

ALLEGATO A1)

ATTO DI NOMINA A RESPONSABILE DEL TRATTAMENTO DATI AI SENSI DELL'ART. 28 DEL REGOLAMENTO UE 2016/679

TRA

La Casa di Cura Villa Fiorita srl, di seguito “Struttura”, partita IVA/codice fiscale n., con sede legale in Prato, Via..... n....., nella persona del Dr. nato a il, in qualità di Legale Rappresentante/Amministratore Delegato domiciliato per la carica presso la Casa di Cura stessa, di seguito anche “Titolare”

E

l'Azienda USL Toscana Centro, in persona del Dr. Direttore SOC Anatomia Patologica Empoli e Prato – P.O. Santo Stefano Prato e P.O San Giuseppe di Empoli -, codice fiscale.....domiciliato per la carica presso la sede dell'Azienda sita in Firenze P.zza S.Maria Nuova, 1 50122 (FI), Partita IVA/codice fiscale 06593810481, di seguito anche “Responsabile”, congiuntamente indicate anche come le “Parti”

Premesso che:

- l'art. 28 del Regolamento UE n. 2016/679 (General Data Protection Regulation), di seguito “GDPR”, riconosce al Titolare del trattamento la facoltà di avvalersi di uno o più Responsabili del Trattamento dei dati - in possesso di esperienza, capacità, conoscenza tali da mettere in atto misure tecniche e organizzative idonee a soddisfare i requisiti del GDPR - previa stipula di un contratto o altro atto giuridico che determini la materia del trattamento, la durata, la natura e la finalità, il tipo di dati personali trattati e le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento;
- la Casa di Cura Villa Fiorita srl e l'Azienda Usl Toscana Centro hanno sottoscritto con Delibera n.del un contratto avente ad oggetto “Approvazione Schema di Convenzione da sottoscrivere con Casa di Cura Villa Fiorita di Prato per fornitura dietro pagamento di corrispettivo di prestazioni sanitarie di Anatomia Patologica – Branca K-, periodo dalla data di apposizione dell'ultima firma in formato digitale e fino al 31/12/2021”, di seguito Convenzione;
- ai fini del rispetto della normativa, ciascuna persona che tratta dati personali deve essere autorizzata e istruita in merito agli obblighi normativi per la gestione dei suddetti dati durante lo svolgimento delle proprie attività;
- tenuto conto delle attività di trattamento necessarie e/o opportune per dare esecuzione agli obblighi concordati tra le Parti, previa valutazione di quanto imposto

dal Regolamento UE n. 2016/679, il Titolare ha ritenuto che il Responsabile presenti garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate a soddisfare i requisiti del GDPR ed a garantire la tutela dei diritti e le libertà degli interessati coinvolti nelle suddette attività di trattamento;

Tutto quanto sopra premesso

La Struttura, in qualità di Titolare del Trattamento, con la presente

NOMINA

l'Azienda USL Toscana Centro RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI ai sensi dell'art. 28 del GDPR, per il trattamento dei dati personali di cui è Titolare la Struttura e di cui il Responsabile può venire a conoscenza nell'esercizio delle attività espletate per conto del Titolare.

Articolo 1 - Natura e finalità del trattamento

Il trattamento dei dati personali è effettuato esclusivamente per la corretta esecuzione delle attività concordate tra le Parti, di cui alla citata Convenzione e precisamente fornitura di esami e prestazioni sanitarie di Medicina di Laboratorio in regime di urgenza a favore di utenti afferenti alla Casa di Cura

Articolo 2 - Categorie di dati personali trattati

Il Responsabile del trattamento per espletare le attività pattuite tra le Parti per conto del Titolare tratta direttamente o anche solo indirettamente le seguenti categorie di dati:

- Anagrafici
- (particolari) sensibili.

Articolo 3 - Categorie di interessati cui si riferiscono i dati trattati

Per effetto della presente nomina le categorie di interessati, i cui dati personali possono essere trattati, sono:

- pazienti / utenti
- familiari dei pazienti / utenti
- dipendenti e collaboratori.

Articolo 4 - Obbligo alla riservatezza

Il Responsabile e i soggetti dal medesimo autorizzati al trattamento dei dati devono garantire assoluta riservatezza, sicurezza d'accesso e integrità dei dati trattati, avendo cura di adottare preventivamente misure tecniche ed organizzative adeguate a evitare ogni rischio per i diritti e le libertà degli interessati.

