rispetto della normativa vigente in materia di privacy;
b) di rispettare le misure di sicurezza e di adottare tutte le misure che siano idonee a prevenire e/o evitare la comunicazione o diffusione dei dati, il rischio di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non autorizzato o non conforme alle finalità della raccolta;
c) di nominare al loro interno i soggetti incaricati del trattamento;
d) di garantire che i dati trattati siano portati a conoscenza soltanto del personale incaricato del trattamento;

e) di trattare i dati personali, anche di natura sensibile e sanitaria, dei Pazienti esclusivamente per le finalità previste dal contratto o dalla convenzione;
f) di attenersi alle disposizioni impartite dal Titolare del trattamento;
g) di specificare i luoghi dove fisicamente avviene il trattamento dei dati.

Nel caso di mancato rispetto delle predette disposizioni, i Responsabili esterni del trattamento devono intendersi autonomi "Titolari" del trattamento e quindi soggetti ai rispettivi obblighi e pertanto rispondono direttamente e in via esclusiva per le eventuali violazioni alla legge. La designazione viene effettuata mediante "atto di nomina" inserito negli accordi, convenzioni o contratti che prevedono l'affidamento di trattamenti di dati personali esternamente all'Azienda.
Sarà compito del Responsabile esterno nominare i propri autorizzati e impartire loro la dovuta istruzione per garantire il trattamento e la conservazione dei dati in modo puntuale, lecito e sicuro.
Ogni trattamento di dati affidato all'esterno della struttura elencato nell'apposito allegato A02, ove sono indicati anche i luoghi dove vengono fisicamente trattati e conservati i dati.
Al Titolare del trattamento spetta il compito di vigilare sull'operato del Responsabile esterno affinché non vengano mai meno le misure minime di sicurezza dei dati.

7. PROCEDURA AZIENDALE DI VIDEOSORVEGLIANZA

Principi e finalità

La parte specifica del modello relativa alla videosorveglianza è redatta in relazione all'istallazione dell'impianto di videosorveglianza con registrazione di immagini presso la sede legale della società conformemente alla normativa vigente di cui all'art. 4 della Legge n. 300/1970 (statuto dei lavoratori) - così come modificato dall'art. 23 D.Lgs. 151/2015 (noto come *Job Act*) attuativo della legge delega 183/2014 - nonché a quanto prescritto dalla normativa in materia di Privacy di cui al (ex) D.Lgs 196/2003 come modificato dal D.Lgs 101/2018 e dal Reg. EU n. 679/2016, nonché Autorizzazione del Ministero del Lavoro e delle Politiche Sociali – Direzione Territoriale del Lavoro –

Servizio Ispezione – Linea 3.1 – protocollo n. 22567 del 4.03.2013, notificata al RLS di TERI srl in data 26.03.2013

Il menzionato sistema è stato istallato per le seguenti finalità:

a) Tutela del patrimonio aziendale, ovvero per prevenire il compimento di atti vandalici, di danneggiamento, furti e aggressioni;

b) Esigenze di sicurezza dei luoghi di lavoro, ovvero per garantire la sicurezza degli ambienti di lavoro a tutela dei lavoratori e delle persone che a vario titolo frequentano i locali aziendali.

Secondo quanto specificato anche dal Provvedimento in materia di videosorveglianza 8 aprile 2010 del Garante per la protezione dei dati personali, la videosorveglianza è un'attività di trattamento di dati personali ovvero la raccolta, la registrazione, la conservazione e, in generale, l'utilizzo di immagini configura un trattamento di dati

personali o di informazioni relative a persone fisiche identificate o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione.

Pertanto, lo svolgimento delle attività relative e/o connesse alla videosorveglianza, deve avvenire nel rispetto dei principi e delle prescrizioni contemplate dalla menzionata normativa in materia di Privacy nonché in osservanza del Provvedimento in questione.

Si elencano di seguito i principi contemplati dalla normativa sulla Privacy.

1) *Principio di necessità*

   Uno dei principali principi che devono essere rispettati nello svolgimento delle attività inerenti alla videosorveglianza è il principio di necessità ovvero il trattamento dei dati personali (immagini video) deve essere effettuato solo ed esclusivamente per il perseguimento delle finalità stabilite, riducendo al minimo l'utilizzazione dei dati.

