VILLA ESTHER
casa di cura

MANUALE OPERATIVO:
"ADEMPIMENTI PER IL TRATTAMENTO E LA PROTEZIONE DEI DATI PERSONALI"
REG.UE 2016/679 (G.D.P.R.)

LINEE GUIDA E PROCEDURE

Data revisione: gennaio 2022

D.P.O.: CIULLO SILVANA Silvana Ciullo

AUDITOR: GIANLUCA ANGELICOLA

A.D.S.: ERIO SALA

PREMESSA

La **Casa di Cura "Villa Esther"** di Bojano è un istituto clinico privato accreditato presso il Servizio Sanitario Nazionale (S.S.N.). La Clinica eroga prestazioni sia in regime di ricovero (ordinario, day hospital, day surgery), con una dotazione di 74 posti letto, sia in forma ambulatoriale in numerose branche specialistiche mediche, chirurgiche e riabilitative. Dispone inoltre di un servizio di diagnostica per immagini. L'accesso ai suoi servizi si effettua in convenzione con il S.S.N., muniti di richiesta del medico generico su ricettario regionale, o in forma privatistica

SCOPO E CAMPO DI APPLICAZIONE

Questo manuale è stato redatto con lo scopo di descrivere i principi e i criteri generali adottati dalla **Casa di Cura "Villa Esther"** in materia di protezione dati, nonché le modalità gestionali ed operative relative agli adempimenti connessi alla tutela dei dati personali a cui devono attenersi tutti coloro che a vario titolo possono essere coinvolti in trattamenti di dati personali.

La Casa di Cura "Villa Esther" ha adottato tutte quelle misure tecnico-organizzative che sono apparse idonee ad assicurare la *compliance* alle norme nazionali e comunitarie (REG.UE 2016/679 e D.lgs 101/18).

Ai fini del corretto espletamento degli adempimenti richiesti dal Regolamento UE 2016/679 "Regolamento generale sulla protezione dei dati" (di seguito anche "GDPR" o "Regolamento") il modello organizzativo prevede il coinvolgimento dei seguenti soggetti:

a) il **Titolare del trattamento**, in persona del legale rappresentante della società, cui compete la responsabilità delle scelte e delle decisioni relative alle misure da attuare per garantire la conformità alla normativa nonché la responsabilità del controllo sulla loro efficacia e sul loro rispetto da parte degli operatori;
b) il **DPO** – (Data Protection Officer);
c) gli **Autorizzati al trattamento**, ossia le persone fisiche incaricate per iscritto dal Titolare di compiere le operazioni di trattamento e che operano sotto la sua diretta autorità, attenendosi alle istruzioni agli stessi impartite;
d) i **Responsabili del trattamento**, che sono coloro (persona fisica o giuridica, autorità pubblica, servizio o altro organismo) che trattano dati personali per conto del titolare del trattamento: la società, anche attraverso appositi contratti con gli outsourcer, nominati responsabili del trattamento, garantisce che i dati personali oggetto di trattamento siano dai medesimi trattati in conformità a quanto previsto dal Regolamento e dalla normativa nazionale.

RIFERIMENTI NORMATIVI

- *Regolamento Generale sulla Protezione dei Dati (Reg. UE 2016/679);*
- *D.L. 196/2003 (Codice della privacy) così come novellato dal D.lgs. 101/2018;*
- *Linee Guida 5/2020 "Sul consenso ai sensi del regolamento (UE) 2016/679", adottate dal Comitato Europeo per la protezione dei dati, il 4 maggio 2020;*
- *Linee-guida sulle notifiche di violazioni dei dati personali.*

RIFERIMENTI DOCUMENTALI

MODELLO	DESCRIZIONE	RIFERIMENTO
MD PRE INF ANALISI - REV._04_2020	Informativa resa ai pazienti dall'accettazione	Allegato 1
MD PRE INF RICOVERO - REV._04_2020		Allegato 2
INFO REFERTO ONLINE REV 01		Allegato 3
PRIVACY POLICY	Informativa pubblicata sul sito: https://www.villaestherbojano.it/privacy/	Allegato 4
INFORMATIVA REFERTO ONLINE REV 01_2021		Allegato 1
INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI PRENOTAZIONE ON-LINE		Allegato 2
INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI E ACQUISIZIONE DEL CONSENSO		Allegato 3
NOMINA SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI	Nomina resa all'assunzione e consegnata a tutti i dipendenti dal 25 maggio 2018 (redatta tramite il software AGYO Privacy)	Allegato 5
NOMINA RESPONSABILI ESTERNI (EX ART.28 REG.UE 2016/679)		Allegato 6
MD PRD PRIVACY DIPENDENTI REV_ 01_2020	Nomina resa all'assunzione e consegnata a tutti i dipendenti dal 25 maggio 2018	Allegato 7

MODELLO	DESCRIZIONE	RIFERIMENTO
INFORMATIVA TRIAGE	Modulistica redatta da Marzo 2020 a seguito delle Disposizioni Nazionali per il contrasto e contenimento della diffusione del Virus Covid-19 negli ambienti di lavoro	Allegato 8
NOTA INTEGRATIVA - DIPENDENTI E COLLABORATORI		Allegato 9
SCHEDA PERSONALE MISURAZIONE TEMPERATURA CORPOREA		Allegato 10
INTEGRAZIONE INFORMATIVA		
INFORMATIVA GREEN PASS DIPENDENTI E COLLABORATORI_REV_01_2021		Allegato 11
NOMINA SOGGETTI AUTORIZZATI_COVID19_GREEN PASS_VERFICATORE_REV_01		Allegato 12
NOMINA SOGGETTI AUTORIZZATI_COVID19_GREEN PASS_ AMMINISTRATIVO_REV_01		Allegato 13
PROCEDURA CONTROLLO GREEN PASS_REV_01		Allegato 14
FASE 2 INFORMATIVA_COMPLETA		Allegato 15

MODELLO	DESCRIZIONE	RIFERIMENTO
REGISTRO FORMAZIONE ADEGUAMENTO PRIVACY_PERSONALE	Modulistica prodotta dal referente privacy	Allegato 16
REGISTRO DELLE CHIAVI E DELLE MAIL		Allegato 17
REGISTRO DEGLI ASSET		Allegato 18
POLICY_PER_LA_GESTIONE_DEI_DATA_BREACH_REV_02_2021	Modulistica prodotta dal referente privacy a seguito di istruzioni dell'ADS, revisionata dal DPO e da un Auditor esterno	Allegato 19
REGISTRO DEI TRATTAMENTI (COVID)	Integrazione al Registro dei Trattamenti in seguito delle Disposizioni Nazionali per il contrasto e contenimento della diffusione del Virus Covid-19 negli ambienti di lavoro	Allegato 20
GESTIONE STRUMENTI IT E LINEE GUIDA SICUREZZA NELL'ACCESSO AI DATI_rev_01_22	Modulistica prodotta dall'ADS su specifiche indicazioni del Titolare, revisionata dal DPO e da un Auditor esterno	Allegato 21
REGISTRO DEI TRATTAMENTI (estratto)	Registro dei Trattamenti obbligatorio ai sensi dell'Art.32 del REG.UE 2016/679 (redatto ed aggiornato tramite il software AGYO Privacy)	Allegato 22

DEFINIZIONI

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

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

3) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

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

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

6) **«archivio»:** qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

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

8) «**responsabile del trattamento**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

9)«**destinatario**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

10) «**terzo**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

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

12) «**violazione dei dati personali**»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

13) «**dati genetici**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

14) «**dati biometrici**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
15) «**dati relativi alla salute**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

16) «**stabilimento principale**»: a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale; b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

17) «**rappresentante**»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

18) «**impresa**»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

19) «**gruppo imprenditoriale**»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate; 20) «norme vincolanti d'impresa»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o

responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

21) «**autorità di controllo**»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 Reg. Ue 2016/679;

22) «**autorità di controllo interessata**»: un'autorità di controllo interessata dal trattamento di dati personali in quanto: a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo; b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure c) un reclamo è stato proposto a tale autorità di controllo;

23) «**trattamento transfrontaliero**»: a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

24) «**obiezione pertinente e motivata**»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del regolamento UE 2016/679, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al suddetto regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

25) «**servizio della società dell'informazione**»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio (1);

26) «**organizzazione internazionale**»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati

27) **«comunicazione»:** il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione Europea, dal responsabile o dal rappresentante nel territorio dell'Unione Europea, dalle persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interlocuzione.

28) **«diffusione»:** il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante loro messa a disposizione o consultazione.

FUNZIONI INTERNE ED ESTERNE

Il TITOLARE DEL TRATTAMENTO

Il Titolare del trattamento, è la **CASA DI CURA VILLA ESTHER SRL, rappresentato dall'Amministratore Unico** a cui competono le decisioni in ordine alle finalità e ai mezzi del trattamento dei dati personali e che ne risponde di fronte alla legge, oltre che la responsabilità delle scelte e delle decisioni relative alle misure da attuare per garantire la conformità alla normativa nonché la responsabilità del controllo sulla loro efficacia e sul loro rispetto da parte degli operatori (**principio di *accountability***).

In particolare il Titolare:

- determina le **finalità** del trattamento, ovvero gli obbiettivi e gli scopi per i quali si procede al trattamento;
- determina le **modalità** di trattamento, quindi le categorie di dati trattati, le operazioni di trattamento, i soggetti coinvolti nelle singole operazioni;
- individua i soggetti esterni all'Organizzazione ai quali affidare uno o più trattamenti (*cfr.* Responsabili esterni del trattamento);
- determina i soggetti o le categorie di soggetti a cui i dati possono essere comunicati;
- determina se i dati possano essere diffusi e l'ambito di diffusione;
- determina la durata di conservazione dei dati;
- determina gli strumenti utilizzati per effettuare il trattamento
- determina le misure di sicurezza atte a garantire, su base permanente, la riservatezza, l'integrità e la disponibilità dei dati.
- assicura il rispetto di principi informativi del trattamento di dati personali ovvero che i dati: siano trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- stabilisce procedure appropriate per garantire all'interessato i diritti di cui agli artt. 15-23 del Regolamento UE 2016/679;
- redige un Registro delle attività di Trattamento (art. 30 Reg. UE 2016/679);
- stabilisce protocolli e procedure da attivare in caso di violazione dei dati personali (*data breach*);
- Effettua una Valutazione di impatto sulla protezione dei dati (DPIA) allorché un tipo di trattamento preveda l'uso di nuove tecnologie e, considerata la natura, l'oggetto, il contesto e le finalità di trattamento, possa presentare un rischio per i diritti e le libertà delle persone fisiche.
- designa un Responsabile della Protezione dei Dati (DPO) nei casi di cui all'art. 37 del REG.UE 2016/679.

RESPONSABILE ESTERNO DEL TRATTAMENTO

La selezione dei responsabili (esterni) del trattamento (cfr. definizioni) è preordinata al possesso di garanzie e requisiti di sicurezza adeguati a tutelare riservatezza, integrità e disponibilità dei dati.

Per tali motivi il Responsabile non può ricorrere ad altro responsabile (sub-responsabile) senza previa autorizzazione scritta da parte del Titolare.

L'incarico, il contratto di servizio o di fornitura deve essere accompagnato da un altro atto giuridico, da un *addendum*, o da una serie di clausole riguardanti la disciplina dei trattamenti in oggetto ed in particolare: la durata, la natura e le finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento; che il responsabile del trattamento:

a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il

responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
c) adotti tutte le misure richieste ai sensi dell'articolo 32 del Reg. 2016/679;
d) non ricorra ad altro responsabile senza previa autorizzazione da parte del Titolare;
e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del Reg. UE 2016/679, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;
h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI

Agiscono sotto l'autorità del Titolare del trattamento e sono coloro che materialmente effettuano operazioni di trattamento di dati: nel contesto aziendale, dunque, con modalità ed abilitazioni diverse secondo le rispettive competenze, trattasi tanto di personale sanitario che tecnico o amministrativo.

Tutte le risorse devono essere formate sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

La formazione riguarda i principi generali e le norme applicabili alle operazioni di trattamento generalmente intese, gli obblighi che tali figure hanno nei confronti dei pazienti, degli assistiti e del Titolare del trattamento e le misure di sicurezza e buone prassi richieste nello svolgimento della loro attività professionale.

In particolare la formazione approfondisce almeno i seguenti argomenti:

1. **Inquadramento normativo sulla protezione dei dati;**
   - Diritto alla riservatezza, diritto alla tutela della sfera di vita privata ed evoluzione al diritto al corretto trattamento dei dati personali come diritto con propria autonoma dignità;
   - Elementi essenziali del diritto alla protezione dei dati personali.

2. **Il Regolamento europeo sulla protezione dei dati personali: oggetto e finalità;**
   - Criticità delle moderni strumenti di condivisione delle informazioni;
   - Tutela preventiva della violazione dei dati personali attraverso norme di natura amministrativa;
   - Novità introdotte con il Reg. UE 679/2016.

3. **Definizioni e principi applicabili al trattamento dei dati personali;**
   - Definizioni;
   - Correttezza, trasparenza e legalità;
   - Minimizzazione dei dati e limitazione delle finalità.

4. **Le categorie particolari di dati;**

5. **Basi giuridiche, limiti ed eccezioni al trattamento dei dati particolari;**
   - Art. 6 ed art. 9 del Reg. UE 679/2016.

6. **Consenso al trattamento dei dati personali;**
   - Art. 7 del Reg. UE 679/2016.

7. **Disciplina per il trattamento dei dati relativi alla salute in ambito sanitario:**
   - Trattamenti per finalità di cura;
   - Particolari casi di trattamento di dati sanitari;
   - Trattamenti per finalità di sanità pubblica;
   - Trattamenti per motivi di interesse pubblico rilevante in ambito sanitario.

8. **Il responsabile esterno al trattamento dei dati ed il soggetto incaricato: definizione delle responsabilità e obbligo di segretezza (nomina degli incaricati al trattamento e "profondità di accesso" alle informazioni sanitarie dei pazienti);**

9. **Diritti degli interessati;**

10. **Sanzioni:**
    - Responsabilità civile e penale ed amministrativa per violazione dei dati personali.

A tutti i designati dovranno essere date istruzioni specifiche riguardo le operazioni di trattamento loro affidate. Ciò dovrebbe avvenire attraverso un **atto formale di nomina a soggetto autorizzato al trattamento** contenente, per ogni trattamento: operazioni di trattamento consentite, finalità del trattamento, categorie di dati trattati, categorie di interessati ed *asset*.
La nomina contiene inoltre una sintesi delle misure di sicurezza organizzative a cui il personale deve attenersi.
Il personale dipendente è inoltre tenuto a conoscere ed osservare tutti i regolamenti interni, ivi incluso il **regolamento di utilizzo degli strumenti informatici e telematici** e le procedure da attivare in caso di Data Breach.

All'interno della Casa di Cura Villa Esther sono presenti le seguenti figure professionali:

a) **PERSONALE INFERMIERISTICO:**
   - Infermiere: DM 739/1994
   - Assistente sanitario: DM 69/97

b) **PERSONALE DELLA RIABILITAZIONE:**
   - Fisioterapista: DM 741/1994

c) **OPERATORI TECNICI**

d) **OPERATORI SOCIO-SANITARI**

e) **PERSONALE AMMINISTRATIVO E TECNICO**

RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI (DPO)

Figura professionale ha cui è riservata la prerogativa di garantire piena ed effettiva esecuzione del Regolamento Generale sulla Protezione dei Dati.

Il DPO è incaricato almeno dei seguenti compiti:

a) informare e fornire consulenza al Titolare del trattamento o al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

c) fornire, se richiesto, un parere in merito alla **valutazione d'impatto sulla protezione dei dati** e sorvegliarne lo svolgimento;

d) cooperare con l'autorità di controllo;

e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Reg. UE 2016/679, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

AMMINISTRATORE DI SISTEMA

All'Amministratore di Sistema (ADS) sono attribuiti i seguenti compiti:

- sovrintendere alle risorse del sistema informatico centralizzato e consentirne l'utilizzazione a tutti i responsabili e gli incaricati che ne abbiano titolo, mediante l'adozione dei sistemi di sicurezza adeguati alla protezione dei dati personali;
- garantire la gestione e manutenzione degli strumenti elettronici aziendali;
- garantire la protezione dei dispositivi e dei programmi 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 da aggiornare con cadenza almeno semestrale;
- garantire gli aggiornamenti periodici e a correggerne difetti dei sistemi IT;
- impartire istruzioni organizzative e tecniche che prevedono il salvataggio dei dati;
- adottare idonee misure che assicurino l'integrità e la disponibilità dei dati;
- adottare idonee misure che assicurino il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati.

ISTRUZIONI DI BASE AGLI INCARICATI DEL TRATTAMENTO

Nell'ambito delle mansioni affidate, i soggetti incaricati al trattamento sono istruiti affinché i dati personali siano:

- trattati in modo lecito e secondo correttezza;
- raccolti e registrati per scopi determinati, espliciti e legittimi;
- aggiornati;
- pertinenti, completi e non eccedenti rispetto alle finalità del trattamento;
- conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario al raggiungimento delle finalità preposte.

L'incaricato al trattamento, inoltre, anche quando soggetto al segreto professionale, deve:

- assicurare la riservatezza nonché la protezione dei dati personali dei quali venga a conoscenza durante l'esecuzione dei servizi prestati;
- utilizzare i dati personali solo per le finalità connesse allo svolgimento delle attività sopra richiamate, con divieto di qualsiasi altra diversa utilizzazione.
- controllare e custodire fino alla restituzione gli atti e i documenti contenenti dati personali sensibili o giudiziari affidatigli per lo svolgimento dei propri compiti in maniera che ad essi non accedano persone prive di autorizzazione, restituendoli al termine delle operazioni affidate
- assicurare il rispetto delle misure di sicurezza sviluppando misure idonee a prevenire l'eventuale distruzione, dispersione o accesso non autorizzato ai documenti, e adottando, in presenza di specifici rischi, particolari cautele quali la consultazione in copia di alcuni documenti e la conservazione degli originali in cassaforte o armadi blindati;
- non fare alcun uso delle informazioni non disponibili agli utenti o non rese pubbliche, ottenute in ragione della propria attività anche in via confidenziale, per proprie ricerche o per realizzare profitti e interessi privati;
- non utilizzare strumenti di social networking per la condivisione di dati personali riferiti a pazienti;
- non raccogliere immagini dei pazienti mediante dispositivi elettronici di ripresa non autorizzati, inclusi telefoni cellulari.

IL TRATTAMENTO DEI DATI IN FORMATO CARTACEO

Casa di Cura Privata Villa Esther S.r.l., per garantire il corretto trattamento dei dati personali comuni e appartenenti a Categorie particolari di dati personali contenuti in documenti cartacei, fornisce le seguenti istruzioni:

- gli atti e i documenti andranno gestiti in condizioni di riservatezza, evitandone il libero accesso da parte di terzi estranei, facendo uso di armadi, cassettiere e altri mobili muniti di serratura.
  All'uopo verranno nominati formalmente e riportato su apposito registro i soggetti designati alla custodia delle chiavi e degli archivi.
- al termine dell'attività lavorativa tutti i documenti contenenti dati personali dovranno essere riposti negli armadi, chiusi a chiave; gli armadi ubicati in luoghi non presidiati (corridoi, vani scale, locali comuni di piano etc.), contenenti dati personali, dovranno essere dotati di serratura e dovranno naturalmente essere tenuti chiusi a chiave;
  garantire la riservatezza anche in occasione della eventuale distruzione o invio a macero del materiale contenente dati personali.