Il Responsabile e i soggetti autorizzati al trattamento sono tenuti all'obbligo di riservatezza e del segreto professionale nonché del segreto d'ufficio e sono comunque tenuti ad evitare l'eventuale comunicazione e/o conoscenza dei dati

trattati da parte di soggetti non autorizzati, secondo le prescrizioni del GDPR e del D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018.

Articolo 5 – Disponibilità e uso dei dati

Qualunque sia la finalità e la durata del trattamento effettuato da parte del Responsabile:

- il trattamento dei dati può consistere nelle sole operazioni strettamente inerenti all'oggetto della Convenzione e funzionali alla realizzazione e gestione delle attività affidate dal Titolare al Responsabile, secondo quanto previsto dal GDPR; salvo specifici ed ulteriori accordi tra le parti in relazione a determinati trattamenti.
- i dati non potranno essere ceduti, in tutto o in parte, ad altri soggetti e dovranno essere restituiti alla conclusione dell'incarico o in qualsiasi momento il Titolare ne faccia richiesta;
- il Responsabile si impegna a non vantare alcun diritto sui dati e sui materiali presi in visione.

Coerentemente con quanto prescritto dal GDPR, è fatto divieto al Responsabile –di contattare gli interessati per finalità diverse da quelle previste nella Convenzione stipulata dalle Parti. salvo specifici ed ulteriori accordi tra le parti in relazione a determinati trattamenti.

Articolo 6 - Cessazione del trattamento

Una volta cessati i trattamenti oggetto del Contratto, salvo rinnovo, il Responsabile si impegna a restituire al Titolare i dati personali acquisiti, pervenuti a sua conoscenza o da questi elaborati in relazione all'esecuzione del servizio prestato e, solo successivamente, si impegna a cancellarli dai propri archivi oppure a distruggerli, ad eccezione dei casi in cui i dati debbano essere conservati in virtù di obblighi di legge. Resta inteso che la dimostrazione delle ragioni che giustificano il protrarsi degli obblighi di conservazione è a carico del Titolare e che le uniche finalità perseguibili con tali dati sono esclusivamente circoscritte a rispondere a tali adempimenti normativi.

Articolo 7 - Validità e Revoca della nomina

La presente nomina avrà validità per tutta la durata del rapporto giuridico intercorrente tra le Parti e potrà essere revocata a discrezione del Titolare.

La presente nomina non costituisce aggravio in capo al Responsabile, rientrando la medesima negli obblighi normativi che regolano i rapporti con il Titolare sotto il profilo della protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Articolo 8 - Sub-Responsabili

Per l'espletamento di specifiche attività di trattamento oggetto della Convenzione, il Responsabile del trattamento potrà avvalersi di altri Responsabili, valendo la presente quale autorizzazione generale ai sensi dell'art. 28, par.2, del GDPR, a tal fine è tenuto a trasmettere al Titolare l'elenco aggiornato dei soggetti designati quali Sub-Responsabili, informandolo preventivamente in caso di eventuali modifiche inerenti all'aggiunta o la sostituzione di tali soggetti.

Ai sensi dell'art. 28, par. 4, del GDPR, il Responsabile è tenuto ad acquisire dai Sub-Responsabili l'impegno scritto a trattare i dati nel rispetto degli stessi obblighi ai quali è vincolata l'Azienda in virtù del presente Atto di Nomina a Responsabile del Trattamento.

L'Azienda risponde dinanzi al Titolare dell'eventuale inadempimento dei Sub-Responsabili, fatta salva la facoltà di dimostrare che l'evento dannoso, conseguente all'inadempimento, non è in alcun modo imputabile al Responsabile, ai sensi dell'art. 82, par. 1 e par. 3 del GDPR.

Articolo 9 - Designazione e autorizzazione degli incaricati

Il Responsabile del trattamento garantisce la puntuale individuazione dei soggetti operanti a qualsiasi titolo nella propria organizzazione quali soggetti autorizzati al trattamento.

In particolare il Responsabile del trattamento si impegna a consentire l'accesso e il trattamento dei dati personali solo a personale debitamente formato e specificamente designato, anche ai sensi dell'art. 2-quaterdecies del D.Lgs 196/2003 e s.m.i.