2) *Principio di Liceità*

   Il trattamento dei dati personali (immagini video) deve essere effettuato nel rispetto delle norme di legge (non solo della normativa in materia di Privacy)

3) *Principio di Correttezza*

   Il trattamento dei dati personali (immagini video) deve essere effettuato nel rispetto delle esigenze reciproche dell'Azienda (Titolare del Trattamento) e degli Interessati (persone che, a vario titolo, frequentano e/o accedono ai locali aziendali dove sono istallate le telecamere).

4) *Principio di Trasparenza*

   L'azienda deve assicurare la consapevolezza degli interessati in ordine al trattamento delle immagini video che li riguardano (obblighi

di informativa di cui si dirà di seguito).

5) *Principio di integrità e riservatezza*
I dati (immagini video) devono essere trattati in modo da garantire un'adeguata sicurezza e protezione dei dati stessi, mediante misure tecniche e organizzative adeguate e idonee ad evitare trattamenti non autorizzati e/o illeciti e accessi non consentiti.

6) *Principio di limitazione delle finalità*
Il trattamento dei dati deve essere effettuato per scopi (finalità) determinati, espliciti e legittimi; trattamenti successivi a quelli iniziali (ovvero a quelli per cui i dati sono stati inizialmente raccolti) non devono avere finalità incompatibili a quella originale (salvo casi espressamente previsti dalla legge.

7) *Principio di limitazione della conservazione.*
I dati trattati devono essere conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali i dati stessi sono stati trattati (salvo eccezioni previste dalla legge). Al rispetto dei menzionati principi si aggiunge il rispetto di tutti gli adempimenti previsti dalla citata normativa che si elencano di seguito.

Informativa

Sempre in osservanza della normativa in materia di privacy, gli interessati (ovvero tutti coloro che transitano nelle aree videocontrollate) devono essere opportunamente informati del fatto che stanno per accedere ad una zona videosorvegliata. A tal fine, negli ambienti e spazi sottoposti a videosorveglianza, l'azienda ha istallato, in posizione chiaramente visibile, prima del raggio di azione delle telecamere, appositi cartelli contenenti l'informativa minima e semplificata conforme al modello stabilito dal Garante nel suindicato Provvedimento.

Inoltre l'Azienda ha affisso nella bacheca presente nella sala di attesa, l'informativa completa che contiene tutti gli elementi prescritti dall'art. 13 Reg UE 679/2017.

In proposito il Garante raccomanda che l'informativa resa in forma semplificata deve rinviare ad un testo più completo contenente tutti gli elementi dell'art.13 Reg UE 679/2017 da rendere disponibile agevolmente per gli interessati con modalità facilmente accessibili anche con strumenti informatici e telematici (in particolare tramite reti intranet, affissioni in bacheche e/o locali aziendali, etc.).

Registrazione delle immagini

La registrazione delle immagini – attività riconducibile ad un trattamento di dati personali - sono effettuate nel rispetto dei suindicati principi di necessità, proporzionalità e limitazione della conservazione ossia l'eventuale conservazione delle immagini video deve essere commisurata al grado di indispensabilità e per il solo tempo necessario al raggiungimento delle finalità perseguite. Viene dunque fissato un limite massimo di conservazione, il quale potrà essere superato in presenza di richieste investigative da parte dell'autorità giudiziaria e/o della polizia giudiziaria.
L'Azienda stabilisce il periodo di cancellazione delle immagini video in 24 ore, che può aumentare in considerazione delle esigenze di conservazione in relazione alle festività e agli orari di chiusura e apertura degli uffici (es. venerdì sera e lunedì mattina). La cancellazione delle registrazioni video è automatica allo scadere del termine fissato.