ALLEGATI

VILLA ESTHER
casa di cura

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI ED ACQUISIZIONE DEL CONSENSO

AI SENSI DEGLI ARTT. 13 E 9 DEL REG.UE 2016/679

PAZIENTE (Interessato):

NOME	_____	*COGNOME*	_____
DATA DI NASCITA	____/____/____	LUOGO DI NASCITA	_____

1. PERCHÉ LE FORNIAMO QUESTE INFORMAZIONI

Ai sensi del Regolamento UE 2016/679 (di seguito Regolamento o GDPR), con il presente documento vogliamo illustrare le modalità adottate da **Casa di Cura Privata Villa Esther S.r.l.** per il trattamento dei Suoi dati personali.

2. PRINCIPI APPLICABILI ALLE ATTIVITÀ DI TRATTAMENTO

Il trattamento dei Suoi dati personali avviene nel rispetto dei principi fissati all'articolo 5 del Regolamento UE 2016/679, che qui si ricordano brevemente:

- liceità, correttezza e trasparenza del trattamento, nei confronti dell'interessato;
- limitazione della finalità del trattamento, compreso l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati;
- minimizzazione dei dati: ossia, i dati devono essere adeguati pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento;
- esattezza e aggiornamento dei dati, compresa la cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;
- limitazione della conservazione: ossia, è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
- integrità e riservatezza: occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento.

3. TITOLARE DEL TRATTAMENTO

Il Titolare del trattamento è **Casa di Cura Privata Villa Esther S.r.l.**, raggiungibile ai seguenti indirizzi:
Casa di Cura Privata Villa Esther S.r.l., via Gino Di Biase n. 18 – 86021 Bojano (CB) Tel. 0874/751001 - privacy@villaesther.it.

4. DATA PROTECTION OFFICER DPO/RESPONSABILE DELLA PROTEZIONE DEI DATI RPD

Casa di Cura Privata Villa Esther S.r.l. ha provveduto a nominare il Responsabile della protezione dei dati, che è raggiungibile ai seguenti indirizzi:
Casa di Cura Privata Villa Esther S.r.l., via Gino Di Biase n. 18 – 86021 Bojano (CB) Tel. 0874/751001 - privacy@villaesther.it.

5. LE FINALITÀ E LA BASE GIURIDICA DEL TRATTAMENTO.

I dati personali acquisiti dal Titolare, ai sensi del REG.UE 2016/679, sono trattati per le seguenti finalità:

MODALITÀ DEL TRATTAMENTO	FINALITÀ	BASE GIURIDICA
I DATI PERSONALI sono raccolti, archiviati e protetti nel pieno rispetto dei principi dettati dal REG.UE 2016/679 e dal D.lgs 101/18.	approfondire lo stato di salute attuale	Art.6.1 c) - Art. 9.2 h) REG.UE 2016/679
	permettere la corretta identificazione delle analisi cliniche, delle immagini diagnostiche, degli esami cardiologici, ortopedici, endoscopici, oculistici, di chirurgia generale, urologia e pneumologia;	Art.6.1 c) - Art. 9.2 h) REG.UE 2016/679
	permettere il regolare svolgimento dei prelievi, delle operazioni radiologiche e delle procedure cardiologiche, ortopediche, endoscopiche, oculistiche, di chirurgia generale, urologia e pneumologia;	Art.6.1 c) - Art. 9.2 h) REG.UE 2016/679
	archiviare i dati per esigenze future	Art.6.1 c) - Art. 9.2 h) REG.UE 2016/679
	registrare i dati sanitari per fini gestionali o di fatturazione.	Art.6.1 c) - Art. 9.2 a) REG.UE 2016/679
	espletare ricerche scientifiche in campo medico, biomedico o epidemiologico.	Ar.2-sexies del D.lgs 101/18 e art.9 par.4 REG.UE 2016/679

6. DESTINATARI DEI DATI

I dati possono essere trattati da:

- soggetti esterni operanti in qualità di titolari quali, a titolo esemplificativo, autorità ed organi di vigilanza e controllo ed in generale soggetti, pubblici o privati, legittimati a richiedere i dati (es. ASREM per consegna impegnative, SOGEI S.p.a.);
- soggetti esterni designati come responsabili del trattamento ai sensi dell'art. 28 del GDPR, a cui sono impartite adeguate istruzioni operative: Laboratori esterni per talune analisi specialistiche. L'elenco completo dei Responsabili del trattamento è disponibile presso il titolare del trattamento **Casa di Cura Privata Villa Esther S.r.l.**
- Enti o organismi di ricerca autorizzati dall'ordinamento nazionale o sovranazionale all'espletamento di ricerche scientifiche in campo medico, biomedico o epidemiologico (sarà applicato prevalentemente il principio di pseudonimizzazione).

7. PERIODO DI CONSERVAZIONE DEI DATI

I dati forniti verranno conservati per il tempo necessario per adempiere alle finalità citate, e per un periodo successivo non definibile per adempiere agli obblighi di legge previsti per il titolare.

ALLEGATO 1

VILLA ESTHER
casa di cura

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI ED ACQUISIZIONE DEL CONSENSO

AI SENSI DEGLI ARTT. 13 E 9 DEL REG.UE 2016/679

8. TRASFERIMENTO DEI DATI PERSONALI A PAESE TERZO O AD UNA ORGANIZZAZIONE INTERNAZIONALE

I dati personali non sono trasferiti in paesi terzi o ad organizzazioni internazionali.

9. ATTIVITÀ DI PROFILAZIONE

I dati personali acquisiti non sono oggetto di processi decisionali automatizzati, inclusa la "profilazione" che consiste in una forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato, ove ciò produca effetti giuridici che la riguardano o incida in modo analogo significativamente sulla sua persona.

10. DIRITTI RICONOSCIUTI E MODALITÀ DI ESERCIZIO

Gli interessati del trattamento, oltre al diritto di proporre reclamo a un'autorità di controllo, possono esercitare i seguenti diritti:

Art. 15 Diritto di accesso - L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle informazioni riguardanti il trattamento.

Art. 16 Diritto di rettifica - L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Art. 17 Diritto alla cancellazione (diritto all'oblio) - L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali.

Art. 18 Diritto di limitazione del trattamento - L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:

a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;

b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;

c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;

d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1 del regolamento, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

Art. 20 Diritto alla portabilità dei dati - L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti.

Nell'esercitare i propri diritti relativamente alla portabilità dei dati, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.

Art. 21 Diritto di opposizione - L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano compresa la profilazione sulla base di tali disposizioni.

Art. 22 Diritto di non essere sottoposto a processo decisionale automatizzato, compresa la profilazione - L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

I diritti possono essere esercitati facendo richiesta direttamente al Titolare del trattamento o al Responsabile della protezione dei dati (RPD), contattabili agli indirizzi riportati p.to 3 e 4. L'interessato può presentare reclamo al GARANTE PER LA PROTEZIONE DEI DATI PERSONALI www.garanteprivacy.it) oppure al EUROPEAN DATA PROTECTION SUPERVISOR (www.edps.europa.eu).

Dopo aver letto e compreso il presente documento, __l__ sottoscritt__ **AUTORIZZA il trattamento dei propri dati personali idonei a rivelare lo stato di salute nonché alle particolari categorie di dati personali per finalità amministrativo-contabili nonché alla loro comunicazione, per le medesime finalità, agli organismi pubblici autorizzati al recepimento di tali informazioni ed a professionisti in materia contabile e fiscale. Il consenso è necessario allo svolgimento del servizio di cura ed in caso di diniego Villa Esther srl non potrà dare esecuzione al servizio medesimo.**

Bojano (CB), ____/____/_____

firma leggibile per presa visione ed accettazione: _____

PERSONA DIVERSA DA INTERESSATO SE INTERDETTO/INABILITATO O MINORE:

Nome _____ Cognome _____

C.F. ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

Rapporto con Interessato ☐ Tutore ☐ Curatore ☐ Genitore ☐ Altro: _____)

Bojano (CB), ____/____/_____

firma leggibile per presa visione ed accettazione: _____

ALLEGATO 2

VILLA ESTHER
casa di cura

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI ED ACQUISIZIONE DEL CONSENSO

AI SENSI DEGLI ARTT. 13 E 9 DEL REG.UE 2016/679

PAZIENTE (Interessato):

NOME	_____	*COGNOME*	_____
DATA DI NASCITA	____/____/____	LUOGO DI NASCITA	_____

1. PERCHÉ LE FORNIAMO QUESTE INFORMAZIONI

Ai sensi del Regolamento UE 2016/679 (di seguito Regolamento o GDPR), con il presente documento vogliamo illustrare le modalità adottate da **Casa di Cura Privata Villa Esther S.r.l.** per il trattamento dei Suoi dati personali.

2. PRINCIPI APPLICABILI ALLE ATTIVITÀ DI TRATTAMENTO

Il trattamento dei Suoi dati personali avviene nel rispetto dei principi fissati all'articolo 5 del Regolamento UE 2016/679, che qui si ricordano brevemente:

- liceità, correttezza e trasparenza del trattamento, nei confronti dell'interessato;
- limitazione della finalità del trattamento, compreso l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati;
- minimizzazione dei dati: ossia, i dati devono essere adeguati pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento;
- esattezza e aggiornamento dei dati, compresa la cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;
- limitazione della conservazione: ossia, è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
- integrità e riservatezza: occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento.

3. TITOLARE DEL TRATTAMENTO

Il Titolare del trattamento è **Casa di Cura Privata Villa Esther S.r.l.,** raggiungibile ai seguenti indirizzi:
Casa di Cura Privata Villa Esther S.r.l., via Gino Di Biase n. 18 – 86021 Bojano (CB) Tel. 0874/751001 - privacy@villaesther.it.

4. DATA PROTECTION OFFICER DPO/RESPONSABILE DELLA PROTEZIONE DEI DATI RPD

Casa di Cura Privata Villa Esther S.r.l. ha provveduto a nominare il Responsabile della protezione dei dati, che è raggiungibile ai seguenti indirizzi:
Casa di Cura Privata Villa Esther S.r.l., via Gino Di Biase n. 18 – 86021 Bojano (CB) Tel. 0874/751001 - privacy@villaesther.it.

5. LE FINALITÀ E LA BASE GIURIDICA DEL TRATTAMENTO.

I dati personali acquisiti dal Titolare, ai sensi del REG.UE 2016/679, sono trattati per le seguenti finalità:

MODALITÀ DEL TRATTAMENTO	FINALITÀ	BASE GIURIDICA
I DATI PERSONALI sono raccolti, archiviati e protetti nel pieno rispetto dei principi dettati dal REG.UE 2016/679 e dal D.lgs 101/18.	Compilazione cartella clinica e cartella amministrativa.	Art.6.1 c) - Art. 9.2 h) REG.UE 2016/679; D.P.R 128/1969; Circ. Min. Sanità 19/12/86, n. 61;
	regolare svolgimento delle prestazioni sanitarie richieste (terapie, cure, diagnosi e dimissione). Compilazione scheda di dimissione ospedaliera.	Art.6.1 c) - Art. 9.2 h) REG.UE 2016/679; D.M. 28/12/1991
	archiviare i dati per esigenze future.	Art.6.1 c) - Art. 9.2 h) REG.UE 2016/679
	registrare i dati sanitari per fini gestionali o di fatturazione.	Art.6.1 c) - Art. 9.2 a) REG.UE 2016/679
	espletare ricerche scientifiche in campo medico, biomedico o epidemiologico.	Ar.2-sexies del D.lgs 101/18 e art.9 par.4 REG.UE 2016/679

6. DESTINATARI DEI DATI

I dati possono essere trattati da:

- soggetti esterni operanti in qualità di titolari quali, a titolo esemplificativo, autorità ed organi di vigilanza e controllo ed in generale soggetti, pubblici o privati, legittimati a richiedere i dati (es. ASREM per consegna impegnative, SOGEI S.p.a.) o, dietro specifica richiesta, all'Autorità Giudiziaria.
- soggetti esterni designati come responsabili del trattamento ai sensi dell'art. 28 del GDPR, a cui sono impartite adeguate istruzioni operative: Laboratori esterni per talune analisi specialistiche. L'elenco completo dei Responsabili del trattamento è disponibile presso il titolare del trattamento **Casa di Cura Privata Villa Esther S.r.l.;**
- Enti o organismi di ricerca autorizzati dall'ordinamento nazionale o sovranazionale all'espletamento di ricerche scientifiche in campo medico, biomedico o epidemiologico (sarà applicato prevalentemente il principio di pseudonimizzazione).

7. PERIODO DI CONSERVAZIONE DEI DATI

I dati forniti verranno conservati per il tempo necessario per adempiere alle finalità citate, le cartelle cliniche vengono conservate illimitatamente secondo quanto previsto dalla normativa vigente.

8. TRASFERIMENTO DEI DATI PERSONALI A PAESE TERZO O AD UNA ORGANIZZAZIONE INTERNAZIONALE

I dati personali non sono trasferiti in paesi terzi o ad organizzazioni internazionali.

9. ATTIVITÀ DI PROFILAZIONE

I dati personali acquisiti non sono oggetto di processi decisionali automatizzati, inclusa la "profilazione" che consiste in una forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti

riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato, ove ciò produca effetti giuridici che la riguardano o incida in modo analogo significativamente sulla sua persona.

10. DIRITTI RICONOSCIUTI E MODALITÀ DI ESERCIZIO

Gli interessati del trattamento, oltre al diritto di proporre reclamo a un'autorità di controllo, possono esercitare i seguenti diritti:

Art. 15 Diritto di accesso - L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle informazioni riguardanti il trattamento.

Art. 16 Diritto di rettifica - L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Art. 17 Diritto alla cancellazione (diritto all'oblio) - L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali.

Art. 18 Diritto di limitazione del trattamento - L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:

a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;

b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;

c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;

d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1 del regolamento, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

Art. 20 Diritto alla portabilità dei dati - L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti.

Nell'esercitare i propri diritti relativamente alla portabilità dei dati, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.

Art. 21 Diritto di opposizione - L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano compresa la profilazione sulla base di tali disposizioni.

Art. 22 Diritto di non essere sottoposto a processo decisionale automatizzato, compresa la profilazione - L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

I diritti possono essere esercitati facendo richiesta direttamente al Titolare del trattamento o al Responsabile della protezione dei dati (RPD), contattabili agli indirizzi riportati p.to 3 e 4. L'interessato può presentare reclamo al GARANTE PER LA PROTEZIONE DEI DATI PERSONALI www.garanteprivacy.it) oppure al EUROPEAN DATA PROTECTION SUPERVISOR (www.edps.europa.eu).

Dopo aver letto e compreso il presente documento, __l__ sottoscritt__ **AUTORIZZA** il trattamento dei propri dati personali idonei a rivelare lo stato di salute nonché alle particolari categorie di dati personali per finalità amministrativo-contabili nonché alla loro comunicazione, per le medesime finalità, agli organismi pubblici autorizzati al recepimento di tali informazioni ed a professionisti in materia contabile e fiscale. **Il consenso è necessario allo svolgimento del servizio di cura ed in caso di diniego Villa Esther srl non potrà dare esecuzione al servizio medesimo.**

Bojano (CB), ____/____/_____

firma leggibile per presa visione ed accettazione: _____

PERSONA DIVERSA DA INTERESSATO SE INTERDETTO/INABILITATO O MINORE:

Nome _____ Cognome _____

C.F. ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐

Rapporto con Interessato ☐ Tutore ☐ Curatore ☐ Genitore ☐ Altro: _____)

Bojano (CB), ____/____/_____

firma leggibile per presa visione ed accettazione: _____

__l__ sottoscritt__, inoltre, AUTORIZZA il personale sanitario della struttura a fornire informazioni circa il proprio stato di salute a:

_____

(NOME E COGNOME)

_____

(NOME E COGNOME)

ALLEGATO 3

VILLA ESTHER
casa di cura

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI PER REFERTAZIONE ON-LINE

AI SENSI DELL'ART. 13 DEL REG.UE 2016/679
Rev_01_2021

Gent.mo Interessato (Paziente),

ai sensi del Regolamento UE 2016/679 (di seguito Regolamento o GDPR), con il presente documento vogliamo illustrare le modalità adottate dalla **Casa di Cura Privata Villa Esther S.r.l.** per il trattamento dei Suoi dati personali con riferimento all'erogazione dei servizi facoltativi di refertazione *on-line*, messi a disposizione dei pazienti e utenti dalla struttura sanitaria del Titolare.

TITOLARE DEL TRATTAMENTO	**Casa di Cura Privata Villa Esther S.r.l.** Via Gino Di Biase n. 18 – 86021 Bojano (CB) Tel. 0874/751001 - privacy@villaesther.it
DATA PROTECTION OFFICER (DPO)	privacy@villaesther.it
PRINCIPI APPLICABILI ALLE ATTIVITÀ DI TRATTAMENTO	Il trattamento dei Suoi dati personali avviene nel rispetto dei principi fissati all'art.5 del REG.UE 2016/679, che qui si ricordano brevemente: • liceità, correttezza e trasparenza del trattamento, nei confronti dell'interessato; • limitazione della finalità del trattamento; • minimizzazione dei dati: ossia, i dati devono essere adeguati pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento; • esattezza e aggiornamento dei dati, compresa la cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento; • limitazione della conservazione; • integrità e riservatezza: occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento.
DATI PERSONALI OGGETTO DEL TRATTAMENTO	Il Titolare tratterà i Suoi dati personali, raccolti in occasione e nell'ambito della Sua specifica richiesta di accedere e usufruire dei servizi di refertazione on-line con riferimento alle seguenti categorie di referti: **risultati di tutti gli esami di laboratorio e analisi cliniche svolti presso Casa di Cura Privata Villa Esther.** Tali dati sono sia dati comuni, tra cui, a titolo esemplificativo e non esaustivo, nome, cognome, numero di telefono mobile, indirizzo e-mail e, in generale, i dati di contatto sia dati relativi a particolari categorie di cui all'art. 9 del GDPR, vale a dire dati idonei a rivelare, tra l'altro, l'origine razziale ed etnica, nonché dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi allo stato di salute e alla vita sessuale.