Nello specifico il Responsabile:

- individua le persone autorizzate al trattamento dei dati, impartendo loro, per iscritto, istruzioni dettagliate in merito alle operazioni consentite e alle misure di sicurezza da adottare in relazione alle criticità dei dati trattati;
- vigila regolarmente sulla puntuale applicazione da parte dei soggetti autorizzati di quanto prescritto, anche tramite verifiche periodiche;
- garantisce l'adozione dei diversi profili di autorizzazione dei soggetti incaricati, in modo da limitare l'accesso ai soli dati necessari alle operazioni di trattamento consentite rispetto alle mansioni svolte;
- verifica periodicamente la sussistenza delle condizioni per la conservazione dei profili di autorizzazione dei soggetti incaricati, modificando tempestivamente detto profilo ove necessario (es. cambio di mansione);
- cura la formazione e l'aggiornamento professionale delle persone autorizzate che operano sotto la sua responsabilità circa le disposizioni normative vigenti in materia di tutela dei dati personali.

Articolo 10 – Responsabile della protezione dei Dati

Ai sensi dell'art. 37 del GDPR, il Responsabile si impegna a comunicare al Titolare il nominativo e i dati di contatto del Responsabile della Protezione dei Dati.

Articolo 11 - Diritti degli interessati

Premesso che l'esercizio dei diritti riconosciuti all'interessato ai sensi degli artt. 15 e seguenti del GDPR sarà gestito direttamente dal Titolare, il Responsabile si rende disponibile a collaborare con il Titolare stesso, fornendogli tutte le informazioni necessarie a soddisfare le eventuali richieste ricevute in tal senso.

Il Responsabile si impegna ad assistere il Titolare con misure tecniche e organizzative adeguate al fine di soddisfare l'obbligo del Titolare di dare seguito alle richieste per l'esercizio dei diritti dell'interessato.

In particolare, il Responsabile dovrà comunicare al Titolare, senza ritardo e comunque non oltre cinque giorni lavorativi dalla ricezione, le istanze eventualmente ricevute e avanzate dagli interessati in virtù dei diritti previsti dalla vigente normativa (es. diritto di accesso, ecc.) e a fornire le informazioni necessarie al fine di consentire al Titolare di evadere le stesse entro i termini stabiliti dalla normativa.

Articolo 12 - Registro dei trattamenti

Il Responsabile tiene un registro di tutte le attività di trattamento dei dati svolte per conto del Titolare, ai sensi dell'art. 30, paragrafi 2 e 3, del GDPR

Il Responsabile si impegna a mettere a disposizione del Titolare e/o dell'Autorità Garante, su esplicita richiesta, il suddetto registro dei trattamenti.

Articolo 13 - Sicurezza dei dati personali

Il Responsabile è tenuto, ai sensi dell'art. 32 del GDPR, ad adottare le necessarie e adeguate misure di sicurezza, in modo tale da ridurre al minimo i rischi di distruzione accidentale o illegale, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non consentito ai dati personali trasmessi, conservati o comunque trattati, o il trattamento non conforme alle finalità della raccolta.

Articolo 14 - Sicurezza e Amministrazione del Sistema (ADS)

Il Responsabile fornisce, su richiesta, al Titolare, la lista nominativa degli ADS, con questi intendendo le persone fisiche che svolgono per conto del Responsabile ed in esecuzione dei compiti concordati ed affidati dal Titolare, attività di gestione e manutenzione di impianti di elaborazione con cui vengono effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i software complessi che trattano dati del Titolare, le reti locali e gli apparati di sicurezza di quest'ultimo, o comunque che possano intervenire sulle misure di sicurezza a presidio dei medesimi dati.

Articolo 15 - Modalità di trattamento

Il Responsabile si impegna:

- a trattare - tramite i propri dipendenti, collaboratori esterni, consulenti, specificamente designati incaricati del trattamento - i dati per le finalità connesse allo svolgimento delle attività demandate dal Titolare al Responsabile nell'ambito della Convenzione, in modo lecito e secondo correttezza, nel pieno rispetto delle disposizioni previste dal GDPR, nonché dalle seguenti istruzioni:
- non divulgare o rendere noti a terzi - per alcuna ragione ed in alcun momento, presente o futuro ed anche una volta cessati i trattamenti oggetto della Convenzione - i dati personali ricevuti dal Titolare o pervenuti a sua conoscenza in relazione all'esecuzione del servizio prestato, se non previamente autorizzato per iscritto dal Titolare, fatti salvi eventuali obblighi di legge o ordini dell'Autorità Giudiziaria
- collaborare con il Titolare per garantire la puntuale osservanza e conformità alla normativa in materia di protezione dei dati personali;
- dare immediato avviso al Titolare in caso di cessazione dei trattamenti concordati;
- in caso di ricezione di richieste specifiche avanzate dall'Autorità Garante per la protezione dei dati personali o altre autorità, a coadiuvare il Titolare per quanto di sua competenza;
- segnalare eventuali criticità al Titolare che possono mettere a repentaglio la sicurezza dei dati, al fine di consentire idonei interventi da parte dello stesso;