Descrizione del sistema di video - sorveglianza
Il sistema consiste in una "centrale operativa" con funzioni di controllo e supervisione collocata presso l'ufficio amministrazione della struttura e da un insieme di punti di ripresa costituiti da telecamere fisse.
Un'attenta analisi delle finalità ha comportato delle valutazioni geometriche per il posizionamento delle telecamere, per accertarsi che il campo ripreso ed i dati personali acquisiti siano congrui con le finalità dell'impianto. Sono state individuate delle posizioni ben specifiche nelle quali si raccoglie il massimo di elementi utili a soddisfare le finalità dichiarate ed il minimo ragionevolmente e tecnicamente possibile di dati personali, non inerenti alle finalità dichiarate.
Il posizionamento delle telecamere è funzionale alla sorveglianza della struttura, degli accessi e delle aperture per le quali si ritiene necessaria l'installazione del suddetto impianto. Più precisamente:
Le immagini riprese da tutte le telecamere verranno registrate su unità Hard Disk attraverso l'apposito videoregistratore DVR. L'apparecchiatura di registrazione, nonché gli accessori per il funzionamento sono stati collocati in modo da garantirne la sicurezza.
La chiavi di accesso all'armadio – contenitore del DVR sono custodite in luogo sicuro dal Responsabile del Trattamento.
L'impianto di videosorveglianza sarà in funzione 24 ore su 24 anche nelle giornate di chiusura con una registrazione massima di 24 ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione, nonché nel caso in cui si debba aderire ad
una specifica richiesta investigativa e dell'Autorità Giudiziaria o di Polizia Giudiziaria, dopo di ché il sistema DVR provvederà automaticamente alla cancellazione delle registrazioni, sovrascrivendo le nuove. Su richiesta dell'Autorità Giudiziaria o della Polizia Giudiziaria, le sole immagini utili alla ricerca dei responsabili saranno riversate, a cura dell'incaricato del Trattamento, su un nuovo supporto informatico, al fine della loro conservazione in relazione agli illeciti o alle indagini. Al fine di garantire l'assoluta riservatezza delle registrazioni, il sistema prevenderà la visione solo attraverso l'inserimento di un utente e una password in possesso solo al personale autorizzato e al titolare dell'esercizio.
La visualizzazione delle immagini spetta esclusivamente al Titolare del Trattamento dei dati, non potrà costituire supporto all'accertamento

dell'obbligo di diligenza del lavoratore (o essere occasione indiretta per tale accertamento) e dell'adozione di provvedimenti sanzionatori, ma soltanto ai fini della sicurezza e della tutela del patrimonio aziendale. Ad ogni altro soggetto non autorizzato è inibita sia la visione sia la disponibilità delle immagini e dei dati rilevati dal sistema.

Non è previsto alcun collegamento diretto con le forze dell'ordine e pertanto non sarà possibile la visione in tempo reale delle immagini da postazione remota.

Le inquadrature delle telecamere sono tali da cogliere un'immagine il più pertinente possibile ai soli accessi all'Azienda evitando, il più possibile, di inquadrare i luoghi circostanti non pertinenti al patrimonio aziendale.

Misure di sicurezza

In osservanza della normativa in materia di Privacy, i dati personali (quindi le immagini video) devono essere protetti da idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, perdita, anche accidentale, di accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta.

L'Azienda ha, quindi, adottato idonee misure di sicurezza tecniche e organizzative al fine di tutelare la sicurezza e la riservatezza dei dati trattati.

Nel dettaglio: L'accesso ai locali (sala regia) dove sono ubicati i sistemi di visualizzazione delle immagini (monitor) è consentita al solo personale incaricato del trattamento nonché, eventualmente, ai tecnici esterni addetti all'assistenza e/o alla manutenzione degli impianti.

I sopra menzionati soggetti, autorizzati all'accesso ai predetti locali e/o ai sistemi di visualizzazione, sono tenuti ad osservare scrupolosamente il presente regolamento nonché le istruzioni fornite dal Titolare del trattamento, con particolare riferimento al corretto trattamento di dati pertinenti e non eccedenti rispetto allo scopo per cui sono stati istallati gli impianti.

Incaricato esterno della manutenzione dell'impianto di videosorveglianza e del DVR in caso di eventuali disservizi del sistema è: la Ditta Simone Andreoli, nella persona del lr.p.t. Sig. Simone Andreoli, sedente per la carica in Nettuno, alla Via Pineta, 67 – email: andreoli.si@tiscali.it – pec: simoneandreoli@pecimprese.it – cell: 339.4728607.