LE FINALITÀ E LA BASE GIURIDICA DEL TRATTAMENTO

I dati personali acquisiti dal Titolare, ai sensi del REG.UE 2016/679, sono trattati per le seguenti finalità:

TRATTAMENTO	FINALITÀ	BASE GIURIDICA
I DATI PERSONALI sono raccolti, archiviati e protetti nel pieno rispetto dei principi dettati dal REG.UE 2016/679 e dal D.lgs 101/18.	I Suoi Dati Personali saranno trattati nell'ambito della normale attività del Titolare, per consentirLe di consultare direttamente on-line, mediante registrazione e accesso all'area riservata del sito Web, i Referti dei propri accertamenti diagnostici eseguiti nelle strutture del Titolare.	Per le finalità sopra indicate, la base di legittimità dei trattamenti è il Suo specifico consenso *ex* artt. 6, par. 1, lett. a) e art. 9, par. 2, lett. a), del GDPR.

Previa prestazione del Suo consenso al momento della accettazione, il Titolare Le fornirà il codice identificativo dell'esame e le istruzioni per accedere servizio di refertazione *on-line*, nonché apposite istruzioni circa le modalità tecniche di funzionamento dei servizi stessi, alle quali si rinvia.

Lei potrà inoltre manifestare il Suo consenso direttamente on-line all'atto della registrazione/autenticazione sul portale messo a diposizione del Titolare per la consegna dei Referti.

E', comunque, Suo diritto manifestare una volontà contraria, in relazione ai singoli esami clinici a cui si sottoporrà di volta in volta, ovvero che i relativi referti non siano oggetto del servizio di refertazione on-line precedentemente scelto.

NON POSSONO ESSERE COMUNICATI TRAMITE MODALITÀ DIGITALI ACCERTAMENTI RELATIVI AD INDAGINI GENETICHE O ALL'HIV.

MODALITÀ DEL TRATTAMENTO

Il trattamento dei Dati Personali avverrà – secondo i principi correttezza, liceità e trasparenza – tramite supporti e/o strumenti informatici, manuali e/o telematici, con logiche strettamente correlate alle finalità del trattamento e comunque garantendo la riservatezza e sicurezza dei dati stessi e il rispetto degli obblighi specifici sanciti dalla legge.

La disponibilità, la gestione, l'accesso, la conservazione e la fruibilità dei dati è garantita dall'adozione di misure tecniche e organizzative per assicurare idonei livelli di sicurezza ai sensi degli artt. 25 e 32 del GDPR, nonché per assicurare la conformità alle pertinenti disposizioni di settore secondo il diritto dell'Unione Europea e il diritto nazionale, ivi comprese le Linee Guida in tema di referti on-line del Garante per la Protezione dei Dati Personali del 25 giugno 2009.

Il trattamento è svolto ad opera di soggetti appositamente autorizzati dal Titolare e in ottemperanza a quanto previsto dall'art. 29 del GDPR. In ogni caso sarà garantita la loro sicurezza logica e fisica e la loro riservatezza.

DESTINATARI DEI DATI

I dati possono essere trattati da:

- **soggetti esterni designati come responsabili esterni del trattamento** ai sensi dell'art. 28 del GDPR, a cui sono impartite adeguate istruzioni operative: Laboratori esterni per talune analisi specialistiche (ad eccezione di quei soggetti che ricevono dati pseudonimizzati) L'elenco completo dei Responsabili del trattamento è disponibile presso il titolare del trattamento Casa di Cura Privata Villa Esther S.r.l;
- **Medico curante** (se comunicato da Lei Interessato).

PERIODO DI CONSERVAZIONE DEI DATI

I Dati Personali saranno conservati solo per il tempo necessario ai fini per cui sono raccolti, rispettando il principio di minimizzazione di cui all'articolo 5, comma 1, lett. c), del GDPR nonché gli obblighi di legge cui è tenuto il Titolare, fatto salvo, in ogni caso, il diritto di revoca del consenso, in ogni momento, da parte dell'Interessato.

In caso di consultazione on-line tramite il sito Web della struttura sanitaria, si rende noto che i Referti saranno disponibili per un tempo limitato, pari a 45 giorni.

DIRITTI RICONOSCIUTI E MODALITÀ DI ESERCIZIO

Gli interessati del trattamento, oltre al diritto di proporre reclamo a un'autorità di controllo, possono esercitare i seguenti diritti:

- **Art. 15 Diritto di accesso** - L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle informazioni riguardanti il trattamento.
- **Art. 16 Diritto di rettifica** - L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.
- **Art. 17 Diritto alla cancellazione (diritto all'oblio)** - L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali.
- **Art. 18 Diritto di limitazione del trattamento** - L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:
  - l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;
  - il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
  - benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
  - l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1 del Regolamento, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.
- **Art. 20 Diritto alla portabilità dei dati** - L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti. Nell'esercitare i propri diritti relativamente alla portabilità dei dati, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.
- **Art. 21 Diritto di opposizione** - L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano;
- **Art. 22 Diritto di non essere sottoposto a processo decisionale automatizzato, compresa la profilazione** - L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

I diritti possono essere esercitati facendo richiesta direttamente al Titolare del trattamento o al Responsabile della protezione dei dati (RPD), contattabili agli indirizzi su riportati. L'interessato può presentare reclamo al GARANTE PER LA PROTEZIONE DEI DATI PERSONALI www.garanteprivacy.it) oppure al EUROPEAN DATA PROTECTION SUPERVISOR (www.edps.europa.eu)

Bojano, lì ____/____/_____

_____

Firma leggibile per presa visione ed accettazione

ALLEGATO 4

PRIVACY POLICY
https://www.villaestherbojano.it/

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI

art.13 REG.UE 2016/679

TITOLARE DEL TRATTAMENTO
Casa di Cura Privata Villa Esther S.r.l.
Via Gino Di Biase n. 18 – 86021 Bojano (CB) Tel. 0874/751001
P.I. 01706190707 - PEC: casadicuravillaesther@pecsicura.it

DATA PROTECTION OFFICER DPO/RESPONSABILE DELLA PROTEZIONE DEI DATI RPD
privacy@villaesther.it

Gent.mo Utente,
di seguito la **Casa di Cura Privata Villa Esther S.r.l.**, in qualità di **Titolare del Trattamento Dati** ed in persona del Legale Rappresentante *pro-tempore*, desidera informaLa sulle modalità di gestione di questo sito. Presti pertanto particolare attenzione all'Informativa che segue, tenendo presente che essa:

a) Risponde specificatamente ai sensi dell'art. 13 del Regolamento U.E. 2016/679 - Codice in materia di protezione dei dati personali - per la protezione dei dati personali, accessibili per via telematica a partire dall'indirizzo: https://www.villaestherbojano.it/. L'informativa è valida solo per il sito ufficiale e non anche per altri siti web eventualmente consultati tramite link.
b) L'informativa si ispira alle codificazioni più attendibili relative ai Requisiti Minimi per la raccolta dei dati personali online (le modalità, i tempi e la natura delle informazioni che i titolari del trattamento devono fornire agli utenti quando questi si collegano a pagine web.

DEFINIZIONI		– per **"dato personale"** (ex 4 numero 1 del Regolamento UE 2016/679), 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; – per **"trattamento"** (ex 4 numero 2 del Regolamento UE 679/2016), si intende qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione. Tale trattamento deve essere improntato ai principi di correttezza, liceità, trasparenza, tutelando la Sua riservatezza e i Suoi diritti.
DATI PERSONALI RACCOLTI	**DATI DI NAVIGAZIONE**	I sistemi informatici e le procedure software preposte al funzionamento di questo sito acquisiscono, nel corso del loro normale esercizio, alcuni dati personali la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di Internet. In questa categoria di dati rientrano gli indirizzi IP o i nomi a dominio dei computer e dei terminali utilizzati dagli utenti, gli indirizzi in notazione URI/URL (*Uniform Resource Identifier/Locator*) delle

		risorse richieste, l'orario della richiesta, il metodo utilizzato nel sottoporre la richiesta al server, la dimensione del file ottenuto in risposta, il codice numerico indicante lo stato della risposta data dal server (buon fine, errore, ecc.) ed altri parametri relativi al sistema operativo e all'ambiente informatico dell'utente.
	DATI COMUNICATI DALL'UTENTE	L'invio facoltativo, esplicito e volontario di messaggi agli indirizzi di contatto. Invio dei dati personali per richiedere una prenotazione (Compilazione *format*).

FINALITÀ	***BASE GIURIDICA***
navigazione sul presente sito web	legittimo interesse art. 6 co. 1 lett.f) G.D.P.R.
richiesta di contatto o richiesta prenotazione	

MODALITÀ DEL TRATTAMENTO	I dati saranno trattati dal Titolare con sistemi elettronici e manuali secondo i principi di correttezza, lealtà e trasparenza previsti dalla normativa applicabile in materia di protezione dei dati personali e tutelando la riservatezza dell'Interessato tramite misure di sicurezza tecniche e organizzative per garantire un livello di sicurezza adeguato.
CONSERVAZIONE DEI DATI	I trattamenti sono svolti in forma automatizzata e manuale, con modalità e strumenti volti a garantire la massima sicurezza e riservatezza, ad opera di soggetti di ciò appositamente incaricati. Nel rispetto di quanto previsto dall'art. 5 comma 1 lett.e) del REG.UE 2016/679 i dati personali raccolti verranno conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali i dati personali sono trattati. La conservazione dei dati di natura personale forniti dipende dalla finalità del trattamento: a) navigazione sul presente sito web (si veda la cookies policy): • per richiesta di contatto (**12 mesi**); • gestione prenotazione (massimo **6 mesi**);
DIRITTI DELL'INTERESSATO	L'Interessato potrà esercitare, in relazione al trattamento dei dati ivi descritti, i diritti previsti dal GDPR (artt. 15-21), ivi inclusi: • ricevere conferma dell'esistenza dei Dati e accedere al loro contenuto (diritti di accesso); • aggiornare, modificare e/o correggere i Dati (diritto di rettifica); • chiederne la cancellazione o la limitazione del trattamento dei Dati trattati in violazione di legge compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i Dati sono stati raccolti o altrimenti trattati (diritto all'oblio e diritto alla limitazione); • proporre reclamo all'Autorità di controllo (Garante per la protezione dei dati personali www.garanteprivacy.it) in caso di violazione della disciplina in materia di protezione dei dati personali; Per esercitare tali diritti l'Interessato può rivolgersi al Titolare oppure al DPO. Nel contattare il Titolare, l'Interessato dovrà accertarsi di includere il proprio nome, email/indirizzo postale e/o numero/i di telefono per essere sicuro che la sua richiesta possa essere gestita correttamente.

ALLEGATO 5

CONSIDERATO CHE

È necessario attuare la migliore qualità conseguibile nel trattamento dei dati personali e ciò è possibile attuando in piena autonomia la gestione dei compiti del proprio ufficio;

Risulta necessario configurare la propria struttura secondo criteri di efficienza e efficacia, delegando compiti operativi a personale che possieda abilità e formazione opportune per svolgere le mansioni a esso delegato;

A seguito di apposita attività conoscitiva e valutativa è risultato che ..... **codice fiscale** ..... offre garanzie sufficienti circa le proprie qualità professionali e personali, in particolare esperienza, capacità e affidabilità nella conoscenza della base normativa (Regolamento UE 2016/679) e delle prassi in materia di protezione dei dati personali, nonché della capacità di assolvere i compiti con scrupolosità e diligenza

NOMINA

..... **codice fiscale** ....., quale **Persona Autorizzata** (art. 4 Regolamento UE 2016/679) per i trattamenti riportati di seguito insieme alle caratteristiche peculiari quali la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali, le categorie di interessati e i permessi accordati:

- Data Inizio:
- Data Fine:
- Finalità:
- Categoria Dati:
- Interessati:

La persona autorizzata si impegna a: ...

- garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli e a non divulgare, neanche dopo la cessazione dell'incarico di Persona Autorizzata, alcuna delle informazioni di cui è venuto a conoscenza nell'adempimento dei compiti assegnatigli, sia perché connesso con tali attività che per caso fortuito (art. 28 par. 3 lettera b Regolamento UE 2016/679);

- ove applicabile, rispettare l'obbligo di riservatezza in ottemperanza alle norme deontologiche caratteristiche della professione esercitata secondo le norme vigenti (art. 28 par. 3 lettera b Regolamento UE 2016/679)

Istruzioni specifiche ricevute:

BOIANO, 06/12/2021

ALLEGATO 6

CONSIDERATO CHE

A seguito di apposita attività conoscitiva e valutativa è risultato che **Azienda Sanitaria Regionale Molise partita iva 01546900703 - codice fiscale 01546900703** offre garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti imposti dal Regolamento UE 2016/679 e garantisca la tutela dei diritti dell'interessato (art. 28 par. 1 Regolamento UE 2016/679), con il presente atto

NOMINA

Azienda Sanitaria Regionale Molise partita iva 01546900703 - codice fiscale 01546900703, quale **Responsabile del Trattamento** per i trattamenti riportati di seguito insieme alle caratteristiche peculiari quali la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati:

SDO e impegnative

- Data Inizio: 25/05/2018
- Data Fine: Criterio determinazione periodo
- Finalità: Registrazione pazienti e gestione amministrativa
- Categoria Dati: Stato di salute
- Interessati: Pazienti

Il Responsabile del Trattamento si impegna (art. 28 par. 3 Regolamento UE 2016/679) a:

- trattare i dati personali soltanto su istruzione documentata del Titolare del Trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in questa circostanza il Responsabile del Trattamento informa il Titolare del Trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

- garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza);

- adottare tutte le misure richieste per la sicurezza del trattamento (art. 32 Regolamento UE 2016/679);

- rispettare le condizioni per ricorrere a un altro responsabile del trattamento (art. 28 par. 2 e par. 4 Regolamento UE 2016/679);

- assistere il titolare del trattamento con misure tecniche e organizzative adeguate, tenendo conto della natura del trattamento e nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;

- assistere il titolare del trattamento nel garantire il rispetto degli obblighi relativi alla sicurezza dei dati personali (artt. 32, 33, 34 Regolamento UE 2016/679) e alla valutazione di impatto sulla protezione dei dati e consultazione preventiva (artt. 35, 36 Regolamento UE 2016/679), tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

- su scelta del titolare del trattamento, cancellare o restituire tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;

- mettere a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi discendenti dalla normativa (art. 28 Regolamento UE 2016/679), consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

Istruzioni ricevute per responsabile:

Istruzioni ricevute per rappresentante del responsaible:

BOIANO, 01/02/2022

ALLEGATO 7

VILLA ESTHER
casa di cura

INFORMATIVA DIPENDENTI

Trattamento dei dati ai sensi del regolamento UE 2016/679

1. PERCHÉ FORNIAMO QUESTE INFORMAZIONI

Ai sensi del Regolamento UE 2016/679 (di seguito Regolamento o GDPR), con il presente documento vogliamo illustrare le modalità adottate da **Casa di Cura Privata Villa Esther S.r.l.** per il trattamento dei Suoi dati personali.

2. PRINCIPI APPLICABILI ALLE ATTIVITÀ DI TRATTAMENTO

Il trattamento dei Suoi dati personali avviene nel rispetto dei principi fissati all'articolo 5 del Regolamento UE 2016/679, che qui si ricordano brevemente:

- liceità, correttezza e trasparenza del trattamento, nei confronti dell'interessato;
- limitazione della finalità del trattamento, compreso l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati;
- minimizzazione dei dati: ossia, i dati devono essere adeguati pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento;
- esattezza e aggiornamento dei dati, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;
- limitazione della conservazione: ossia, è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
- integrità e riservatezza: occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento.

3. TITOLARE DEL TRATTAMENTO

Il Titolare del trattamento è **Casa di Cura Privata Villa Esther S.r.l.** raggiungibile ai seguenti indirizzi:
Casa di Cura Privata Villa Esther S.r.l., via Gino Di Biase n. 18 – 86021 Bojano (CB) Tel. 0874/751001 - privacy@villaestherbojano.it

4. DATA PROTECTION OFFICER DPO/RESPONSABILE DELLA PROTEZIONE DEI DATI RPD

Casa di Cura Privata Villa Esther S.r.l. ha provveduto a nominare il Responsabile della protezione dei dati, che è raggiungibile ai seguenti indirizzi: Casa di Cura Privata Villa Esther S.r.l., via Gino Di Biase n. 18 – 86021 Bojano (CB) Tel. 0874/751001 - privacy@villaestherbojano.it.

5. LE FINALITÀ E LA BASE GIURIDICA DEL TRATTAMENTO.

I dati personali acquisiti, ai sensi del regolamento UE 2016/679, sono trattati per le seguenti finalità:

- costituzione e gestione del rapporto di lavoro,
- gestione dei dati fiscali, previdenziali ed assicurativi,
- gestione delle cause di sospensione del contratto (maternità, infortunio, malattia, ecc.),
- adempimenti in materia di sicurezza del lavoro ed a quant'altro stabilito da leggi, contratti e regolamenti aziendali.

La base giuridica che giustifica il trattamento è il Suo Contratto di lavoro.

6. DESTINATARI DEI DATI

I dati possono essere trattati da:

- soggetti esterni operanti in qualità di titolari quali, a titolo esemplificativo, autorità ed organi di vigilanza e controllo ed in generale soggetti, pubblici o privati, legittimati a richiedere i dati (es. ASREM);
- soggetti esterni designati come responsabili del trattamento ai sensi dell'art. 28 del GDPR, a cui sono impartite adeguate istruzioni operative; es. società assicurative, consulenti del lavoro, consulenti fiscali, consulenti legali, sindacati e patronati. Inoltre aziende fornitrici dei seguenti servizi: applicativi ed applicazioni web e software gestionali, software e applicativi per contabilità ed amministrazione, formazione del personale, medicina del lavoro, consulenza e audit sui sistemi di gestione.

L'elenco completo dei Responsabili del trattamento è disponibile presso il titolare del trattamento.

7. PERIODO DI CONSERVAZIONE DEI DATI

I dati forniti verranno conservati per il tempo necessario per adempiere alle finalità citate, e per un periodo successivo fino a 10 anni per adempiere agli obblighi di conservazione previsti dalle normative civilistiche, fiscali e tributarie.

8. TRASFERIMENTO DEI DATI PERSONALI A PAESE TERZO O AD UNA ORGANIZZAZIONE INTERNAZIONALE

I dati personali non sono trasferiti in paesi terzi o ad organizzazioni internazionali.

9. ATTIVITA' DI PROFILAZIONE

I dati personali acquisiti non sono oggetto di processi decisionali automatizzati, inclusa la "profilazione" che consiste in una forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato, ove ciò produca effetti giuridici che la riguardano o incida in modo analogo significativamente sulla sua persona

10. DIRITTI RICONOSCIUTI E MODALITÀ DI ESERCIZIO

Gli interessati del trattamento, oltre al diritto di proporre reclamo a un'autorità di controllo, possono esercitare i seguenti diritti:

Art. 15 Diritto di accesso - L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle informazioni riguardanti il trattamento.

Art. 16 Diritto di rettifica - L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Art. 17 Diritto alla cancellazione (diritto all'oblio) - L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali.

Art. 18 Diritto di limitazione del trattamento - L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi:

a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;

b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;

c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;

d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1 del regolamento, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

Art. 20 Diritto alla portabilità dei dati - L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti.

Nell'esercitare i propri diritti relativamente alla portabilità dei dati, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.

Art. 21 Diritto di opposizione - L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano compresa la profilazione sulla base di tali disposizioni.