Articolo 16 – Violazione dei dati

Il Responsabile si impegna a notificare al Titolare, senza ingiustificato ritardo dall'avvenuta conoscenza, e comunque entro 72 ore - con comunicazione da inviarsi all'indirizzo PEC del titolare - ogni violazione dei dati personali (*data breach*), fornendo altresì:

- la descrizione della natura della violazione, l'indicazione delle categorie dei dati personali e il numero approssimativo di interessati coinvolti;
- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- la descrizione delle probabili conseguenze;
- la descrizione delle misure adottate o di cui dispone per porre rimedio alla violazione o, quantomeno, per attenuarne i possibili effetti negativi.

Fermo quanto sopra previsto, il Responsabile si impegna a prestare ogni più ampia assistenza al Titolare, al fine di consentirgli di assolvere agli obblighi di cui agli artt. 33 - 34 del GDPR.

Una volta definite le ragioni della violazione, il Responsabile di concerto con il Titolare e/o altro soggetto da quest'ultimo indicato, su richiesta, si attiverà per implementare nel minor tempo possibile tutte le misure di sicurezza fisiche e/o logiche e/o organizzative atte ad arginare il verificarsi di una nuova violazione della stessa specie di quella verificatasi, al riguardo anche avvalendosi dell'operato di subfornitori.

Articolo 17 - Valutazione di impatto e consultazione preventiva

Con riferimento agli artt. 35 e 36 del GDPR, il Responsabile si impegna, su richiesta, ad assistere il Titolare nelle attività necessarie all'assolvimento degli obblighi previsti dai succitati articoli, sulle base delle informazioni in proprio possesso, in ragione dei trattamenti svolti in qualità di Responsabile del trattamento, ivi incluse le informazioni relative agli eventuali trattamenti effettuati dai Sub - Responsabili.

Articolo 18 - Trasferimento dei dati personali

Il Responsabile del trattamento si impegna a circoscrivere gli ambiti di circolazione e trattamento dei dati personali (es. memorizzazione, archiviazione, conservazione dei dati sui propri server) ai Paesi facenti parte dell'Unione Europea, con espresso divieto di trasferirli in Paesi extra UE che non garantiscano (o in assenza di) un livello adeguato di tutela, ovvero, in assenza di strumenti di tutela previsti dal Regolamento UE 2016/679 CAPO V.

Articolo 19 - Attività di audit

Il Responsabile si impegna a mettere a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di sicurezza descritti nel presente documento e, in generale, il rispetto delle obbligazioni assunte in forza del presente atto e del GDPR, consentendo e, su richiesta, contribuendo alle attività di audit, comprese le ispezioni, realizzate dal Titolare o da altro soggetto da esso incaricato.

Articolo 20 - Ulteriori istruzioni

Il Responsabile informa prontamente il Titolare delle eventuali carenze, situazioni anomale o di emergenza rilevate nell'ambito del servizio erogato - in particolare ove ciò possa riguardare il trattamento dei dati personali e le misure di sicurezza adottate dal Responsabile - e di ogni altro episodio o fatto rilevante che intervenga e che riguardi comunque l'applicazione del GDPR (ad es. richieste del Garante, esito delle ispezioni svolte dalle Autorità, ecc.) o della normativa nazionale ancorchè applicabile.

Articolo 21 - Norme finali e responsabilità

Il Responsabile dichiara sin d'ora di mantenere indenne e manlevato il Titolare da qualsiasi danno, onere, spesa e conseguenza che dovesse derivare al Titolare stesso a seguito della violazione, da parte del Responsabile o di suoi Sub - Responsabili, degli

impegni relativi al rispetto della disciplina in materia di protezione dei dati personali o delle istruzioni contenute nei relativi atti di nomina, anche in seguito a comportamenti addebitabili ai loro dipendenti, rappresentanti, collaboratori a qualsiasi titolo.

Prato, li _____

Il titolare del trattamento dei dati

p. La Casa di Cura Villa Fiorita srl

il Legale Rappresentante / Amministratore Delegato,

Dr.

(data e firma in formato digitale)

Il responsabile del trattamento dei dati

p. Azienda USL Toscana Centro il Direttore SOC Anatomia Patologica Empoli e

Prato

Dr.-

(data e firma in formato digitale)

Azienda USL Toscana centro



Azienda USL Toscana Centro
P.zza Santa Maria Nuova 1
50122 Firenze
C.F./P.IVA 06593810481