Detto incaricato esterno del dovrà attuare tutte le precauzioni di natura tecnica, procedurale ed organizzativa per garantire il rispetto del trattamento secondo la legge e le misure di sicurezza per impedire usi impropri dei dati.

Il titolare dei trattamenti osserva scrupolosamente i principi di liceità, necessità e proporzionalità, limitando i dettagli delle immagini alle reali necessità, e disponendo eventuali automatismi di ripresa avendo cura di evitare luoghi ed accessi privati, luoghi di lavoro ecc.

Diritti degli interessati

Il GDPR garantisce all'interessato i diritti previsti agli articoli da 15 a 22.

Nello specifico, gli interessati possono:

a) chiedere al titolare l'accesso alle immagini;

b) opporsi al trattamento;

c) chiedere la limitazione del trattamento e/o la cancellazione ove applicabili.

d) Gli interessati possono altresì proporre reclamo all'Autorità di controllo competente. Non è in concreto esercitabile il diritto di aggiornamento o integrazione, nonché il diritto di rettifica di cui all'art. 16 GDPR in considerazione della natura intrinseca dei dati trattati (immagini raccolte in tempo reale riguardanti un fatto obiettivo). Non è esercitabile il diritto alla portabilità dei dati di cui all'art. 20 GDPR in quanto il trattamento è effettuato in esecuzione di un legittimo interesse del titolare. L'interessato potrà richiedere di visionare le

immagini in cui ritiene di essere stato ripreso esibendo o allegando alla richiesta idonei documenti di riconoscimento. La risposta ad una richiesta di accesso non potrà comprendere eventuali dati riferiti a terzi, a meno che la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato.

8. CIFRATURA DEI DATI RELATIVI ALLO STATO DI SALUTE

Qualora la tipologia dei dati trattati comprendesse anche quelli di tipo sanitario relativi allo stato di salute o alla vita sessuale degli interessati sono previste idonee misure per gestire la separazione dei dati dall'individuazione diretta dell'interessato ed individuare i casi in cui necessita la loro cifratura.

Misure di sicurezza ambito organizzativo

La sicurezza dei dati si esplica nella loro diligente custodia al fine di prevenirne alterazioni, distruzione, diffusioni non autorizzate o trattamenti non conformi alle finalità della raccolta.

Il Titolare del trattamento appronta ed approntera ove necessario tutti i mezzi necessari per il perseguimento dei fini legati alla sicurezza dei dati, sfruttando anche le conoscenze acquisite in base al progresso tecnico e tecnologico.

Sono previste specifiche misure di sicurezza sia per quanto riguarda la custodia dei documenti presenti negli archivi cartacei sia per ciò che concerne l'accesso controllato ai locali.

I) Conferimento di incarichi e responsabilità in osservanza della normativa in materia di Privacy. In particolare, in linea con l'assetto organizzativo aziendale, sono stati designati gli incaricati/autorizzati

al trattamento dei dati personali nonché i Responsabili del trattamento ai sensi dell'art. 28 Reg UE 679/2016;

2) Adozione di un *"Regolamento Aziendale in ordine all'utilizzo degli strumenti informatici, posta elettronica, internet e dei servizi di telefonia, e quindi al trattamento dei dati con l'ausilio di strumenti elettronici"*;
3) Inserimento, a livello di Sistema nelle e-mail aziendali, di una frase per la tutela della riservatezza, con finalità cautelative nei casi in cui un messaggio di posta elettronica possa arrivare ad un soggetto diverso dal destinatario autorizzato a conoscere i dati protetti dalla privacy;
4) Adozione di un "Regolamento Aziendale che comprenda espressamente il paragrafo e le istruzioni sulla Videosorveglianza" in linea con quanto disposto dal Provvedimento generale dell'Autorità Garante della Privacy dell'8 aprile 2010 con redazione di adeguate informative;
5) Regole in ordine all'aggiornamento periodico del personale incaricato del trattamento nonché in ordine all'individuazione dell'ambito del trattamento consentito ai singoli incaricati;
6) Regole e istruzioni in ordine alla cancellazione dei dati personali.

a. Misure di sicurezza ambito tecnologico

Al fine di determinare le misure di sicurezza adeguate (art.32 c.1 gdpr) si è fatto riferimento allo specifico ambito di attività dell'organizzazione in oggetto ed al relativo rischio.