Art. 22 Diritto di non essere sottoposto a processo decisionale automatizzato, compresa la profilazione - L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

I diritti possono essere esercitati facendo richiesta direttamente al Titolare del trattamento o al Responsabile della protezione dei dati (RPD), contattabili agli indirizzi riportati p.to 3 e 4. L'interessato può presentare reclamo al GARANTE PER LA PROTEZIONE DEI DATI PERSONALI (www.garanteprivacy.it) oppure al EUROPEAN DATA PROTECTION SUPERVISOR (www.edps.europa.eu).

11. OBBLIGHI LEGALI/CONTRATTUALI O DI REQUISITI NECESSARI PER LA CONCLUSIONE DI UN CONTRATTO

Il conferimento dei dati per le finalità di cui al p.to 5 è obbligatorio. In loro assenza, non si potrà adempiere correttamente ed efficacemente a tutti gli adempimenti contrattuali e di legge previsti.

DICHIARAZIONE DI RICEVUTA DELL'INFORMATIVA E CONSENSO AL TRATTAMENTO DI PARTICOLARI CATEGORIE DI DATI PERSONALI

Io sottoscritto/a _____ dichiaro di avere ricevuto le informazioni di cui all'art. 13 del REG. UE 2016/679.

Bojano (CB), lì ___/___/_____

firma leggibile per accettazione

_____

VILLA ESTHER
casa di cura

INFORMATIVA

Gent.mi,

al fine di limitare il diffondersi del COVID-19 ("Corona Virus") e per tutelare il personale interno ed i pazienti, l'accesso è condizionato da un *Pre-Triage* teso a verificare la presenza di particolari sintomi riconducibili al Virus.

I dati raccolti dal nostro personale sono archiviati solo in forma cartacea e resi inaccessibili, ad esclusione di una specifica richiesta da parte di Autorità Pubbliche preposte. Terminata l'emergenza tutti i dati saranno eliminati.

La mancata raccolta comporterà un divieto di accesso alla Struttura.

Grazie per la collaborazione

Bojano (CB) 09 marzo 2020

Allegato 9

INTEGRAZIONE

VILLA ESTHER
casa di cura

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI
PER DIPENDENTI E COLLABORATORI

Validità delle disposizioni: a partire dalla presente data fino a nuove disposizioni

Ai sensi dell'art.13 del REG.UE 2016/679 (*cd.* GDPR) e secondo le disposizioni del DPCM 11 marzo 2020 e del Protocollo del 14 marzo 2020, si forniscono di seguito le informazioni in merito al trattamento dei dati personali dei soggetti che, durante l'emergenza COVID-19, accedono ai locali e agli uffici del Titolare o ad altri luoghi a quest'ultimo riferibili.

TITOLARE: Casa di Cura Privata Villa Esther S.r.l. - via Gino Di Biase n. 18 – 86021 Bojano (CB) - privacy@villaesther.it	
TIPOLOGIA DI DATI PERSONALI TRATTATI E DI INTERESSATI	Nei limiti delle finalità e delle modalità definite nella presente informativa, sono oggetto di trattamento: a) i dati attinenti all'attestazione di una temperatura corporea non superiore a 37,5; b) dichiarazioni attinenti tutte le misure della quarantena o dell'isolamento fiduciario con sorveglianza sanitaria. I dati personali oggetto di trattamenti si riferiscono: • al personale dipendente ed assimilati ad integrazione dell'informativa già fornita per il trattamento dei dati personali funzionale all'instaurazione e all'esecuzione del rapporto di lavoro; • ai collaboratori, ai fornitori, trasportatori, appaltatori, consulenti, visitatori e altri soggetti terzi autorizzati ad accedere ai locali, agli uffici o altri luoghi riferibili al Titolare.
FINALITÀ E BASE GIURIDICA DEL TRATTAMENTO	I dati personali saranno trattati esclusivamente per finalità di prevenzione dal contagio da COVID-19, in esecuzione del Protocollo di sicurezza anti-contagio adottato ai sensi dell'art. 1, n. 7, lett. d) del DPCM 11 marzo 2020 e del Protocollo del 14 marzo 2020. condiviso Governo/Parti sociali
NATURA DEL CONFERIMENTO DEI DATI PERSONALI	Il conferimento dei dati è necessario per accedere ai locali e agli uffici del Titolare o ad altri luoghi comunque a quest'ultimo riferibili. **Un eventuale rifiuto a conferirli impedisce di consentire l'ingresso.**
MODALITÀ, AMBITO E DURATA DEL TRATTAMENTO **DESTINATARI**	Il trattamento è effettuato da personale che agisce sulla base di specifiche istruzioni fornite in ordine alle finalità e alle modalità del trattamento. I dati personali non saranno oggetto di diffusione, né di comunicazione a terzi, se non in ragione delle specifiche previsioni normative (comunicazione all'Autorità sanitaria ed all' INAIL e condivisione di informazioni per la ricostruzione della filiera degli eventuali contatti stretti di un lavoratore risultato positivo al COVID-19). I dati saranno trattati per il tempo strettamente necessario a perseguire la citata finalità di prevenzione dal contagio da COVID-19 e conservati non oltre il termine dello stato d'emergenza, attualmente fissato al 31 luglio 2020 della Delibera del Consiglio dei Ministri 31 gennaio 2020.
DIRITTI DEGLI INTERESSATI	In qualsiasi momento, gli interessati hanno il diritto di accedere ai propri dati personali, di chiederne la rettifica, l'aggiornamento e la relativa cancellazione. È, altresì, possibile opporsi al trattamento e richiederne la limitazione. Queste richieste potranno essere rivolte direttamente al Titolare del trattamento, ai recapiti indicati in premessa. Inoltre, nel caso in cui si ritenga che il trattamento sia stato svolto in violazione della normativa sulla protezione dei dati personali, è riconosciuto il diritto di presentare reclamo all'Autorità Garante per la protezione dei dati personali, Piazza Venezia, 11 - 00187 – Roma oppure tramite il sito ufficiale www.garanteprivacy.it.

Bojano (CB) lì 08/05/2020

_____

VILLA ESTHER
casa di cura

SCHEDA PERSONALE MISURAZIONE TEMPERATURA CORPOREA

GIUGNO 2020

COGNOME E NOME DEL LAVORATORE:	

DATA	Ora Ingresso	Ora uscita	Firma del Lavoratore
1 giugno 2020	:	:	
2 giugno 2020	:	:	
3 giugno 2020	:	:	
4 giugno 2020	:	:	
5 giugno 2020	:	:	
6 giugno 2020	:	:	
7 giugno 2020	:	:	
8 giugno 2020	:	:	
9 giugno 2020	:	:	
10 giugno 2020	:	:	
11 giugno 2020	:	:	
12 giugno 2020	:	:	
13 giugno 2020	:	:	
14 giugno 2020	:	:	
15 giugno 2020	:	:	
16 giugno 2020	:	:	
17 giugno 2020	:	:	
18 giugno 2020	:	:	
19 giugno 2020	:	:	
20 giugno 2020	:	:	
21 giugno 2020	:	:	
22 giugno 2020	:	:	
23 giugno 2020	:	:	
24 giugno 2020	:	:	
25 giugno 2020	:	:	
26 giugno 2020	:	:	
27 giugno 2020	:	:	
28 giugno 2020	:	:	
29 giugno 2020	:	:	
30 giugno 2020	:	:	

Il Lavoratore dichiara giornalmente sotto la propria responsabilità di aver ricevuto i dispositivi di protezione Individuali e di non aver avuto "contatti stretti" con alcun soggetto positivo al Covid-19. Informativa privacy esposta ed allegata.

VILLA ESTHER
casa di cura

INFORMATIVA
PER LA MISURAZIONE DEI PARAMETRI CORPOREI

Art. 13 REG.UE 2016/679

Giugno 2020

Gent.li interessati,

a causa dell'emergenza sanitaria in corso, siamo obbligati a rispettare alcune precauzioni volte alla tutela della salute per l'accesso ai luoghi di lavoro. Chiediamo quindi la collaborazione di tutti (pazienti, dipendenti, collaboratori, visitatori) per il rispetto del *"protocollo di regolamentazione delle misure per il contrasto e il contenimento della diffusione del virus Covid-19 negli ambienti di lavoro "*condiviso tra Governo e Parti sociali.

Queste misure approvate anche dal Garante Privacy, impongono il trattamento di dati personali, e talvolta di dati particolari. Tali dati verranno trattati unicamente nelle modalità e per le finalità di seguito esposte:

TITOLARE DEL TRATTAMENTO

Casa di Cura Privata Villa Esther S.r.l.

Casa di Cura Privata Villa Esther S.r.l., via Gino Di Biase n. 18 – 86021 Bojano (CB) Tel. 0874/751001 - privacy@villaesther.it

DATA PROTECTION OFFICER DPO/RESPONSABILE DELLA PROTEZIONE DEI DATI RPD

Casa di Cura Privata Villa Esther S.r.l. ha provveduto a nominare il Responsabile della Protezione dei Dati, che è raggiungibile ai seguenti indirizzi:
Casa di Cura Privata Villa Esther S.r.l., via Gino Di Biase n. 18 – 86021 Bojano (CB) Tel. 0874/751001 - privacy@villaesther.it

TIPOLOGIA DI DATI TRATTATI

Con riferimento al trattamento oggetto della presente informativa, il personale autorizzato procederà alla misurazione della temperatura e tratterà i seguenti dati personali anche particolari (c.d. sensibili): - nome, cognome, stato di salute con specifiche patologie e misurazione della temperatura corporea (c.d. febbre). Si precisa che soltanto il dato rilevato mediante Termo-Scanner non verrà tracciato ad eccezione di particolari condizioni quali il superamento della soglia di 37,5°.

Finalità Del Trattamento	*Base Giuridica*	*Periodo Conservazione Dati*	*Natura Del Conferimento*
Prevenzione contagio COVID-19 ed eventuale attivazione protocollo di sicurezza sanitaria. Il Titolare precisa che nel caso in cui la temperatura corporea dovesse essere pari o superiore a 37,5° l'interessato non potrà accedere in struttura. A fronte di tale situazione l'interessato verrà invitato a leggere le istruzioni di cui al Ministero della Salute previste per COVID-19 e a rispettare scrupolosamente quanto gli verrà indicato dal nostro personale.	Principi generali per la tutela e la salute nei luoghi di lavoro: Art. 6 par. 1 lett. c) GDPR obbligo di legge (art. 2087 c.c. e d.lgs. 81/08 tutela salute e sicurezza nei luoghi di lavoro; DPCM 11/03/2020 art 1 n. 7 lett d) salvaguardia dell'interesse vitale degli operatori che collaborano con il Titolare e di altre persone fisiche quali i visitatori - Art. 9 par. 2 lett. b) – assolvere obblighi ed esercitare diritti specifici del titolare o dell'interessato in materia di diritto del lavoro e della protezione sociale e sicurezza sociale.	I dati saranno trattati per il tempo strettamente necessario a perseguire la citata finalità di prevenzione dal contagio da COVID-19 ovvero per tutto il periodo dello stato d'emergenza, attualmente fissato al 31 luglio 2020 dalla Delibera del Consiglio dei Ministri 31 gennaio 2020.	Il conferimento dei dati è obbligatorio. Il rifiuto comporterà l'impossibilità di accedere nella struttura.

DESTINATARI/CATEGORIE DI DESTINATARI DEI DATI

Qualora si renda necessario i dati trattati saranno comunicati a soggetti indicati dalla legge quali ad esempio: ufficio che si occupa della gestione del personale; addetto alla sicurezza sui luoghi di lavoro, A.S.R.E.M., Protezione Civile, Inail, medico del lavoro e altri soggetti previsti dalla legge.

TRASFERIMENTO DATI VERSO UN PAESE EXTRA UE

I dati personali non saranno trasferiti in paesi fuori dall'Unione Europea.

DIRITTI DEGLI INTERESSATI

Lei potrà far valere i propri diritti come espressi dagli artt. 15 e ss. del Regolamento UE 2016/679, rivolgendosi direttamente al Titolare ai contatti sopra riportati. In particolare, Lei ha il diritto, in qualunque momento di ottenere, da parte del Titolare, l'accesso ai Suoi dati personali e richiedere le informazioni relative al trattamento nonché limitare il loro trattamento. Nel caso in cui ritenga che il trattamento dei dati personali effettuato dal titolare avvenga in violazione di quanto previsto dal Regolamento (UE) 2016/679, lei ha il diritto di proporre reclamo alla Autorità di controllo – Garante Italiano (https://www.garanteprivacy.it/).

Si ringrazia per la gentile collaborazione

Allegato 11

VILLA ESTHER
casa di cura

NOTA INFORMATIVA
PER DIPENDENTI E COLLABORATORI

Validità delle disposizioni: a partire dalla presente data fino a nuove disposizioni

Gent.mi,

in questi giorni si stanno susseguendo una serie di disposizioni delle Autorità competenti che individuano misure per il contrasto e il contenimento del virus Covid-19 (Coronavirus).

Siete, quindi, TUTTI impegnati a riflettere sulla possibilità che **negli ultimi 14 giorni abbiate manifestato sintomi da contagio, abbiate effettuato soggiorni in zone a rischio epidemiologico o siate stati in contatto stretto con persone con sospetto o conferma di contagio da Covid-19.**

Tali precauzioni sono ancora più rilevanti per la nostra Azienda, in quanto siete chiamati ad adottare le più adeguate misure per la tutela degli ospiti/pazienti e collaboratori della nostra struttura.

Le recenti disposizioni (*protocollo di regolamentazione delle misure per il contrasto e il contenimento della diffusione del virus Covid-19 negli ambienti di lavoro*), approvate anche dal Garante Privacy, impongono al **lavoratore di informare tempestivamente e responsabilmente il datore di lavoro della presenza di qualsiasi sintomo influenzale durante l'espletamento della prestazione lavorativa, avendo cura di rimanere ad adeguata distanza dalle persone presenti.**

Inoltre, tutto il personale (collaboratori, fornitori e gli addetti alle pulizie, ecc.) prima di accedere al luogo di lavoro, potrà essere sottoposto al controllo della temperatura corporea. Se tale temperatura risulterà superiore ai 37,5°, non sarà consentito l'accesso alla struttura.

Vi invitiamo pertanto caldamente a riflettere su quanto esposto sopra e a:

- comunicare al datore di lavoro/direttore sanitario eventuali stati di rischio in base alle disposizioni vigenti, provvedendo contestualmente ad informare gli organi preposti;
- seguire scrupolosamente le indicazioni diffuse dagli Enti competenti e dall'Azienda circa le misure e le raccomandazioni nel contesto dell'emergenza Covid-19 (Coronavirus).

Bojano, 18 marzo 2020

Distinti saluti.

Ad integrazione dell'informativa già resa in precedenza ai sensi dell'art. 13 GDPR, si comunica che: Gli eventuali dati personali raccolti verranno trattati dal Titolare del trattamento per l'accesso alla struttura, in modo da preservare la salute di pazienti, ospiti e operatori circa la diffusione del virus sars-Cov-19 (=Coronavirus). La base giuridica del trattamento è la sussistenza di motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero sulla base del diritto interno, in relazione al DPCM 1 e 8 marzo 2020 (riferito all'art. 9, par. 2, lettera "i" del Regolamento Europeo 679/2016). I dati raccolti non saranno condivisi con terze parti, se non in assolvimento di eventuali obblighi di legge, saranno detenuti all'unico scopo indicato più sopra e per i tempi di gestione dell'emergenza indicati dalle leggi e regolamenti vigenti. A tal fine I dati saranno trattati esclusivamente dal Titolare del trattamento, dagli eventuali responsabili del trattamento appositamente incaricati, nonché dal relativo personale appositamente istruito al trattamento e alla protezione dei dati. Le richieste per l'esercizio dei diritti personali, come da informativa che potrà ricevere e/o richiedere, potranno essere inviate al Titolare o al DPO.

Allegato 12

VILLA ESTHER

NOMINA (EXTRA)
SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI
(ARTT.4 E 29 REG.UE 2016/679 - ART.2 QUATERDECIES D.LGS 101/2018)

REV_01_2021

La **Casa di Cura Privata Villa Esther S.r.l.** ai sensi del Regolamento UE 2016/679 in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali, in qualità **di Titolare del Trattamento** ed in persona del Rappresentante Legale *pro-tempore*,

NOMINA

_____

(nome, cognome, codice fiscale)

quale Persona Autorizzata (artt.4 e 29 Regolamento UE 2016/679 art.2 *quaterdecies* D.lgs 101/2018) per i trattamenti riportati di seguito insieme alle caratteristiche peculiari quali la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali, le categorie di interessati e i permessi accordati:

TRATTAMENTO	**GESTIONE DEL RISCHIO COVID-19 – VERIFICA GREEN PASS**
TIPOLOGIA DI TRATTAMENTO	Verifica del "*GreenPass*" mediante App ufficiale "VerficaC19" attraverso lettura ottica del Qr-Code, nonché gestione di nominativi dipendenti esenti da controllo perché in possesso di certificato di esenzione.
BASE GIURIDICA	Art 6 lett. c) Reg Ue 679/2016 e DL N.127 del 21/09/2021
FINALITÀ	Verifica del "*GreenPass*" o del "Certificato Verde Covid-19" cartaceo per gestire gli accessi alla struttura.
NATURA	Dati identificativi; dato particolare crittografato e validità del certificato Verde.
CATEGORIE DI INTERESSATI	Dipendenti/collaboratori ed assimilati
ASSET	Smartphone con installata App: "Verifica C19"

La persona autorizzata si impegna a:

- **garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli e a non divulgare, neanche dopo la cessazione dell'incarico alcuna delle informazioni di cui è venuta a conoscenza nell'adempimento dei compiti assegnatigli, nè per negligenza né per imprudenza;**
- Impedire alle persone sfornite di Green pass l'accesso ai locali aziendali e ad avvisare il Titolare o l'ufficio risorse umane indicando il nominativo del lavoratore respinto.
- **SVOLGERE CORRETTAMENTE LA MANSIONE DI CONTROLLO ASSEGNATA;**
- **IN CASO DI INESATTO O MANCATO CONTROLLO SARÀ SOGGETTO A SANZIONE DISCIPLINARE DA PARTE DEL TITOLARE;**
- non lasciare incustoditi e accessibili gli *Asset* forniti dal Titolare durante una sessione di trattamento;
- non effettuare copie di Dati Personali su Device Mobili;
- fornire al Titolare, a semplice richiesta e secondo le modalità indicate da questo, tutte le informazioni relative all'attività svolta, al fine di consentire lo svolgimento efficace della propria attività di controllo.

Con la firma in calce si prende atto e si accetta quanto previsto nella presente assegnazione ed in ottemperanza con REG.UE 2016/679 e del D.lgs 101/2018 per i trattamenti sopra riportati insieme alle loro caratteristiche peculiari

Bojano (CB), lì ____/_____/_____

Persona Autorizzata

_____

(firma leggibile)

Timbro/firma del ***Titolare del Trattamento***

_____

Allegato 13

VILLA ESTHER

NOMINA (EXTRA)
SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI
(ARTT.4 E 29 REG.UE 2016/679 - ART.2 QUATERDECIES D.LGS 101/2018)

REV_01_2021

La **Casa di Cura Privata Villa Esther S.r.l.** ai sensi del Regolamento UE 2016/679 in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali, in qualità **di Titolare del Trattamento** ed in persona del Rappresentante Legale *pro-tempore*,

NOMINA

_____

(nome, cognome, codice fiscale)

quale Persona Autorizzata (artt.4 e 29 Regolamento UE 2016/679 art.2 *quaterdecies* D.lgs 101/2018) per i trattamenti riportati di seguito insieme alle caratteristiche peculiari quali la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali, le categorie di interessati e i permessi accordati:

TRATTAMENTO	**GESTIONE DEL RISCHIO COVID-19 – APPLICAZIONE SANZIONE GREEN PASS NON VALIDO**
TIPOLOGIA DI TRATTAMENTO	Compilazione modulistica ufficiale comprovante il mancato possesso di valido Green Pass
E BASE GIURIDICA	Art 6 lett. c) REG.Ue 679/2016 e DL N.127 del 21/09/2021
FINALITÀ	Applicazione delle disposizioni DL N.127 del 21/09/2021
NATURA	Dati identificativi, orario, luogo, evidenza della mancanza di green pass nel senso di mancata esibizione o green pass negativo, eventuali motivazioni evidenziate dal lavoratore.
DESTINATARI	Consulente del Lavoro/personale preposto all'elaborazione Buste Paga, Prefetto e/o altre Autorità competenti
CATEGORIE DI INTERESSATI	Personale dipendente, collaboratori ed assimilati
ASSET	Modulistica ufficiale - notifica

La persona autorizzata si impegna a:

- **garantire la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli e a non divulgare, neanche dopo la cessazione dell'incarico alcuna delle informazioni di cui è venuta a conoscenza nell'adempimento dei compiti assegnatigli, nè per negligenza né per imprudenza;**
- Impedire alle persone sfornite di Green pass l'accesso ai locali aziendali e ad avvisare il Titolare o l'ufficio risorse umane indicando il nominativo del lavoratore respinto.
- **SVOLGERE CORRETTAMENTE LA MANSIONE DI CONTROLLO ASSEGNATA;**
- **IN CASO DI INESATTO O MANCATO CONTROLLO SARÀ SOGGETTO A SANZIONE DISCIPLINARE DA PARTE DEL TITOLARE;**
- non lasciare incustoditi e accessibili gli *Asset* forniti dal Titolare durante una sessione di trattamento;
- non effettuare copie di Dati Personali su Device Mobili;
- fornire al Titolare, a semplice richiesta e secondo le modalità indicate da questo, tutte le informazioni relative all'attività svolta, al fine di consentire lo svolgimento efficace della propria attività di controllo.

Con la firma in calce si prende atto e si accetta quanto previsto nella presente assegnazione ed in ottemperanza con REG.UE 2016/679 e del D.lgs 101/2018 per i trattamenti sopra riportati insieme alle loro caratteristiche peculiari

Bojano (CB), lì ____/_____/_____

Persona Autorizzata

_____

(firma leggibile)

Timbro/firma del ***Titolare del Trattamento***

_____

PROCEDURA PER L'ORGANIZZAZIONE DELLE VERIFICHE DEL POSSESSO DEL GREEN PASS PER ACCEDERE AI LUOGHI DI LAVORO

Approvazione:	Nome	Firma
DATORE DI LAVORO	MARCO DI BIASE	

INDICE

1. SCOPO

La presente procedura ha lo scopo di definire le modalità di controllo del possesso della Certificazione Verde (Green Pass) per l'accesso ai luoghi di lavoro a far data dal 15 ottobre 2021 e fino alla cessazione dello stato di emergenza, oggi prevista per il 31 dicembre 2021.

2. CAMPO DI APPLICAZIONE

La presente procedura è predisposta in applicazioni delle disposizioni contenute nel Decreto Legge 21 settembre 2021 art.3, relative alla verifica del possesso della Certificazione Verde COVID-19 (Green Pass) per l'accesso al luogo di lavoro, e indica le modalità operative che gli incaricati al controllo dovranno applicare per verificare il possesso della Certificazione Verde (Green Pass) necessaria per l'accesso al luogo di lavoro.

3. DEFINIZIONI

Certificazione Verde: certificazione digitale e stampabile (cartacea), che contiene un codice a barre bidimensionale (QR Code) e un sigillo elettronico qualificato. In Italia, viene emessa soltanto attraverso la piattaforma nazionale del Ministero della Salute. Le modalità di ottenimento della Certificazione Verde sono indicate nel D.L. 52/2021 (ovvero: ottenuta tramite tampone negativo, certificato di avvenuta guarigione o vaccino).

Green Pass: Certificazione Verde

Incaricato al Controllo: Persona incaricata dal datore di lavoro per la verifica del possesso della Certificazione Verde Covid-19.

Interessato: Lavoratore dipendente o altra persona che deve accedere, alla Struttura, a qualsiasi titolo, per ragioni di lavoro, formazione o volontariato.

Procedura: Modo specifico per svolgere un'attività o un processo.

VerificaC19: Applicazione avente scopo di verificare codice a barre bidimensionale (QR Code) per la verifica del possesso della Certificazione Verde.

APP: Applicazione installabile su dispositivo elettronico portatile o fisso

4. RESPONSABILITÀ

Datore di Lavoro: è il responsabile della designazione del/gli Incaricato/i al Controllo e della predisposizione e attuazione della presente procedura.

Incaricato al Controllo: Responsabile delle attività di controllo previste dalla presente procedura.

Addetto all'accertamento delle violazioni: è il responsabile dell'attivazione delle procedure amministrative di accertamento delle violazioni amministrative previste dalla normativa di riferimento.

5. MODALITÀ DI DESIGNAZIONE

L'incaricato al controllo della certificazione verde è designato dal datore di lavoro attraverso lettera di incarico e dopo aver ricevuto istruzioni specifiche sulle modalità del controllo.

Ai fine dell'attivazione delle procedure relative all'accertamento e alla irrogazione delle sanzioni amministrative previste dall'art. 3 del DL 127/2021 comma 4 in relazione al comma 9, viene nominato nella qualità di responsabile l'Amministratore Unico Signor. Marco Di Biase.

6. MODALITÀ DI SVOLGIMENTO DEL CONTROLLO DA PARTE DEGLI INCARICATI

Lo svolgimento dell'attività di controllo dovrà essere effettuato tramite applicazione software ufficiale che garantisce non siano acquisite, in nessun modo, informazioni personali diverse e ulteriori rispetto rispetto a quelle relative al certificato verde, memorizzate sul dispositivo.

Nello specifico l'applicazione è denominata "Verifica-C19".

La modalità di utilizzo è la seguente:

a) Si procederà ad eseguire un controllo a campione all'ingresso in Struttura, così come previsto dalla norma. La scelta si è resa necessaria poiché il controllo sistematico porterebbe inevitabilmente a creare disservizi nell'ordinato accesso dei lavoratori nonché assembramenti.

I soggetti addetti procederanno al controllo di almeno un interessato ogni 5 (cinque) che chiederanno di accedere alla Struttura, assicurando, complessivamente, nel corso dei vari giorni di controllo, che tutto il personale richiedente l'accesso venga sottoposto al controllo previsto.

Un'altra attività di controllo a campione sarà effettuata all'interno dei locali della Struttura. In questo caso, il campione sarà composto da almeno 6 (sei) soggetti interessati nell'arco della giornata.

b) L'incaricato richiede all'interessato il QR Code (digitale o cartaceo) del proprio certificato verde (Green Pass).
c) L'incaricato procede alla verifica attraverso l'APP "VerificaC-19" legge il QR Code.
d) L'APP mostrerà, unicamente , all'Incaricato al controllo, le seguenti informazioni:
    a. Validità della certificazione verde (Green Pass)
    b. Nome cognome e data di nascita dell'intestatario.
e) L'incaricato potrà richiedere che l'interessato dimostri adeguatamente la corrispondenza delle proprie generalità con quelle presenti su Green Pass.

f) L'incaricato consentirà l'accesso ai luoghi di lavoro al lavoratore che, sprovvisto di Certificazione Verde (Green Pass), abbia presentato, precedentemente alla data del 15 ottobre 2021, al medico del Lavoro del Titolare, una di certificazione medica di esonero dalla campagna vaccinale per COVID19 conforme alle indicazioni del Ministero della Salute per gli esonerati dalla vaccinazione. (art.1 – comma 3 e art. 3 – comma 3 del Decreto Legge 21 settembre 2021, n. 127).

L'Azienda comunicherà verbalmente, a tutti gli addetti incaricati al controllo, l'elenco dei "lavoratori esonerati", i quali saranno tenuti al massimo riserbo nel pieno rispetto della "privacy".

g) L'incaricato non consente l'accesso all'interessato qualora l'applicazione dia esito negativo per la verifica della validità del certificato verde presentato o qualora l'interessato non esibisca il certificato verde (Green Pass).

h) L'incaricato non consente l'accesso all'interessato che, qualora richiesto, non dimostri la corrispondenza delle proprie genera generalità con quelle indicate sul certificato verde esibito.

i) L'incaricato al controllo comunica al proprio datore di lavoro l'eventuale esito negativo della verifica della certificazione verde.

j) L'incaricato al controllo redige verbale di accertamento di eventuali violazioni della normativa di riferimento indicando in maniera dettagliata le circostanze accertate e consegnando detto verbale, senza ritardo, al responsabile della procedura amministrativa sanzionatoria.

k) L'incaricato non deve effettuare:
   a. Fotografie
   b. Copie cartaceo o digitali di documenti di identità o certificazioni Verdi (Green Pass)

l) L'incaricato al controllo non conserva alcuna informazione relativamente alle attività di verifica delle certificazioni Verdi.

m) L'incaricato al controllo, non può cedere l'incarico se non autorizzato dal datore di lavoro.

n) L'incaricato avverte il datore di lavoro qualora riscontri situazioni non previste dalla presente procedura.

Il datore di lavoro, anche in deroga totale e/o parziale alla presente procedura, si riserva di applicare le disposizioni di all'art. 3 del DL 8.10.2021 n139 introduttivo dell'art. 9-octeis del D.L. 22 aprile 2021 n. 52 convertito, con modificazioni, dalla Legge 17 giugno 2021 n. 87.

7. STRUMENTI DI VERIFICA

Il datore di lavoro mette a disposizione degli incaricati al controllo i dispositivi necessari per lo svolgimento dell'incarico assegnato. L'incaricato non utilizza dispositivi privati per lo svolgimento dell'attività indicata nella presente procedura.

VILLA ESTHER
casa di cura

Allegato 15

INFORMATIVA
PER LA MISURAZIONE DEI PARAMETRI CORPOREI

Art. 13 REG.UE 2016/679

04 maggio 2020

Gent.li interessati,

a causa dell'emergenza sanitaria in corso, siamo obbligati a rispettare alcune precauzioni volte alla tutela della salute per l'accesso ai luoghi di lavoro. Chiediamo quindi la collaborazione di tutti (pazienti, dipendenti, collaboratori, visitatori) per il rispetto del "*protocollo di regolamentazione delle misure per il contrasto e il contenimento della diffusione del virus Covid-19 negli ambienti di lavoro* "condiviso tra Governo e Parti sociali.

Queste misure approvate anche dal Garante Privacy, impongono il trattamento di dati personali, e talvolta di dati particolari. Tali dati verranno trattati unicamente nelle modalità e per le finalità di seguito esposte:

TITOLARE DEL TRATTAMENTO
Casa di Cura Privata Villa Esther S.r.l.

Casa di Cura Privata Villa Esther S.r.l., via Gino Di Biase n. 18 – 86021 Bojano (CB) Tel. 0874/751001 - privacy@villaesther.it

DATA PROTECTION OFFICER DPO/RESPONSABILE DELLA PROTEZIONE DEI DATI RPD

Casa di Cura Privata Villa Esther S.r.l. ha provveduto a nominare il Responsabile della Protezione dei Dati, che è raggiungibile ai seguenti indirizzi:
Casa di Cura Privata Villa Esther S.r.l., via Gino Di Biase n. 18 – 86021 Bojano (CB) Tel. 0874/751001 - privacy@villaesther.it

TIPOLOGIA DI DATI TRATTATI

Con riferimento al trattamento oggetto della presente informativa, il personale autorizzato procederà alla misurazione della temperatura e tratterà i seguenti dati personali anche particolari (c.d. sensibili): - nome, cognome, stato di salute con specifiche patologie e misurazione della temperatura corporea (c.d. febbre). Si precisa che soltanto il dato rilevato mediante Termo-Scanner non verrà tracciato ad eccezione di particolari condizioni quali il superamento della soglia di 37,5°.

Finalità Del Trattamento	*Base Giuridica*	*Periodo Conservazione Dati*	*Natura Del Conferimento*
Prevenzione contagio COVID-19 ed eventuale attivazione protocollo di sicurezza sanitaria. Il Titolare precisa che nel caso in cui la temperatura corporea dovesse essere pari o superiore a 37,5° l'interessato non potrà accedere in struttura. A fronte di tale situazione l'interessato verrà invitato a leggere le istruzioni di cui al Ministero della Salute previste per COVID-19 e a rispettare scrupolosamente quanto gli verrà indicato dal nostro personale.	Principi generali per la tutela e la salute nei luoghi di lavoro: Art. 6 par. 1 lett. c) GDPR obbligo di legge (art. 2087 c.c. e d.lgs. 81/08 tutela salute e sicurezza nei luoghi di lavoro; DPCM 11/03/2020 art 1 n. 7 lett d) e lett. d) salvaguardia dell'interesse vitale degli operatori che collaborano con il Titolare e di altre persone fisiche quali i visitatori - Art. 9 par. 2 lett. b) – assolvere obblighi ed esercitare diritti specifici del titolare o dell'interessato in materia di diritto del lavoro e della protezione sociale e sicurezza sociale.	fino a conclusione dell'emergenza sanitaria e secondo le indicazione impartite dal Governo e ad ogni modo non oltre il 31 dicembre c.a.	Il conferimento dei dati è obbligatorio. Il rifiuto comporterà l'impossibilità di accedere nella struttura.

DESTINATARI/CATEGORIE DI DESTINATARI DEI DATI

Qualora si renda necessario i dati trattati saranno comunicati a soggetti indicati dalla legge quali ad esempio: ufficio che si occupa della gestione del personale; addetto alla sicurezza sui luoghi di lavoro, A.S.R.E.M., Protezione Civile, Inail, medico del lavoro e altri soggetti previsti dalla legge.

TRASFERIMENTO DATI VERSO UN PAESE EXTRA UE

I dati personali non saranno trasferiti in paesi fuori dall'Unione Europea.

DIRITTI DEGLI INTERESSATI

Lei potrà far valere i propri diritti come espressi dagli artt. 15 e ss. del Regolamento UE 2016/679, rivolgendosi direttamente al Titolare ai contatti sopra riportati. In particolare, Lei ha il diritto, in qualunque momento di ottenere, da parte del Titolare, l'accesso ai Suoi dati personali e richiedere le informazioni relative al trattamento nonché limitare il loro trattamento. Nel caso in cui ritenga che il trattamento dei dati personali effettuato dal titolare avvenga in violazione di quanto previsto dal Regolamento (UE) 2016/679, lei ha il diritto di proporre reclamo alla Autorità di controllo – Garante Italiano (https://www.garanteprivacy.it/).

Il lavoratore è in ogni caso invitato ad informare tempestivamente e responsabilmente il datore di lavoro della presenza di qualsiasi sintomo influenzale durante l'espletamento della prestazione lavorativa, avendo cura di rimanere ad adeguata distanza dalle persone presenti.

Si ringrazia per la gentile collaborazione

VILLA ESTHER

REGISTRO FORMAZIONE ADEGUAMENTO PRIVACY - REG.UE 2016/679 – D.lgs. 101/2018

COGNOME	NOME	SETTORE DI APPARTENENZA	DATA	ARGOMENTI	FIRMA
				IL NUOVO REGOLAMENTO EUROPEO 2016/679 ED IL CODICE COMPORTAMENTALE DEI SOGGETTI AUTORIZZATI E DEI COLLABORATORI	

I dati raccolti ai sensi dell'art.13 del REG.UE 2016/679 sono ad uso esclusivo dell'attestazione della formazione conservati soltanto in maniera cartacea presso:
Casa di Cura Privata Villa Esther S.r.l.

DPO – Silvana Ciullo

Docente - Dott. Gianluca Angelicola

VILLA ESTHER

REGISTRO FORMAZIONE ADEGUAMENTO PRIVACY - REG.UE 2016/679 – D.lgs. 101/2018

COGNOME	NOME	SETTORE DI APPARTENENZA	DATA	ARGOMENTI	FIRMA
			15/04/2021	IL NUOVO REGOLAMENTO EUROPEO 2016/679 ED IL CODICE COMPORTAMENTALE DEI SOGGETTI AUTORIZZATI E DEI COLLABORATORI REGOLE AZIENDALI PER L'UTILIZZO DEI SISTEMI INFORMATICI	

I dati raccolti ai sensi dell'art.13 del REG.UE 2016/679 sono ad uso esclusivo dell'attestazione della formazione conservati soltanto in maniera cartacea presso:
Casa di Cura Privata Villa Esther S.r.l.

DPO – Silvana Ciullo

Docente - Dott. Gianluca Angelicola

VILLA ESTHER
casa di cura

REGISTRO DI CUSTODIA E AFFIDAMENTO DELLE CHIAVI E DELLE E-MAIL – REDATTO AI SENSI DELL'ART. 32 REG.UE 2016/679.

Ai fini della sicurezza delle informazioni e della protezione dei dati personali il Titolare, o la persona da Questi designata, compila il seguente registro avendo cura di indicare il locale e/o gli schedari/armadi dotati di serrature ed il soggetto affidatario delle chiavi.

Necessario tenere aggiornata la parte del registro inerente il numero di copie esistenti per ciascuna chiave.