L'organizzazione in oggetto operando nell'ambito dei servizi sanitari alla persona, sulla base di autorizzazione del servizio sanitario regionale, per quanto attiene al rischio è assimilabile ad una Amministrazione Pubblica, pertanto per la definizione delle misure di sicurezza si può prendere a riferimento la Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015 *"MISURE MINIME DI SICUREZZA ICT PER LE PUBBLICHE AMMINISTRAZIONI"*

La Direttiva fornisce un riferimento utile a stabilire se il livello di protezione offerto da un'infrastruttura risponde alle esigenze operative, individuando anche gli interventi idonei per il suo adeguamento.

Il raggiungimento di elevati livelli di sicurezza, quando è molto elevata la complessità della struttura e

l'eterogeneità dei servizi erogati, può essere eccessivamente oneroso se applicato in modo generalizzato. Pertanto l'azienda dovrà avere cura di individuare al suo interno gli eventuali sottoinsiemi, tecnici e/o organizzativi, caratterizzati da omogeneità di requisiti ed obiettivi di sicurezza, all'interno dei quali potrà applicare in modo omogeneo le misure adatte al raggiungimento degli obiettivi stessi.

Titolare del trattamento

TE.RI. SRL

(MARA VILLANI)

_____

Misure di tutela dei dati personali (Rif. *ex* allegato B del D.lgs. 196/2003) gdpr 2016/679.

Al fine di verificare il rispetto delle misure necessarie a garantire la privacy dei dati personali contenuti negli archivi elettronici e cartacei dell'Azienda, è stata effettuata una verifica con i singoli uffici in relazione alla natura dei dati, al personale addetto ed alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

E' stata pertanto effettuata una analisi dei rischi presenti nell'attuale configurazione del sistema informatico aziendale e dell'ambiente in cui è posto dal punto di vista organizzativo, tecnico e dei comportamenti del personale autorizzato.

Sono state individuate le misure (intese come complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza) che configurano il livello di protezione richiesto in relazione ai rischi previsti, nonché gli strumenti che gli Amministratori di sistema e di rete devono rispettare in materia di sicurezza dei dati.

Il P.I.A. (Piano di Impatto Aziendale) rappresenta pertanto una sintesi dei risultati di tale verifica e delle misure adottate.

La realizzazione del programma di adeguamento ha consentito di dare piena attuazione alle misure di sicurezza di cui al gdpr 2016/679 nonché l'adozione di più ampie misure di sicurezza con la previsione di individuare anche gli ulteriori interventi di natura tecnica ed organizzativa necessari per mantenere gli idonei standard di sicurezza nel trattamento dei dati e il loro costante aggiornamento in relazione alla evoluzione tecnologica in materia.

Titolare del trattamento

TE.RI. SRL

(MARA VILLANI)

_____

Gli aggiornamenti del M.O.P. di TE.RI. srl potranno essere soggetti a modifiche ed integrazioni connesse al perdurare ed all'evolversi dell'emergenza epidemiologica ancora in atto nonché in osservanza delle ulteriori evoluzioni di carattere tecnico – scientifico che si dovessero rendere necessarie ai fini del contenimento del Virus Sars-Cov.2 anche ai fini della tracciabilità eventuale di soggetti interessati (sintomatici ed asintomatici) che potrebbero mettere in pericolo la salvaguardia della salute del personale operante presso il Centro nonché presso il domicilio dei pazienti dallo stesso Centro assistiti. Ogni eventuale ulteriore modifica ed integrazione del presente manuale, nonché ogni integrazione di carattere legislativo e/o tecnico-scientifico che dovesse essere imposta alla struttura da norme Comunitarie, Nazionali o Regionali o dalla struttura poste in essere ai fini della salvaguardia del bene superiore della salute pel proprio personale e della propria utenza sarà tempestivamente comunicata a cura del a cura del Titolare e/o del Responsabile del Trattamento.

Elenco allegati

A01 – Elenco sedi ed uffici nei quali avviene il trattamento dei dati;

A02 – Elenco sedi ed uffici nei quali avviene il trattamento dei dati affidato all'esterno della struttura del titolare (redatto solo all'occorrenza);

A03 – Elenco banche dati

A04 – Organigramma;

A05 – Piano di formazione

A06 – Criteri di assegnazione delle password nei sistemi di elaborazione

A07 – Modalità di protezione dei dati e dei locali;

A08 – Ulteriori misure in caso di trattamento di dati sensibili o giudiziari;

A09 – Elenco programmi adottati per la sicurezza dei dati trattati con strumenti elettronici;

A10 – Procedura di backup e ripristino dati;

A11 – Analisi dei rischi incombenti sui dati;

A12 – Modalità di trattamento dei dati senza l'ausilio di strumenti elettronici.

ROMA lì

REDATTO DA	ENTE	RESPOSABILE	DATA	FIRMA
Responsabile del trattamento	TE.RI. srl	Renato Bernardini	16.06.2018	

Gli aggiornamenti del M.O.P. di TE.RI. srl potranno essere soggetti a modifiche ed integrazioni connesse al perdurare ed all'evolversi dell'emergenza epidemiologica ancora in atto nonché in osservanza delle ulteriori evoluzioni di carattere tecnico – scientifico che si dovessero rendere necessarie ai fini del contenimento del Virus Sars-Cov.2 anche ai fini della tracciabilità eventuale di soggetti interessati (sintomatici ed asintomatici) che potrebbero mettere in pericolo la salvaguardia della salute del personale operante presso il Centro nonché presso il domicilio dei pazienti dallo stesso Centro assistiti. Ogni eventuale ulteriore modifica ed integrazione del presente manuale, nonché ogni integrazione di carattere legislativo e/o tecnico-scientifico che dovesse essere imposta alla struttura da norme Comunitarie, Nazionali o Regionali o dalla struttura poste in essere ai fini della salvaguardia del bene superiore della salute pel proprio personale e della propria utenza sarà tempestivamente comunicata a cura del a cura del Titolare e/o del Responsabile del Trattamento.

CONTROLLATO DA	ENTE	RESPONSABILE	DATA	FIRMA
DPO	TE.RI. SRL	Avv. Andrea Bernardini	16.06.2018	

APPROVATO DA	ENTE	RESPONSABILE	DATA	FIRMA
Titolare del trattamento	TE.RI. SRL	Mara Villani	16.06.2018	

REV. 2 DEL 03.06.2020

ROMA lì

REDATTO DA	ENTE	RESPOSANBILE	DATA	FIRMA
Responsabile del trattamento	TE.RI. srl	Renato Bernardini	03.06.2020	

CONTROLLATO DA	ENTE	RESPONSABILE	DATA	FIRMA
DPO	TE.RI. SRL	Avv. Andrea Bernardini	03.06.2020	

APPROVATO DA	ENTE	RESPONSABILE	DATA	FIRMA
Titolare del trattamento	TE.RI. SRL	Mara Villani	03.06.2020	

Gli aggiornamenti del M.O.P. di TE.RI. srl potranno essere soggetti a modifiche ed integrazioni connesse al perdurare ed all'evolversi dell'emergenza epidemiologica ancora in atto nonché in osservanza delle ulteriori evoluzioni di carattere tecnico – scientifico che si dovessero rendere necessarie ai fini del contenimento del Virus Sars-Cov.2 anche ai fini della tracciabilità eventuale di soggetti interessati (sintomatici ed asintomatici) che potrebbero mettere in pericolo la salvaguardia della salute del personale operante presso il Centro nonché presso il domicilio dei pazienti dallo stesso Centro assistiti. Ogni eventuale ulteriore modifica ed integrazione del presente manuale, nonché ogni integrazione di carattere legislativo e/o tecnico-scientifico che dovesse essere imposta alla struttura da norme Comunitarie, Nazionali o Regionali o dalla struttura poste in essere ai fini della salvaguardia del bene superiore della salute pel proprio personale e della propria utenza sarà tempestivamente comunicata a cura del a cura del Titolare e/o del Responsabile del Trattamento.