LOCALE/SCHEDARIO/ARCHIVIO **N. COPIE CHIAVI (COMPRESO ORIGINALE)**

LOCALE SCHEDARIO/ARCHIVIO FISICO	AFFIDATARIO	DATA CONSEGNA	FIRMA	DATA RESTITUZIONE	FIRMA
		___/___/_____		___/___/_____	
		___/___/_____		___/___/_____	
		___/___/_____		___/___/_____	
		___/___/_____		___/___/_____	
		___/___/_____		___/___/_____	
		___/___/_____		___/___/_____	
		___/___/_____		___/___/_____	
		___/___/_____		___/___/_____	
		___/___/_____		___/___/_____	

VILLA ESTHER
casa di cura

INDIRIZZO E-MAIL	AFFIDATARIO	DATA CONSEGNA	FIRMA	DATA RESTITUZIONE	FIRMA
		___/___/_____		___/___/_____	
		___/___/_____		___/___/_____	
		___/___/_____		___/___/_____	
		___/___/_____		___/___/_____	
		___/___/_____		___/___/_____	
		___/___/_____		___/___/_____	
		___/___/_____		___/___/_____	
		___/___/_____		___/___/_____	
		___/___/_____		___/___/_____	
		___/___/_____		___/___/_____	
		___/___/_____		___/___/_____	
		___/___/_____		___/___/_____	
		___/___/_____		___/___/_____	
		___/___/_____		___/___/_____	

REGISTRO DEGLI ASSET (HARDWARE E SOFTWARE)

VILLA ESTHER
casa di cura

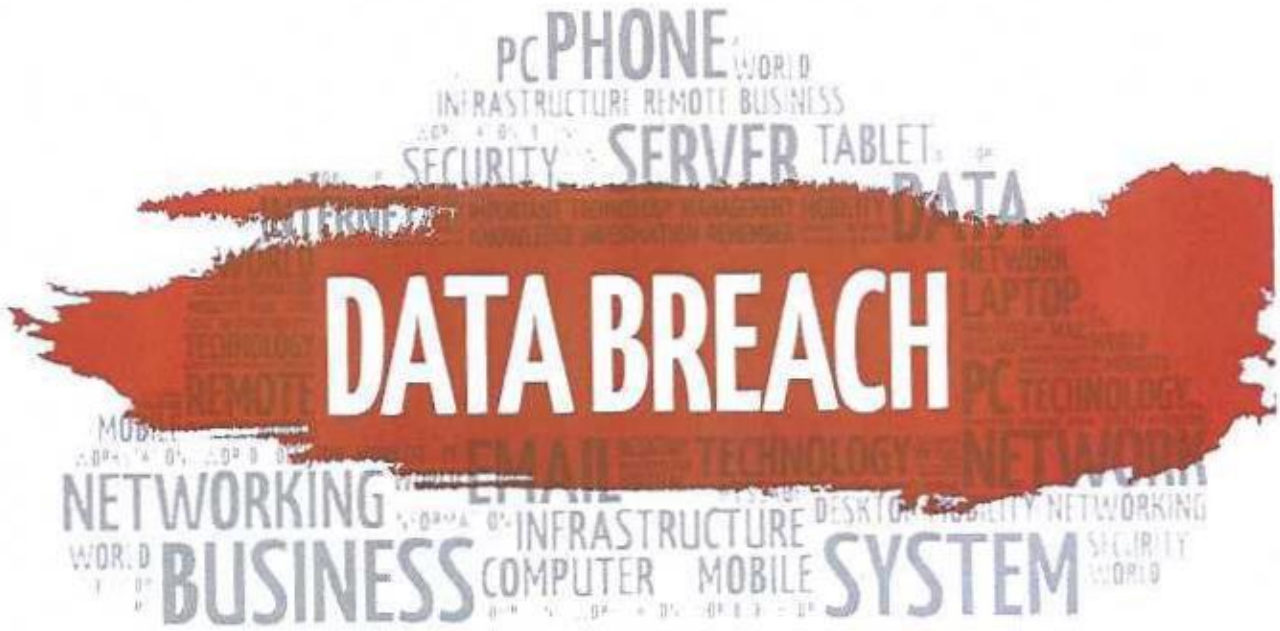
NOME IDENTIFICATIVO	CATEGORIA	SISTEMA OPERATIVO	UTENTE	DESCRIZIONE

Bojano (CB), lì ____/____/_____

Allegato 18

_____

POLICY PER LA GESTIONE DEI DATA BREACH



TITOLARE DEL TRATTAMENTO DATI: CASA DI CURA VILLA ESTHER

Rev.01 del 24/01/2022

INTRODUZIONE

La presente Procedura per la gestione del ***Data Breach*** ha lo scopo di fornire le indicazioni pratiche in caso di Violazione dei Dati Personali.

NORMATIVA DI RIFERIMENTO (REG.UE 2016/679)

Articolo 33

Notifica di una violazione dei dati personali all'autorità di controllo

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.
3. La notifica di cui al paragrafo 1 deve almeno:
a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

Articolo 34

Comunicazione di una violazione dei dati personali all'interessato

1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.
2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).
3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:
a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.
4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

GLOSSARIO E ACRONIMI

Autorità di Controllo: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 GDPR;
Dati Comuni: sono tutti i Dati Personali che non appartengono alle categorie dei Dati Particolari e Dati Giudiziari;
Dati Giudiziari: Dati Personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza;
Dati Particolari: Dati Personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;
Dati relativi alla Salute: i Dati Personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
Dato Personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile ("**Interessato**"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
Device Fissi: si intendono gli strumenti informatici non facilmente removibili dal perimetro aziendale quali personal computer, server locali, stampanti affidati alle Persone Autorizzate per uso professionale;
Device Mobili: in generale si intendono quegli strumenti informatici che per loro natura sono facilmente asportabili dal perimetro aziendale quali chiavette USB, SD cards, hard disk esterni, tablet e smartphone utilizzati dalla Persone Autorizzate per uso professionale;
DPO o **Data Protection Officer**: è una persona fisica, nominata obbligatoriamente nei casi di cui all'art. 37.1 GDPR dal Titolare o dal Responsabile del Trattamento e deve possedere una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati per assisterli nel rispetto a livello interno del GDPR;
GDPR o **Regolamento:** Regolamento Generale sulla Protezione dei dati personali (UE) 2016/679;

Incaricato/i o Persona/e Autorizzata/e: si tratta dei Collaboratori autorizzati al Trattamento dei Dati Personali sotto la diretta autorità del Titolare e/o del Responsabile ex artt. 4(10) e 29 del GDPR. Stante la definizione fornita dal Gruppo di Lavoro Articolo 29 dell'Opinione 2/2017 questa definizione ricomprende: dipendenti ed ex dipendenti, dirigenti, sindaci, collaboratori e lavoratori a partita IVA, lavoratori a chiamata, part-time, *job-sharing*, contratti a termine, stage, senza distinzione di ruolo, funzione e/o livello, nonché consulenti e fornitori del **Titolare**, più in generale, tutti coloro che utilizzino od abbiano utilizzato Strumenti Aziendali o Strumenti Personali operino sulla Rete Aziendale ovvero siano a conoscenza di informazioni aziendali rilevanti quali, a titolo esemplificativo e non esaustivo: (a) i Dati Personali di clienti, dipendenti e fornitori, compresi gli indirizzi di posta elettronica; (b) tutte le informazioni aventi ad oggetto informazioni confidenziali di natura commerciale, finanziaria o di strategia di business; nonché (c) i dati e le informazioni relative ai processi aziendali, inclusa la realizzazione di marchi, brevetti e diritti di proprietà industriale, la cui tutela prescinde dagli effetti pregiudizievoli che potrebbe comportare la diffusione delle medesime;

Limitazione Di Trattamento: il contrassegno dei Dati Personali conservati con l'obiettivo di limitarne il Trattamento in futuro;

Processo Decisionale Automatizzato: decisione basata unicamente sul Trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona;

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

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

Responsabile del Trattamento o **Responsabile**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta Dati Personali per conto del Titolare del Trattamento; deve presentare garanzie sufficienti di attuare misure tecniche e organizzative adeguate in modo tale che il Trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato;

Rete Aziendale: rappresenta il perimetro digitale dello **Associazione**, possibilmente contenente Dati Personali e/o informazioni riservate, comprensivo dei dispositivi hardware/software sia per la gestione dei servizi interni (es. switch, LAN, Wi-Fi) che dei collegamenti da o verso l'esterno (es. boundary router, SSH, VPN).

Strumenti Aziendali: l'insieme di Device Fissi e Device Mobili concessi in comodato d'uso dal **Titolare** alle Persone Autorizzate al fine di svolgere le proprie mansioni comprensivi altresì di eventuali strumenti di diagnostica necessari per l'erogazione della prestazione medica (es.: radiografo);

Strumenti Personali: i Device Mobili di proprietà delle Persone Autorizzate autorizzati ad essere impiegati per uso professionale;

Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il Titolare del Trattamento, il Responsabile del Trattamento e le Persone Autorizzate al Trattamento dei Dati Personali sotto l'autorità diretta del Titolare o del Responsabile;

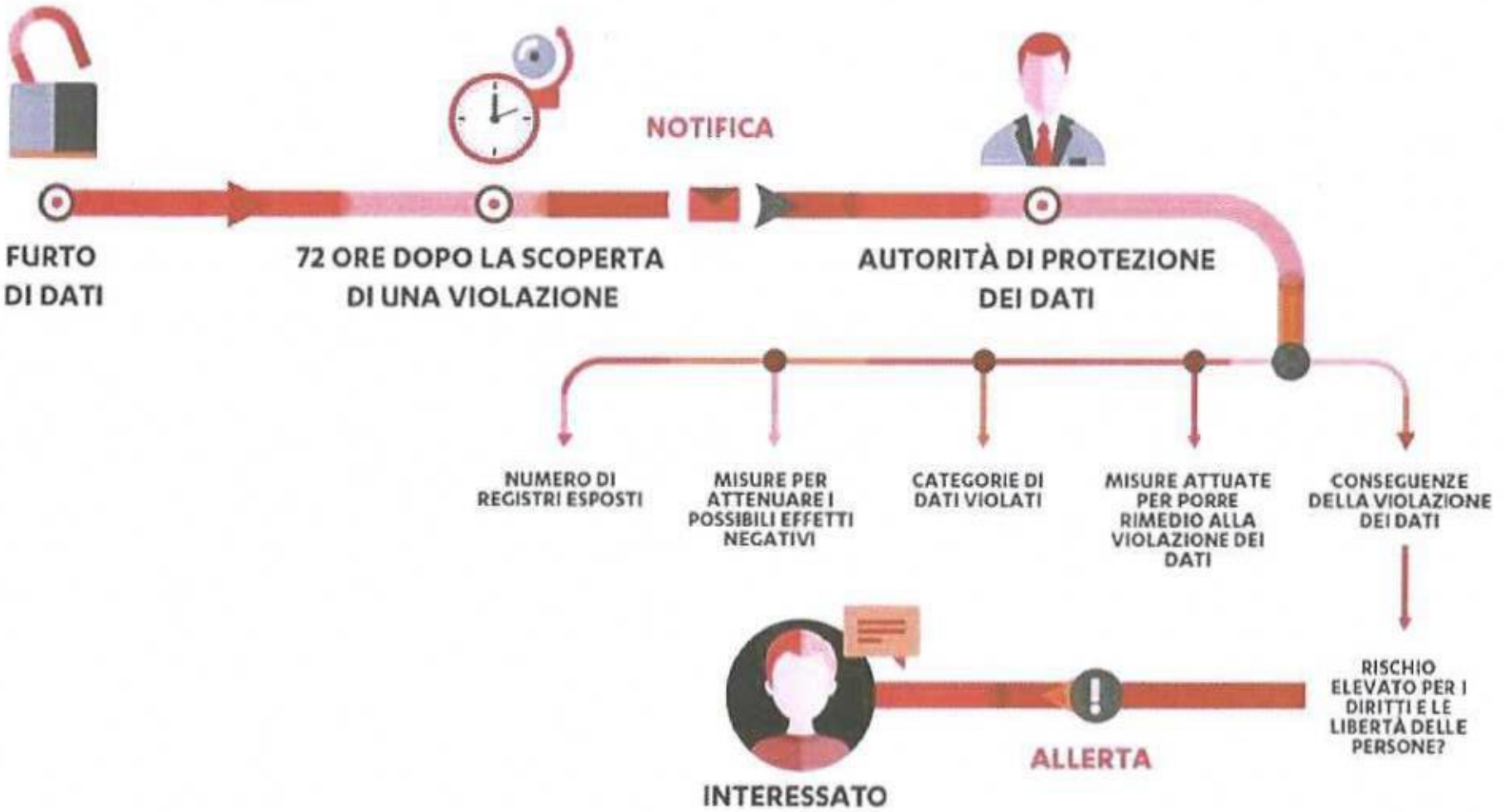
Titolare del Trattamento o **Titolare:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del Trattamento di dati personali; quando le finalità e i mezzi di tale Trattamento sono determinati dal diritto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

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

Violazione Dei Dati Personali ovvero **Data Breach:** è 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.

PREMESSA	**PREMESSA** **COSA È UN DATA BREACH?** Con il termine ***DATA BREACH*** si intende un incidente di sicurezza in cui dati personali, protetti o riservati vengono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato. Solitamente il data breach si realizza con una divulgazione di dati riservati o confidenziali all'interno di un ambiente privo di misure di sicurezze (da esempio, su web) in maniera involontaria o volontaria. Tale divulgazione può avvenire in seguito a: • ***perdita accidentale***: ad esempio, data breach causato da smarrimento di una chiavetta USB contenente dati riservati; • ***furto***: ad esempio, data breach causato da furto di un notebook contenente dati confidenziali; • ***infedeltà aziendale***: ad esempio, data breach causato da una persona interna che avendo autorizzazione ad accedere ai dati ne produce una copia distribuita in ambiente pubblico. • ***accesso abusivo***: ad esempio, data breach causato da un accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite. **POSSIBILI CONSEGUENZE** Quando si verifica un data breach, possono esserci tre possibili effetti collaterali: • Data breach di confidenzialità, quando i dati sono oggetto di divulgazione o accesso da parte di terzi non ***autorizzati;*** • Data breach di disponibilità, quando i dati non sono più disponibili temporaneamente o definitivamente; • Data breach di integrità, quando i dati sono modificati e quindi non più affidabili.
ISTRUZIONI	1) Al verificarsi di uno degli eventi indicati nelle premesse il Singolo soggetto designato/autorizzato al trattamento di dati personali dovrà tempestivamente darne comunicazione scritta al Titolare ed in copia al responsabile dei Sistemi IT entro e non oltre 24 ore dalla conoscenza della violazione; 2) Il Responsabile IT, accertata la violazione, valuterà la gravità dell'evento e contestualmente avviserà il DPO (Responsabile della Protezione dei Dati) documentando data e ora dell'evento, tipologia dei dati coinvolti e relativo ASSET (cartaceo/informatico); 3) Il Titolare, dopo aver consultato il DPO, si attiverà per procedere con le segnalazioni previste dalla legge tramite il sito dell'Autorità Garante (https://servizi.gpdp.it/databreach/s/); 4) Qualora sia stata accertata l'entità considerevole della Violazione di dati personali si procederà ad avvisare i soggetti interessati fornendo indicazioni sulla natura e sulle possibili conseguenze del Data Breach (es: cambio password); 5) Il Titolare avviserà se del caso la Polizia Postale per le opportune indagini ispettive. 6) Il Titolare, di concerto con il DPO, aggiorna il registro delle violazioni dei dati personali; **Tutta la procedura deve concludersi entro 72 ore dall'avvenuta conoscenza del Data Breach.**

Esempio di DATA BREACH



Credits image Kaspersky

ALLEGATI

SCHEDA EVENTO	
CODICE	
Data evento e ora della violazione anche solo presunta (specificando se è presunta)	
Fonte di segnalazione	
Tipologia evento anomalo	
Descrizione evento anomalo	
Numero interessati coinvolti	
Numerosità dei dati personali di cui si presume la violazione	
Data, anche presunta, della violazione e del momento in cui se ne è avuta conoscenza	
Luogo in cui è avvenuta la violazione dei dati (specificare se è avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)	
Descrizione dei sistemi di elaborazione e/o memorizzazione dei dati coinvolti, con indicazione della loro ubicazione	

VIOLAZIONE DI DATI PERSONALI

MODELLO DI COMUNICAZIONE AL GARANTE

Titolare che effettua la comunicazione

Denominazione o ragione sociale: _____

Provincia _____ Comune _____

Cap._____ Indirizzo _____

Nome persona fisica addetta alla comunicazione _____

Cognome persona fisica addetta alla comunicazione _____

Funzione rivestita _____

Indirizzo Email/PEC per eventuali comunicazioni _____

Recapito telefonico per eventuali comunicazioni _____

Eventuali Contatti (altre informazioni) _____

Natura della comunicazione

☐ Nuova comunicazione

☐ Inserimento ulteriori informazioni sulla precedente comunicazione (Numero di riferimento)

☐ Ritiro precedente comunicazione

Breve descrizione del trattamento di dati personali

Quando si è verificata la violazione di dati personali?

☐ Il _____/_____ / _____

☐ Tra il _____/_____ / _____e il _____/_____ / _____

☐ In un tempo non ancora determinato

☐ È possibile che sia ancora in corso

Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

Modalità di esposizione al rischio?

Tipo di violazione

☐ Lettura (presumibilmente i dati non sono stati copiati)

☐ Copia (i dati sono ancora presenti sui sistemi del titolare)

☐ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)

☐ Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)

☐ Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)

☐ Altro: .....

Dispositivo oggetto della violazione

☐ Postazione di lavoro

☐ Dispositivo di acquisizione o dispositivo-lettore

☐ Smart card o analogo supporto portatile

☐ Dispositivo mobile

☐ File o parte di un file

☐ Strumento di *backup*

☐ Rete

☐ Altro: .....

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione:

Quante persone sono state colpite dalla violazione di dati personali?

☐ N. ..... di persone

☐ Circa ..... persone

☐ Un numero (ancora) sconosciuto di persone

Che tipo di dati sono coinvolti nella violazione?

☐ Dati anagrafici

☐ Numero di telefono (fisso o mobile)

☐ Indirizzo di posta elettronica

☐ Dati di accesso e di identificazione (*user name*, *password*, *customer ID*, altro)

☐ Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro)

☐ Altri dati di personali (sesso, data di nascita, età, ...), dati sensibili e giudiziari Ancora sconosciuto

☐ Altro: .....

Livello di gravità della violazione dei dati biometrici (secondo le valutazioni del titolare)?

☐ Basso/trascurabile

☐ Medio

☐ Alto

☐ Molto alto

Misure tecniche e organizzative applicate ai dati colpiti dalla violazione

La violazione è stata comunicata anche agli interessati?

☐ Sì, è stata comunicata il .....

☐ No, perché .....

Qual è il contenuto della comunicazione ai contraenti (o alle persone interessate)?

Quale canale è utilizzato per la comunicazione ai contraenti (o alle persone interessate)?

Quali misure tecnologiche ed organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?

La violazione coinvolge contraenti (o altre figure interessate) che si trovano in altri Paesi UE?

☐ Sì

☐ No

La comunicazione è stata effettuata alle competenti autorità di altri Paesi UE?

☐ No

☐ Sì

Registro delle Violazioni				
Data	Descrizione	Comunicazione al Garante	Comunicazione all'interessato	Misure per evitare il ripetersi della violazione

REGISTRO DELLE ATTIVITA'
DI TRATTAMENTO DATI PERSONALI

ai sensi dell'art. 30 del REG.UE 2016/679

VILLA ESTHER
casa di cura

REGISTRO	**REGISTRO DEI TRATTAMENTI**	
SEDE	**Sede Legale:** Via Gino Di Biase n. 18 – 86021 Bojano (CB)	
Titolare trattamento dati	PERSONA Giuridica	**Casa di Cura Privata Villa Esther S.r.l.**
	P.I.	01706190707
	e-mail	info@villaesther.it
	PEC	casadicuravillaesther@pecsicura.it
	Sito Web	https://www.villaestherbojano.it/
	DPO	**Silvana Ciullo:** privacy@villaesther.it

Data revisione: 19 ottobre 2021

D.P.O.: ***Silvana Ciullo***

Il presente registro è una rappresentazione dell'organizzazione sotto il profilo delle attività di trattamento dati. Esso ha lo scopo di informare, dare consapevolezza e condivisione interna del processo di gestione del dato.

Ai sensi dell'art. 30 del GDPR, il Registro riporta le seguenti informazioni:

- dati di contatto del titolare del trattamento
- finalità per le quali sono trattati tali dati;
- categorie di interessati;
- categorie di dati personali;
- categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

TRATTAMENTO (PROVVISORIO): GESTIONE RISCHIO VIRUS COVID-19

DESIGNATI	
Persone autorizzate	Titolare e soggetti designati

Processo di trattamento	
Descrizione	Raccolta dati informazioni inerenti possibili sintomi riconducibili al COVID ed informazioni personali
Finalità del trattamento	finalità di prevenzione dal contagio da COVID-19, in esecuzione del Protocollo di sicurezza anti-contagio condiviso Governo/Parti sociali.
Base giuridica	DPCM 2 marzo 2021
Tipo di dati personali	all'attestazione di una temperatura corporea non superiore a 37,5; dichiarazioni attinenti tutte le misure della quarantena o dell'isolamento fiduciario con sorveglianza sanitaria
Categorie di interessati	Clienti, fornitori, dipendenti ed assimilàti
Categorie di destinatari	I dati personali non saranno oggetto di diffusione, né di comunicazione a terzi, se non in ragione delle specifiche previsioni normative (comunicazione all'Autorità sanitaria ed all' INAIL e condivisione di informazioni per la ricostruzione della filiera degli eventuali contatti stretti di un lavoratore risultato positivo al COVID-19).
Informativa	SI
Autorizzazione	n.a.
Frequenza trattamento	periodico
Termine cancellazione dati	14 gg
Trasferimento dati (paesi terzi)	No
ASSET	Cartaceo

TRATTAMENTO (PROVVISORIO): CONTROLLO GREEN PASS

DESIGNATI	
Persone autorizzate	Titolare e soggetti designati

Processo di trattamento	
Descrizione	Verifica del Certificato Verde "Green Pass" mediante App ufficiale Verifica C19
Finalità del trattamento	finalità di prevenzione dal contagio da COVID-19, in esecuzione del D.L. 127 del 21 settembre 2021.
Base giuridica	art. 6 lett. c) del GDPR
Tipo di dati personali	Nome, cognome e data di nascita
Categorie di interessati	dipendenti ed assimilàti, collaboratori e fornitori
Categorie di destinatari	I dati personali non saranno oggetto di diffusione, né di comunicazione a terzi, salvo per i dipendenti, che a seguito di controllo a campione, risulti "non valido" il Green Pass
Informativa	SI
Frequenza trattamento	Periodico e a campione
Termine cancellazione dati	--
Trasferimento dati (paesi terzi)	No
ASSET	Smartphone su cui è installata la APP Verifica C-19

TRATTAMENTO (PROVVISORIO): SOSPENSIONE LAVORATIVA ED ALLONTANAMENTO DAL LUOGO DI LAVORO A SEGUITO DI GREEN PASS "NON VALIDO"

DESIGNATI	
Persone autorizzate	Titolare e soggetto designato

Processo di trattamento	
Descrizione	Applicazione del procedimento di sospensione lavorativa ed applicazione della sanzione a seguito di Verifica del Certificato Verde "Green Pass" mediante App ufficiale Verifica C19 il cui esito sia "non valido"
Finalità del trattamento	finalità di prevenzione dal contagio da COVID-19, in esecuzione del D.L. 127 del 21 settembre 2021.
Base giuridica	art. 6 lett. c) del GDPR
Tipo di dati personali	Dati identificativi, dati personali e dati particolari
Categorie di interessati	dipendenti ed assimilàti,
Categorie di destinatari	Prefetto/Ufficio del Personale
Informativa	SI
Frequenza trattamento	Al verificarsi dell'evento
Termine cancellazione dati	Disposizioni di legge (non oltre 10 anni)
Trasferimento dati (paesi terzi)	No
ASSET	Cartaceo ed informatico

LINEE GUIDA PER LA SICUREZZA DELL'ACCESSO AI DATI INFORMATICI

CORRETTO UTILIZZO DELLE WORKSTATION E DEI PC PORTATILI

L'utente che ha disposizione l'accesso a una workstation o un pc portatile ha il dovere di utilizzare la macchina solo ed esclusivamente per lo scopo per cui gli è stata affidata. Inoltre i dispositivi informatici sono strumenti di lavoro appartenenti al patrimonio aziendale e per questo devono essere utilizzati per fini professionali (ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza).

Il Personal Computer (PC) è uno strumento di lavoro affidato al Dipendente di cui lo stesso è responsabile sia per la parte Hardware che Software. Il PC deve essere utilizzato per i soli ambiti inerenti all'attività lavorativa; eventuali informazioni salvate -anche temporaneamente- sulla postazione di lavoro, devono pertanto riguardare esclusivamente la propria attività lavorativa. Ogni utilizzo del PC non afferente alla propria attività lavorativa può contribuire ad innescare disservizi, costi di assistenza e manutenzione e, soprattutto, minacce alla sicurezza dell'intera rete aziendale e/o delle reti telematiche e dei sistemi informatici di terzi esponendo l'organizzazione e gli stakeholder aziendali a crimini informatici.

Tutti i dipendenti della Casa di Cura Villa Esther sono a conoscenza che i dati conservati nel proprio Personal Computer, compresi i messaggi di posta elettronica in entrata e in uscita, possono essere visionati dai Responsabili della struttura in caso di necessità dovute a titolo esemplificativo e non esaustivo, a malfunzionamenti del sistema, esigenze lavorative, assenza dell'Incaricato, ecc... I Responsabili di struttura, pertanto, per l'espletamento delle loro funzioni, hanno la facoltà in qualunque momento di accedere ai dati trattati dai propri collaboratori, ivi compresi gli archivi di posta elettronica in entrata ed uscita, chiedendo formalmente accesso alla struttura I.T. Per cui sono assolutamente vietati comportamenti atti a vietare tali accessi (archivi protetti da password, crittografati, etc.). Nel caso in cui l'utente sia costretto ad assentarsi dal locale in cui è ubicata la stazione di lavoro o nel caso ritenga di non essere in grado di presidiare l'accesso alla medesima è tenuto ad eseguire una delle seguenti operazioni: spegnimento, blocco o disconnessione dalla sessione di lavoro. Ad ogni modo, sulle postazioni di lavoro (fisse e laptop) è stata implementata una policy che prevede il blocco automatico della postazione dopo alcuni minuti di inattività e che richiede di nuovo l'accesso con password.

UTILIZZO DELLE CREDENZIALI DI AUTENTICAZIONE

L'accesso all'elaboratore è protetto da codice identificativo e password (credenziali), che devono essere custodite con la massima diligenza e non divulgate, né trascritte su mezzi facilmente accessibili. Le credenziali di autenticazione per l'accesso ai dispositivi ed alla rete vengono predisposte dagli amministratori della struttura I.T. all'atto dell'assunzione del nuovo dipendente in seguito a confacente comunicazione della struttura Politiche e Gestione Risorse Umane e devono essere obbligatoriamente modificate al primo accesso. La password di accesso alla rete ha un periodo di validità limitato; ad intervalli regolari verrà quindi richiesto all'utente di modificare la password. La password scelta non deve contenere riferimenti agevolmente riconducibili all'Autorizzato, deve essere modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. L'utente non può riutilizzare una password già utilizzata. In caso di estinzione del rapporto contrattuale con l'Incaricato, la struttura Gestione Risorse Umane ne dà tempestiva comunicazione alla struttura I.T. e questi provvede ad inibire l'accesso alle postazioni entro tre giorni lavorativi dal ricevimento della comunicazione (o non appena ne venga a conoscenza).

CREDENZIALI DI ACCESSO AI SERVIZI E AGLI APPLICATIVI

L'Utente che lavora sulla singola macchina potrà gestire ulteriori password legate a software gestionali. Sebbene tali software siano dati in concessione d'utilizzo o completamente esternalizzati e il reparto I.T. non abbia alcun controllo su di essi, la Casa di Cura Villa Esther garantisce che le policy di sicurezza ed accesso garantite del fornitore siano completamente compatibili con l'utilizzo aziendale e con le norme presenti in tale documento.

Per cui a titolo esemplificativo, anche per questi software l'utente ha la facoltà e l'obbligo di monitorare le credenziali seguendo le regole già descritte. Più in generale, l'utente che ha la facoltà di accesso a tali software è tenuto a rispettare le norme e i comportamenti sopra descritti per l'accesso ai dispositivi.

CORRETTO UTILIZZO DELLE CREDENZIALI

Gli utenti sono responsabili della custodia e dell'utilizzo delle proprie credenziali di autenticazione; la password, formata da lettere (maiuscole e minuscole), numeri e/o caratteri speciali, nei limiti consentiti dai sistemi, deve avere le seguenti caratteristiche:

- deve essere di lunghezza non inferiore ad 8 caratteri oppure, nel caso in cui ciò non sia possibile, da un numero di caratteri pari al massimo consentito dal connesso applicativo;
- deve essere composta da caratteri maiuscoli, caratteri minuscoli, numeri e caratteri speciali (es.Hatv%67g);
- non deve contenere riferimenti agevolmente riconducibili all'Incaricato o ad ambiti noti;
- deve essere obbligatoriamente cambiata al primo utilizzo e successivamente ogni 180 giorni (per quanto concerne le credenziali di dominio esiste un meccanismo di scadenza automatica);
- deve essere diversa dalle ultime 10 password precedentemente utilizzate;
- non deve essere basata su nomi di persone, date di nascita, animali, oggetti o parole ricavabili dal dizionario (anche straniere), o tratta da informazioni personali;
- non deve presentare una sequenza di caratteri identici o in gruppi di caratteri ripetuti;
- non deve essere memorizzata in funzioni di log-in automatico, in un tasto funzionale o nel browser utilizzato per la navigazione Internet;
- deve essere annullata e sostituita con una nuova - per motivate necessità di urgente accesso alle informazioni ed impedimento del titolare delle credenziali - da parte degli amministratori dei servizi o loro delegati. In questo caso essa dovrà essere nuovamente modificata al primo accesso da parte dell'Incaricato.

Qualora le limitazioni tecniche del sistema non permettano la configurazione dello stesso al fine di limitare selettivamente l'utilizzo di password "robuste", sarà onere dell'utilizzatore l'impostazione di password secondo le specifiche in precedenza elencate.

L'utente si impegna a non cedere a terzi le proprie credenziali di accesso alla rete, consapevole che la cessione delle stesse consente ad altri l'accesso e l'utilizzo dei relativi servizi, ovvero l'accesso ai dati cui il soggetto è abilitato con conseguenze quali la visualizzazione di informazioni riservate, la distruzione e/o modifica di dati.

È assolutamente proibito accedere alla rete e ai programmi con delle credenziali di autenticazione, in particolare con un codice d'identificazione utente, diverso da quello assegnato. La responsabilità di qualsiasi azione svolta dopo aver eseguito la procedura di autenticazione sarà attribuita all'utente assegnatario delle credenziali. L'utente è quindi responsabile, sia nei confronti dell'Azienda che di terzi, di fatti e atti illeciti, con particolare riferimento all'immissione in rete di contenuti critici o contrari all'ordine pubblico o al buon costume così come definiti dalla giurisprudenza corrente.

È fatto divieto annotare la password su supporti facilmente rintracciabili (quali post-it, quaderni, ecc...) e, soprattutto, in prossimità della stazione di lavoro utilizzata.

L'utente si impegna a modificare tempestivamente la password d'accesso alla rete qualora tale dato sia stato rubato, smarrito, o sia noto a terzi, dandone comunicazione alla struttura I.T. L'Azienda si fa garante della custodia dei dati personali forniti dall'utente e si impegna a non rivelarli a terzi, se non a fronte di legittima richiesta da parte di Autorità Giudiziaria, Autorità di Pubblica Sicurezza e Garante per la Protezione dei Dati Personali.

CREDENZIALI AMMINISTRATIVE

I privilegi di amministrazione sono limitati ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi previa nomina formale ad "Amministratori di Sistema". Laddove il sistema lo permetta, i permessi amministrativi saranno concessi in maniera granulare per consentire unicamente l'evasione delle attività elencate nell'ambito di operatività per cui l'amministratore è stato nominato.

Nella Casa Di Cura Villa Esther non è previsto l'inventario delle utenze amministrative sono invece state consegnate all'amministratore unico e al DPO una busta chiusa con le credenziali di accesso con potere amministrativo per il solo Domain Controller.

UTILIZZO E CUSTODIA DI PEN-DRIVE, CD DATI E SIMILI

Per i supporti magnetici e device esterni si applicano gli stessi criteri che per i documenti cartacei e pertanto la loro custodia dovrà avvenire sempre sottochiave e non dovranno mai essere lasciati incustoditi. Tutti i file di provenienza incerta o esterna -ancorché attinenti all'attività lavorativa- devono essere sottoposti a controllo antivirus prima di essere aperti e/o utilizzati.

I supporti rimovibili (CD e DVD anche riscrivibili, supporti USB, hard disk ecc.) devono essere limitati a quelli strettamente indispensabili alle attività aziendali; in tali supporti non devono essere conservati, nemmeno provvisoriamente, file aziendali congiuntamente a file personali.

Non è permesso scaricare o copiare file contenuti in supporti removibili esterni (USB, hard disk drive, "chiavette USB", ecc..) se non attinenti alla propria attività lavorativa.

Nel caso in cui dati, informazioni, immagini e/o notizie aziendali e/o dati riservati debbano essere salvate su supporti removibili, è obbligatorio conservare, custodire e controllare tali supporti affinché nessun soggetto terzo non autorizzato ne prenda visione o possesso. L'utente assegnatario è l'unico responsabile della custodia dei supporti e dei dati in essi contenuti. I supporti rimovibili devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato e/o alterato e/o distrutto, o, successivamente alla cancellazione, recuperato. Al fine di assicurare la distruzione e/o inutilizzabilità di supporti rimovibili, ciascun utente dovrà utilizzare gli strumenti messi a disposizione dal sistema operativo in uso per procedere alla formattazione a basso livello del supporto.

L'amministratore di sistema ha, in ogni caso, la possibilità di impedire ad ogni singola macchina e/o utente l'utilizzo di suddetti supporti.

UNITÀ DI RETE, MEMORIZZAZIONE FILE E BACKUP

Il disco fisso locale (quindi le cartelle di utilizzo frequente come Desktop, Documenti, etc..) del proprio PC deve essere utilizzato per la sola memorizzazione di file di interesse aziendale. La memorizzazione deve essere limitata a poche ore lavorative dal momento che questi dischi non sono sottoposti a backup. Tutti i file di rilevanza aziendale devono essere salvati sulle aree comuni o sulle aree personale delle share di rete (cartella My Home). È assolutamente da evitare la conservazione in rete di file obsoleti e/o inutili e/o ridondanti e per questo si invita il dipendente ad un attento ed ordinato utilizzo dello spazio di rete.

Qualsiasi file estraneo all'attività lavorativa e/o non espressamente autorizzato, non può, nemmeno in via transitoria, essere salvato sul PC in uso del dipendente e tanto meno essere salvato sulla rete aziendale. La competenza e la gestione delle aree di interesse comune è demandata ai responsabili di funzione di ciascuna area che provvederà ad indicare ai propri collaboratori i criteri sulle modalità di salvataggio e protocollo dei documenti.

Casa di Cura Villa Esther per mezzo dei sui fornitori gestisce lo storage aziendale; i dati conservati in tali aree sono protetti da procedure di backup automatico gestite e monitorate dal concessionario stesso; la policy attuale è configurata per un backup giornaliero e un'archiviazione full mensile con profondità di 1. Il backup incrementale salva i dati inseriti o modificati rispetto all'ultimo backup incrementale eseguito; qualora un file venisse cancellato, può essere ripristinato dai salvataggi per 7 giorni (per poi essere rimosso). Ogni mese viene fatta un'archiviazione completa dei dati, una sorta di fotografia dei dati presenti in quel momento. Questo salvataggio viene mantenuto nei backup per 1 anno. Alla fine dell'anno il salvataggio viene cancellato. Per il ripristino dei dati accidentalmente persi o modificati sulle cartelle di rete è fatto obbligo di avvisare tempestivamente la struttura I.T.

Le copie di backup sono memorizzate di norma su supporti/sistemi custoditi fisicamente in locali ad accesso controllato in completa gestione mentre almeno una copia di backup di alcuni tipi di dati più importanti viene memorizzata su supporti/sistemi distinti logicamente o fisicamente e non direttamente accessibili al sistema stesso.

Le cartelle di rete presenti negli storage sono aree di condivisione di informazioni strettamente professionali e non devono in alcun modo essere utilizzate per scopi diversi; qualunque file non legato all'attività lavorativa non può essere dislocato, nemmeno temporaneamente, in queste unità. Il personale della struttura I.T., senza necessità di esplicita autorizzazione, si riserva la facoltà di procedere alla verifica ed eventuale rimozione di qualsiasi file memorizzato nelle cartelle di rete qualora ritenuto pericoloso per la sicurezza o non attinente all'attività lavorativa. I privilegi di lettura e scrittura delle cartelle vengono definiti dal responsabile di struttura (o suo delegato) valutando il bilanciamento delle esigenze della produttività e della necessaria riservatezza. Tramite una stringente policy aziendale non è data all'utente la possibilità di modificare tali permessi.

Nel caso di cessazione del rapporto di lavoro (mobilità in uscita, pensionamento, dimissioni o decesso), trascorsi ulteriori 60 giorni, periodo stimato pertinente e non eccedente a garantire l'operatività e la continuità di servizio, salvo diverse indicazioni degli assegnatari o dei responsabili, specifiche richieste e casi particolari che verranno opportunamente trattati, il personale della struttura I.T. procederà alla cancellazione definitiva della cartella di rete assegnata in modalità esclusiva e non sarà possibile recuperare i dati in essa contenuti.

MOVIMENTAZIONE DI DATI CON PARTICOLARI REQUISITI DI RISERVATEZZA

Nell'invio di dati afferenti alle "categorie particolari" secondo il Regolamento UE 2016/679 tramite posta elettronica, la spedizione del file deve avvenire in forma di allegato e non come testo del messaggio. Il file allegato dovrà essere protetto con modalità idonee a impedire l'illecita o fortuita acquisizione da parte di soggetti diversi dal destinatario che potrà consistere in una password per l'apertura del file o in una chiave crittografica rese note agli interessati attraverso separata comunicazione (come richiesto dalla vigente normativa).

UTILIZZO INTERNO ED ESTERNO DELLA POSTA ELETTRONICA ORDINARIA

L'indirizzo e-mail assegnato da Villa Esther ai dipendenti è uno strumento di lavoro di proprietà aziendale concesso in uso al lavoratore per un più proficuo svolgimento della prestazione. La Posta Elettronica può essere rilasciata "ad personam", associata ad un ufficio o ad una specifica funzione/progetto/servizio. Le persone assegnatarie delle caselle sono responsabili del corretto utilizzo delle stesse. Tale indirizzo va utilizzato in via esclusiva per tutta la corrispondenza elettronica in entrata ed in uscita. È espressamente vietato utilizzare caselle di posta diverse da quella assegnata reperibili in Internet, quali webmail fornite, ad esempio, da Yahoo, Libero, Hotmail, etc

La posta elettronica è controllata da una piattaforma Google Workspace.

Il dipendente è responsabile del contenuto dei messaggi inviati: al fine di garantire la sicurezza dei sistemi informativi aziendali è vietato utilizzare le caselle di posta assegnate per l'invio di messaggi personali o di contenuto extra lavorativo.

Non è consentito l'utilizzo di caselle di posta elettronica personali, al di fuori di quella aziendale, per le comunicazioni istituzionali. Non è altresì permesso l'utilizzo di caselle di posta aziendali diverse da quella/e assegnate. Tutte le mailbox sono configurate affinché eventuali comunicazioni email indirizzate al di fuori del dominio aziendale riportino un messaggio in calce nel quale viene dichiarata la natura non personale del messaggio nonché i vincoli in materia di riservatezza, con precisazione che le risposte potranno essere conosciute nell'organizzazione di appartenenza del mittente.

Gli allegati ai messaggi in entrata in formato non intrinsecamente sicuro vanno prima di qualsiasi altra iniziativa quando non ne sia personalmente noto il mittente. Gli allegati vanno se possibile trasmessi in formato universale e sicuro (PDF/A).

Tutti i messaggi e-mail da e per l'esterno sono di esclusiva disponibilità dell'Azienda, che potrà accedervi in qualsiasi momento, considerati i fini per cui tale utilizzo è ammesso ai sensi della presente policy. Non sono ammessi contenuti ed utilizzi diversi da quelli richiesti dalle finalità lavorative ed organizzative proprie dell'Azienda per il cui raggiungimento l'Azienda acconsente all'impiego di tale strumento.

SOCIAL NETWORK

Non è consentito l'utilizzo di alcun Social Network se non preventivamente autorizzato dalla Direzione Aziendale.

Il dipendente nell'utilizzo in forma privata, fuori dell'ambiente di lavoro, dei propri profili social è tenuto, anche in quanto pubblico dipendente, a non effettuare commenti denigratori o lesivi in genere della dignità di terzi e/o dell'Azienda. È altresì fatto assoluto divieto pubblicare qualsiasi contributo in forma di immagine o altro formato che possa essere lesivo della dignità, reputazione di terzi e/o dell'Azienda.

Quale conseguenza di utilizzo improprio dei propri profili social potranno essere attivati dall'Azienda procedimenti disciplinari a carico del responsabile e richieste di risarcimento dei danni eventualmente subiti da Villa Esther.

L'Azienda, qualora approvasse l'utilizzo di Social all'interno dell'amministrazione, si riserva la facoltà di attivare profili ufficiali aziendali strettamente correlati all'attività lavorativa.

UTILIZZO DELLA RETE FISICA LOCALE (LAN)

Tutte le postazioni di lavoro operano interconnesse alla rete aziendale e possono così accedere ai dati secondo precise abilitazioni. La rete aziendale interna non può esser utilizzata per scopi diversi da quelli ai quali è destinata.

La configurazione e la gestione di tutti gli apparati attivi e dell'infrastruttura di collegamento sono affidati al settore I.T.

Non è consentita la connessione alla rete aziendale di apparati atti ad effettuare connessioni con altre reti verso l'esterno (router, bridge, modem, impianti wireless, ecc.). Un eventuale uso di tali apparati, qualora necessario, dovrà essere richiesto alla struttura I.T. e ricevere autorizzazione dalle Direzioni competenti. Analogamente non è ammesso, se non per esigenze estemporanee e previa autorizzazione della struttura I.T., l'utilizzo non autorizzato di dispositivi per lo sdoppiamento di punti rete (mini Hub/switch).

Viene fatto esplicito e tassativo divieto di connettere in rete stazioni di lavoro ed ogni altro dispositivo informatico (es. computer e portatili non aziendali) se non previa esplicita e formale autorizzazione della struttura I.T.

È fatto assoluto divieto di configurare servizi già messi a disposizione in modo centralizzato, quali ad esempio, e non solo, DNS, DHCP, NTP, mailing, accesso remoto, proxy server.

È fatto assoluto divieto all'utente di intercettare ed analizzare i pacchetti sulla rete aziendale, utilizzando analizzatori di rete sia software che hardware. Nel caso si riscontrasse la presenza di PC che generano traffico anomalo o che potrebbero far diminuire le prestazioni dell'intero sistema, sarà facoltà del personale della struttura I.T. procedere al blocco, se necessario, dell'attività di rete della postazione.

È fatto divieto di svolgere attività intenzionali che portino in qualunque modo alla saturazione dei sistemi di elaborazione e di trasmissione dati, rendendo anche temporaneamente indisponibili risorse di uso comune agli utenti.

Non è consentito l'accesso agli armadi di rete, la modifica delle connessioni o la manomissione di qualunque impianto o cavo vi sia contenuto.

UTILIZZO DELLA RETE WIRELESS (WLAN)

Ad integrazione della rete LAN descritta nella precedente, alcune aree della Casa di Cura Villa Esther sono servite da reti non cablate -Wireless LAN- per consentire la trasmissione dei dati attraverso canali senza fili. Utilizzando specifici apparati Access Point vengono distribuiti tre SSID: "Villa Esther Admin", "Villa Esther System", "Villa Esther Ospiti".

La WiFi-LAN "Villa Esther System" risulta a tutti gli effetti un'estensione della rete LAN, pertanto, i client connessi, avranno la possibilità di accedere alle medesime risorse della rete locale cablata. La tecnologia è configurata e governata e solo l'amministrazione dispone per il rilascio delle abilitazioni per il tramite della struttura I.T. su comunicazione del MAC-ADDRESS dell'appartato. È fatto divieto assoluto di connettersi a tale infrastruttura utilizzando sistemi diversi dai dispositivi aziendali quali portatili e tablet preventivamente configurati dalla struttura I.T. (per esempio, è vietata la connessione di cellulari, oppure laptop e tablet personali).

La rete "Villa Esther System" è utilizzata al solo scopo di interconnessione dei sistemi strettamente legati al funzionamento delle periferiche di sistema. È tecnologicamente inibita qualunque connessione non preventivamente accordata dal servizio I.T.

La rete "Villa Esther Ospiti" è una rete wireless per fornire connettività Internet agli ospiti della struttura con la possibilità di collegare temporaneamente i propri dispositivi. La rete è completamente scollegata a livello logico da tutta l'infrastruttura informatica dell'azienda e l'accesso è consentito tramite l'utilizzo di credenziali di accesso fornite dall'accoglienza della struttura. L'utilizzo del servizio è regolato da una direttiva interna.

INTERNET

Il PC abilitato alla navigazione in Internet costituisce uno strumento necessario allo svolgimento della propria attività lavorativa. È pertanto vietato accedere a siti il cui contenuto non è riconducibile all'attività lavorativa. L'abilitazione alla

navigazione è assegnata a livello di utenza e deve essere autorizzata dal responsabile di struttura (o suo delegato) che invia opportuna richiesta alla struttura I.T.

È attivo un sistema di protezione della navigazione Internet che prevede il filtraggio automatico del traffico per categorie di contenuti ed è inoltre presente la funzionalità di gestione di specifiche blacklist di url.

È vietata la connessione alla rete Internet mediante l'autonoma installazione di modem, router o altri apparecchi di connettività.

Non è consentito scaricare o copiare (download/upload) di file o software di ogni genere da siti internet accedendo abusivamente ad un sistema informatico o telematico protetto da misure di sicurezza. Allo stesso modo non è consentita la permanenza in un sistema informatico o telematico, servizio applicativo in genere contro la volontà espressa o tacita dell'Azienda.

La Casa di Cura Villa Esther si cautela nei confronti di tali attività bloccando l'accesso a siti Internet non pertinenti l'attività lavorativa e comunque tracciando tutte le attività di navigazione effettuate all'interno dell'azienda stessa.

Ogni file (o software) eventualmente scaricato da Internet avviene sotto la responsabilità esclusiva di ciascun dipendente e deve essere necessariamente preceduto da una analisi volta a verificare l'eventuale presenza di virus; ciò a tutela dell'integrità del patrimonio aziendale. Qualora il singolo utilizzatore dipendente non sia in grado di procedere autonomamente e correttamente al predetto controllo, dovrà contattare la struttura I.T., prima di procedere a qualsiasi operazione che comporti il prelevamento di file da siti Internet.

Non è consentito l'utilizzo dei servizi di messaggistica istantanea -esclusi quelli espressamente autorizzati dall'azienda- programmi di condivisione file (file sharing) e di programmi P2P.

È rigorosamente vietata la registrazione e partecipazione a forum non professionali, l'utilizzo di chatline, di social network, di bacheche elettroniche (esclusi quelli espressamente autorizzati dall'azienda) le registrazioni in guest books anche utilizzando pseudonimi.

Non è consentita alcuna attività legata ad operazioni di hackeraggio e pirateria informatica in generale. È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo i casi direttamente autorizzati dai Responsabili e con il rispetto delle normali procedure d'acquisto.

INSTALLAZIONE SOFTWARE

L'installazione di software deve avvenire esclusivamente ad opera di soggetti provvisti di specifiche abilitazioni preventivamente autorizzati dalla struttura I.T. I software e gli applicativi installati sono parte del patrimonio aziendale e come tali devono essere utilizzati nel rispetto della presente policy e di eventuali indicazioni ricevute dalla struttura I.T.

Al fine di tutelare il sistema informatico -sussistendo il grave pericolo di introdurre codice malevolo e/o di alterare la funzionalità delle applicazioni software esistenti- è fatto divieto a chiunque utilizzi computer aziendali di scaricare dalla rete Internet (installare e/o eseguire) qualsiasi tipo di software non autorizzato.

Non è consentito l'utilizzo di software che consenta l'accesso alla postazione di lavoro - controllo remoto - o ai dati istituzionali al di fuori della rete aziendale (condivisione dati online), ad esclusione degli eventuali applicativi preventivamente forniti ed autorizzati dalla struttura I.T.

Al fine di tutelare l'integrità e la veridicità dei documenti informatici, è vietata la installazione e l'utilizzo di software (e hardware) atti ad intercettare, falsificare, alterare, impedire e interrompere comunicazioni (e/o il contenuto documenti informatici); è altresì vietata l'installazione di software che potrebbero rivelarsi lesivi del sistema informatico aziendale. Non è permesso l'utilizzo di programmi diversi da quelli ufficialmente installati dalla struttura I.T. Al fine di proteggere l'integrità dell'Azienda, il personale non può utilizzare software di proprietà personale, comprese applicazioni

regolarmente acquistate e registrate, programmi shareware e/o freeware, eventuale software scaricato da Internet o proveniente da CD/DVD allegati a riviste e/o giornali o altro software posseduto a qualsiasi titolo.

Non è consentita l'installazione, anche se necessaria, di eventuali driver per stampanti o altri supporti (come ad esempio masterizzatori, scanner, etc.); in questo caso l'utente dovrà richiedere ai tecnici della struttura I.T. di intervenire per effettuare l'installazione.

L'installazione volontaria sul personal computer in dotazione di componenti software in grado di danneggiare, deteriorare o rendere, in tutto o in parte, inservibile il sistema informatico o le informazioni in esso contenute, può costituire, tenuto conto della gravità del comportamento, condotta sanzionata penalmente ai sensi dell'art. 635-bis Cod. Pen.

Sono in uso particolari software volti a fornire, con cadenza programmata (attualmente, la pianificazione è settimanale) report specifici in merito ai software installati nelle postazioni di lavoro. Su tali report sono effettuate attività di analisi volte a rilevare la presenza di software non autorizzato. Gli aggiornamenti del sistema operativo sono necessari, oltre che per obbligo di legge, al fine di proteggere i PC e l'intera rete. È stato attivato il Windows Server Update Services (WSUS) che pianifica e dispone l'installazione degli aggiornamenti in modalità automatica.

È tassativamente vietato all'utente ogni sorta di aggiornamento manuale del software installato se non espressamente autorizzato dalla struttura I.T. Gli aggiornamenti del software e dei driver necessari al buon funzionamento della postazione di lavoro saranno effettuati direttamente dai tecnici della struttura I.T. configurando gli aggiornamenti automatici per ciò che attiene la protezione antivirus ed il sistema operativo, ed intervenendo dietro segnalazione dell'utente per ogni ulteriore update si dovesse rendere necessario.

ANTIMALWARE

Villa Esther utilizza il servizio Antivirus erogato da Microsoft e insito nel sistema operativo. La politica di sicurezza aziendale prevede l'installazione di un software anti malware (antivirus) su tutte le postazioni di lavoro (che lo supportano); esso viene aggiornato automaticamente grazie ad una gestione centralizzata per mezzo di un server dedicato. Sulle postazioni eventualmente off-line, tali aggiornamenti vengono installati non appena si ripresenteranno in linea, di norma, alla prima accensione. Tale modalità permette di elevare al massimo la protezione contro virus ed agenti esterni.

Non è ammesso l'utilizzo di sistemi antivirus diversi, se non espressamente autorizzato dalla struttura I.T.

È stata inoltre abilitata di default su tutti i client la modalità "Scan all files in removable storage devices after plugin" atta ad effettuare la scansione di tutte le periferiche rimovibili che vengono collegate. È inoltre attivo il blocco dell'esecuzione "autorun" che disinnesca l'esecuzione automatica di contenuti al momento della connessione dei dispositivi mobili.

Nel caso il software antivirus rilevi la presenza di un virus che non è riuscito a ripulire, l'utente dovrà immediatamente:

- sospendere ogni elaborazione in corso senza spegnere il computer;
- segnalare l'accaduto all'HelpDesk preposto secondo le vigenti disposizioni.

APPARECCHIATURE DI RIPRODUZIONE/REGISTRAZIONE IMMAGINI

È vietata l'esecuzione di riproduzione/registrazione di immagini, a qualsiasi titolo, con apparecchiature personali o di terzi, se non espressamente autorizzati dalla Direzione Aziendale.

Non è consentito l'utilizzo di sistemi di videoconferenza/audioconferenza se non preventivamente autorizzati dalla struttura I.T. - sussistendo il grave pericolo di introdurre codice malevolo e/o di alterare la funzionalità delle applicazioni software esistenti.

PIANO CONTINUITÀ OPERATIVA

PREMESSA

La Casa di Cura Villa Esther ha adottato il seguente Piano di Continuità Operativa documentato (BCP) integrandolo con una politica di Disaster Recovery (DR) che definisce i possibili disastri e gli scenari di rischio, individua i processi critici e le figure di riferimento, interne ed esterne alla Società, in caso di gravi problemi oltre che le modalità di risoluzione degli stessi.

RUOLI E RESPONSABILITÀ NEL RIPRISTINO DELLE INFORMAZIONI

Sono di seguito elencati gli attori coinvolti nel sistema di ripristino funzionalità e dati, con le relative responsabilità:

- **Erio Sala** in qualità di Amministratore di Sistema. Ha la responsabilità sulla gestione del Dominio di Accesso Windows Server, dei dati nelle cartelle utente (Home folder) e quelle condivise. Il soggetto si occupa anche del server reale dove risiedono i VPS che contengono l'applicativo madre di gestione del sistema sanitario e amministrativo (HIS): pur non avendo accesso ai dati (nella sola disponibilità della ditta fornitrice) ha la responsabilità di conservare i backup e il ripristino degli stessi in caso di necessità. Per conto della ditta NIOLAB, l'AdS ha il ruolo di gestore della rete e di tutti i dispositivi coinvolti: firewall, switch, hub, access point etc. È suo il compito di ripristino si queste funzionalità in caso di interruzioni dovute a scenari avversi.

- **GESAN s.r.l.** ha nella sua **esclusiva disponibilità** tutti i server e i dati in essi contenuti che costituiscono la struttura del sistema di gestione sanitaria e amministrativa della clinica Villa Esther. È questa ditta la responsabile della conservazione dei dati che attengono al loro applicativo WebHospital con annessi e connessi. GESAN ha la responsabilità sulla continuità di funzionamento dei propri software che in termini, solo indicativi e non esaustivi, riguardano sia la direzione **sanitaria** che **amministrativa** come: cartella clinica, refertazione, agende appuntamenti, la fatturazione, il CUP etc.

- **MEDIS ITALIA s.r.l.** è il gestore del sistema software **RIS/PACS** ossia di tutti quegli applicativi che riguardano la radiodiagnostica (TC, Ecografia, RX, etc.). Medis controlla l'insieme formato da server, workstation e dispositivi che garantiscono il funzionamento e l'accesso ai dati del servizio. Ha il compito di conservare e custodire i backup di tutte le immagini, video e informazioni che le competono ma anche dei risultati degli stessi come referti, dosaggi etc.

- **SCS Computer s.r.l.** è il gestore della struttura software **LIS** e come tale ha la responsabilità di tutto l'apparato che governa il laboratorio di analisi della casa di cura Villa Esther. Nella sua **esclusiva disponibilità** tutta i dati grezzi (e/o rifiniti) che provengono dai macchinari del laboratorio, di quelli elaborati dagli operatori, dei referti prodotti dal reparto e di tutto ciò riguarda questa branca di assistenza sanitaria. A loro è affiadata la conservazione supplementare e le copie di backup. In questa veste la SCS è l'unica che ha il potere e il dovere di analizzare eventi avversi e incidenti e prendere decisioni per assicurare la continuità del business.

POSSIBILI SCENARI DI CRISI E CLASSIFICAZIONE DEGLI INCIDENTI

La Casa di Cura Villa Esther ha ritenuto probabili le seguenti categorie di rischio e misure di prevenzione:

MINACCE FISICHE:	SICUREZZA FISICA
Incendio	rilevazione fumi antincendio estintori formazione del personale per addetti Antincendio
Allagamento	Rilevazione Allagamento Archivi posti in luoghi soprelevati
Furto e danneggiamento	Sistemi di allarme e locali presidiati Protocolli e procedure per l'accesso agli archivi
MINACCE LOGICHE:	SICUREZZA LOGICA
Attacchi informatici della rete	Sicurezza perimetrale: firewall, nat, ids, filtering, vlan, proxy.
Virus e Malware	Sicurezza end-point: Antivirus, aggiornamento dei sistemi operativi autenticazione e autorizzazione dell'incaricato Blocco automatico delle postazioni di lavoro in caso di inattività Filtri alla navigazione internet e antispam
Accesso non autorizzato ad applicazioni e dati	Impostazioni Client - Server Controllo accesso a dati Sistemi di controllo e monitoraggio degli accessi
Indisponibilità dei dati	Salvataggi periodici dei dati Definizione di protocolli per assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi