

ACCORDO SUL TRATTAMENTO DEI DATI AI SENSI E PER GLI EFFETTI DELL'ART. 28 DEL REGOLAMENTO EUROPEO 27 APRILE 2016, N.679 ("GDPR")

Fondazione Teresa Camplani - in persona del Direttore Generale pro-tempore, in qualità di Titolare del trattamento dati, ai sensi dell'art. 4 del Regolamento UE 2016/679 (GDPR),

e

ASST CARLO POMA DI MANTOVA – in persona del Direttore Generale pro-tempore

PREMESSO CHE:

- a. con contratto stipulato tra le Parti (di seguito anche il "Contratto") **Fondazione Teresa Camplani** (di seguito "Titolare del trattamento" oppure "Titolare") ha affidato a **ASST CARLO POMA DI MANTOVA** l'erogazione in suo favore di servizi di PRESTAZIONI SANITARIE;
- b. ai sensi della vigente normativa europea ed italiana in materia di protezione dei dati personali, l'esecuzione dei Servizi comporta il Trattamento di Dati Personali da parte del Fornitore;
- c. il Regolamento (UE) 2016/679, relativo alla protezione delle persone fisiche con riguardo al Trattamento dei Dati Personali, nonché alla libera circolazione di tali dati (General Data Protection Regulation) prescrive all'art. 28 che i trattamenti da parte dei Responsabili del trattamento siano disciplinati mediante un atto giuridico a norma del diritto dell'Unione Europea, che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento;
- d. a mezzo del presente Accordo, le Parti intendono disciplinare il Trattamento dei Dati Personali effettuato dal Fornitore nell'esecuzione dei Servizi di cui al Contratto, ai sensi della Normativa Applicabile sulla protezione dei dati personali;

tanto premesso, costituendo le premesse e gli Allegati parte integrante e sostanziale del presente Accordo,

CONVENGONO E STIPULANO QUANTO SEGUE

1. OGGETTO

Con il presente Accordo, il Titolare affida al Fornitore, identificato come Responsabile del trattamento dei Dati Personali ai sensi dell'art. 28 del GDPR (di seguito "Responsabile del Trattamento" oppure "Responsabile"), tutte le operazioni di trattamento dei dati descritte all'Allegato A del presente Accordo che si rendano necessarie per adempiere ai compiti assegnati in esecuzione del Contratto citato in Premessa, esclusivamente per le finalità e per la durata ivi indicate e in ottemperanza alle istruzioni impartite dallo stesso Titolare.

2. OBBLIGHI DEL RESPONSABILE

La sottoscrizione del presente Accordo vincola il Responsabile del trattamento al Titolare del trattamento e fa sorgere in capo al Responsabile una serie di obblighi, specificamente individuati nell'Allegato B al presente Accordo.

3. MISURE DI SICUREZZA

Il Responsabile conferma di presentare garanzie sufficienti in termini di sicurezza del Trattamento ai sensi dell'articolo 32 del GDPR, impegnandosi, più precisamente, ad adottare e mantenere per l'intera durata del Contratto, misure di sicurezza tecniche fisiche e organizzative adeguate per preservare la sicurezza dei Dati del Titolare e proteggerli da qualsiasi distorsione, alterazione, distruzione accidentale o illecita, danno, perdita, divulgazione o accesso da parte di terzi non autorizzati, tenendo conto della natura del Trattamento e delle informazioni a disposizione dello stesso Responsabile del Trattamento, nonché delle documentate istruzioni impartite dal Titolare in relazione all'adempimento dei suddetti obblighi. Il Responsabile applicherà tali misure di sicurezza al fine di garantire:

- a. se del caso, la pseudonimizzazione e la cifratura dei dati personali;
- b. la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- c. la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- d. la possibilità di testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Il Responsabile adotta inoltre le necessarie misure di sicurezza organizzative e concede l'accesso ai dati personali oggetto di trattamento ai membri del suo personale soltanto nella misura strettamente necessaria per l'attuazione, la gestione e il controllo del contratto. Il Responsabile garantisce, come precisato nell'Allegato B, che le persone autorizzate al trattamento dei dati personali ricevuti si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

I dettagli delle misure di sicurezza adottate saranno resi disponibili al cliente, a fronte di richiesta, e informando immediatamente il Titolare in caso di eventuali modifiche, che possono essere apportate unicamente in favore di misure con un livello di sicurezza uguale o superiore.

Nel valutare l'adeguato livello di sicurezza, le parti tengono debitamente conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi per gli interessati.

4. MODIFICA

Le parti si impegnano a comunicarsi reciprocamente qualsiasi informazione relativa a modifiche necessarie nelle operazioni di trattamento dei dati, ed il Titolare si impegna a fornire al Responsabile le eventuali istruzioni aggiuntive riguardanti il trattamento. Nel corso dell'esecuzione del Contratto, il Titolare dispone le opportune modifiche od integrazioni dei trattamenti oggetto del presente Accordo, descritti all'Allegato A., dandone opportuna comunicazione al Responsabile. L'inserimento di trattamenti che, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possono presentare un rischio elevato

ACCORDO SUL TRATTAMENTO DEI DATI AI SENSI E PER GLI EFFETTI DELL'ART. 28 DEL REGOLAMENTO EUROPEO 27 APRILE 2016, N.679 ("GDPR")

per i diritti e le libertà delle persone fisiche, in particolare ove prevedano l'uso di nuove tecnologie, è sempre preceduto da una valutazione d'impatto effettuata a cura del Titolare con la piena collaborazione del Responsabile.

Eventuali modifiche al presente Accordo, che dovessero rendersi necessarie anche alla luce di future modifiche normative, dovranno essere apportate per iscritto con l'accordo delle Parti.

5. DECORRENZA – DURATA - CESSAZIONE DEL TRATTAMENTO

Il ruolo e le competenze assegnate al Responsabile del trattamento con il presente atto hanno la medesima durata ed efficacia del Contratto intercorrente tra le Parti e pertanto si intendono tacitamente rinnovate ogni anno fino alla cessazione del Contratto stesso o fino alla revoca da parte del Titolare.

Resta fermo, anche successivamente alla cessazione del Contratto, l'obbligo del Responsabile di mantenere la massima riservatezza sui dati e le informazioni relative al Titolare delle quali sia venuto a conoscenza nell'adempimento delle sue obbligazioni.

6. RESTITUZIONE E CANCELLAZIONE DEI DATI PERSONALI

Il Responsabile, all'atto della scadenza del Contratto e/o dei Servizi o, comunque, in caso di cessazione – per qualunque causa – dell'efficacia del presente atto di designazione, salvo la sussistenza di un obbligo di legge o di regolamento nazionale e/o comunitario che preveda la conservazione dei Dati Personali, dovrà interrompere ogni operazione di trattamento degli stessi e dovrà provvedere, a scelta del Titolare, all'immediata restituzione allo stesso dei Dati Personali oppure alla loro integrale cancellazione, in entrambi i casi rilasciando contestualmente un'attestazione scritta che presso lo stesso Responsabile non ne esiste alcuna copia.

In caso di richiesta scritta del Titolare, il Responsabile è tenuto a indicare le modalità tecniche e le procedure utilizzate per la cancellazione/distruzione.

7. DISPOSIZIONI FINALI

Resta inteso che la presente designazione non comporta alcun diritto per il Responsabile ad uno specifico compenso o indennità o rimborso per l'attività svolta, né ad un incremento del compenso spettante allo stesso in virtù del Contratto con la Società.

Per tutto quanto non previsto dal presente Accordo si rinvia alle disposizioni generali vigenti ed applicabili in materia protezione dei dati personali ed in particolare al regolamento (UE) 2016/679, alla luce del quale il presente Accordo deve essere interpretato.

Qualora le clausole del presente Accordo siano giudicate, con provvedimento esecutivo, nulle o inapplicabili, le restanti clausole restano vigenti.

Il presente Accordo è soggetto alla Legge italiana. Per ogni controversia il foro competente è quello della sede legale del Titolare.

Il Titolare del Trattamento

Fondazione Teresa Camplani

Il Direttore Generale pro tempore

ACCETTAZIONE NOMINA

Il sottoscritto Direttore Generale pro tempore di ASST CARLO POMA DI MANTOVA accetta la presente nomina nei contenuti, limiti, obblighi ed istruzioni in essa indicati.

Firma

ACCORDO SUL TRATTAMENTO DEI DATI AI SENSI E PER GLI EFFETTI DELL'ART. 28 DEL REGOLAMENTO EUROPEO 27 APRILE 2016, N.679 ("GDPR")

ALLEGATO A.

DESCRIZIONE DEI TRATTAMENTI DI DATI PERSONALI

EFFETTUATI DAL RESPONSABILE PER CONTO DEL TITOLARE IN ESECUZIONE DEL CONTRATTO DI SERVIZI IN ESSERE TRA LE PARTI

1. Trattamento dati personali

Descrizione e finalità del trattamento	Tipologia (Comuni/ Particolari)	Categorie di interessati	Base giuridica	Periodo di conservazione
Trattamento dati personali dei pazienti per erogazione delle prestazioni sanitarie oggetto del Contratto	Dati personali Comuni e Particolari necessari all'erogazione delle prestazioni	Pazienti Utenti	Obbligo legale e contrattuale; consenso informato al trattamento, ove previsto; Art. 9, par. 2, let. h) Reg. (UE) 2016/679.	Secondo quanto previsto dal Titolare e Massimario del Sistema Sociosanitario lombardo già Sistema Sanitario e Sociosanitario di Regione Lombardia
Trattamento dati identificativi e di contatto di dipendenti e collaboratori per esecuzione contratto, gestione del servizio sanitario	Dati personali comuni	Dipendenti, collaboratori	Obbligo legale e contrattuale	Secondo quanto previsto dal Titolare e Massimario del Sistema Sociosanitario lombardo già Sistema Sanitario e Sociosanitario di Regione Lombardia

**ACCORDO SUL TRATTAMENTO DEI DATI AI SENSI E PER GLI EFFETTI DELL'ART. 28 DEL REGOLAMENTO
EUROPEO 27 APRILE 2016, N.679 ("GDPR")**

ALLEGATO B.

OBBLIGHI DEL RESPONSABILE

1. **Rispetto delle istruzioni impartite dal/i Titolare/i:** Il Responsabile deve assistere e coadiuvare il Titolare nella corretta gestione delle operazioni di trattamento che dovranno esser effettuate nel pieno rispetto degli obblighi previsti dal GDPR. A tale proposito, il Responsabile deve 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 tal caso, il Responsabile deve informare il Titolare circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico.
2. **Esattezza e minimizzazione dei dati:** Se il Responsabile viene a conoscenza del fatto che i dati personali che ha ricevuto sono inesatti o obsoleti, ne informa senza ingiustificato ritardo il Titolare. In tal caso, il Responsabile coopera con il Titolare per cancellarli o rettificarli.
3. **Riservatezza:** Il Responsabile deve assicurare per sé stesso e per le persone, da lui o dal Titolare del trattamento autorizzate al trattamento dei dati personali, piena riservatezza rispetto alle operazioni di trattamento effettuate. Sarà cura del Responsabile, qualora lo reputasse opportuno, vincolare le persone autorizzate al trattamento dei dati al segreto mediante un adeguato obbligo legale di riservatezza, anche per il periodo successivo all'estinzione del rapporto di lavoro intrattenuto con il Responsabile, in relazione alle operazioni di Trattamento da essi eseguite.
4. **Conformità a leggi e regolamenti applicabili:** Il Responsabile è tenuto ad uniformarsi alle disposizioni del GDPR e più in generale, di ogni altra disposizione normativa, nazionale e sovranazionale, in materia di trattamento dei dati personali attualmente in vigore o che in futuro vengano a modificare, integrare o sostituire l'attuale disciplina, nonché dei provvedimenti dell'Autorità Garante competente e delle linee guida adottate dall'European Data Protection Board.
5. **Misure di sicurezza:** Il Responsabile è tenuto a mettere in atto le misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio in merito al trattamento dei dati effettuato (art. 32 GDPR) descritte nel dettaglio all'articolo 3 dell'Accordo sul trattamento dei dati sottoscritto con il Titolare.
6. **Audit:** Il Responsabile del trattamento si impegna a riferire al Titolare, ogni volta che riceve specifica richiesta in tal senso, sui dettagli relativi all'adempimento di quanto disposto dal presente contratto nonché dalla normativa privacy, o attraverso relazioni scritte o attraverso compilazione di check list che verranno fornite. Tale verifica da parte del Titolare potrà avvenire sottoforma di *audit* e/o richieste di informazioni/controlli i cui eventuali costi saranno sostenuti dal Titolare
7. Inoltre, il Responsabile deve contribuire alle attività di revisione, comprese le ispezioni, e ad informare prontamente il Titolare del trattamento di ogni questione rilevante ai fini del presente mandato, quali a titolo indicativo:
 - a. Istanze di interessati;
 - b. Richieste del Garante;
 - c. Esiti delle ispezioni;
 - d. Violazioni del GDPR o di altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati, o la messa in pericolo della riservatezza, della completezza o dell'integrità dei dati personali, come meglio indicato al punto 14 del presente Allegato.
8. **Persone autorizzate al trattamento:** Il Responsabile si avvale di persone autorizzate al trattamento dei dati che operano sotto la sua responsabilità, in quanto deputati alle operazioni di Trattamento, e alle quali fornisce specifiche istruzioni scritte (salvo che il diritto dell'Unione o degli Stati membri non richieda diversamente, art. 29 GDPR). È compito del Responsabile designato vigilare sulla corretta esecuzione delle istruzioni impartite (art. 4.10 GDPR).
9. **Subresponsabile:** Il Titolare del trattamento autorizza il Responsabile del trattamento, individuato con il presente atto, a ricorrere ad un altro Responsabile (di seguito "Subresponsabile") per l'esecuzione di specifiche attività di trattamento. Il Responsabile inoltra al Titolare l'atto di nomina del "Subresponsabile" e lo informa di eventuali modifiche riguardanti l'aggiunta o la sostituzione di altri Responsabili, alle quali il Titolare del trattamento conserva il diritto di opporsi. Al "Subresponsabile" sono imposti, con specifico atto sottoscritto, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto che lega il Titolare e il Responsabile del trattamento. Il "Subresponsabile" è tenuto ad osservare, valutare e organizzare la gestione del trattamento dei dati personali e la loro protezione (mettendo in atto tutte le misure tecniche ed organizzative adeguate ad assicurare un livello di sicurezza adeguato al rischio derivante dal trattamento dati effettuato) affinché questi siano trattati in modo lecito e pertinente e nel rispetto della normativa vigente. Qualora il "Subresponsabile" del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi del "Subresponsabile" anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso "non gli è in alcun modo imputabile" (art. 82. 1 e 82. 3 GDPR).
10. **Trasferimenti internazionali:** Il Responsabile non comunica i dati personali a terzi situati al di fuori dell'Unione europea (nel suo stesso paese o in un altro paese terzo - di seguito: «trasferimento successivo»), a meno che il terzo sia o accetti di essere vincolato dalle presenti clausole, secondo il modulo appropriato. i) il trasferimento successivo è diretto verso un paese che beneficia di una decisione di adeguatezza in conformità dell'articolo 45 del regolamento (UE) 2016/679 che copre il trasferimento successivo; ii) il terzo fornisce in altro modo garanzie adeguate in conformità dell'articolo 46 o 47 del regolamento (UE) 2016/679 in relazione al trattamento in questione; iii) il trasferimento successivo è necessario per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria nell'ambito di specifici procedimenti amministrativi, regolamentari o giudiziari; o iv) il trasferimento successivo è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica. Qualunque trasferimento successivo è soggetto al rispetto da parte dell'importatore di tutte le altre garanzie previste dalle presenti clausole, in particolare la limitazione delle finalità.
11. **Registro dei Trattamenti:** Ove applicabile, il Responsabile deve tenere un Registro delle attività di trattamento svolte sotto la propria responsabilità in nome e per conto del Titolare del trattamento (art. 30 GDPR). Il Registro, anche in formato elettronico, deve contenere tutta una serie di informazioni, che il Responsabile raccoglie anche interfacciandosi con i vari uffici o unità interne e/o esterne all'azienda, che trattano dati personali per conto del Titolare.

In particolare:

 - a. il nome e i dati di contatto del Responsabile del trattamento;
 - b. le categorie dei trattamenti effettuati per conto di ogni Titolare;

ACCORDO SUL TRATTAMENTO DEI DATI AI SENSI E PER GLI EFFETTI DELL'ART. 28 DEL REGOLAMENTO EUROPEO 27 APRILE 2016, N.679 ("GDPR")

- c. i trasferimenti di dati personali verso un Paese terzo o un'organizzazione internazionale;
- d. una descrizione delle misure tecniche adottate.

Il Responsabile del trattamento deve mettere il Registro a disposizione dell'Autorità di controllo, se questa ne fa richiesta, affinché possa fungere da strumento per il monitoraggio dei trattamenti effettuati (Considerando 82 GDPR).

- 12. Valutazione d'impatto (cd. "data protection impact assessment"):** Il Responsabile, ai sensi dell'art. 28.3, lett. f), s'impegna fin da ora, tenuto conto della natura del trattamento e delle informazioni a disposizione del Fornitore, a fornire al Titolare ogni elemento utile all'effettuazione, da parte di quest'ultimo, della valutazione di impatto sulla protezione dei dati, qualora il Titolare sia tenuto ad effettuarla ai sensi dell'art. 35 del Regolamento, nonché ogni collaborazione nell'effettuazione della eventuale consultazione preventiva al Garante da parte di quest'ultimo ai sensi dell'art. 36 del Regolamento stesso.
- 13. Esercizio dei diritti dell'interessato:** Il Responsabile, dovrà informare tempestivamente e per iscritto il Titolare del trattamento, della ricezione di eventuali richieste degli interessati, avanzate ai sensi degli artt. da 15 a 22 del GDPR, in merito, tra l'altro, alle finalità e alle modalità del trattamento, all'origine dei dati, all'aggiornamento, alla rettificazione, cancellazione, alla portabilità e limitazione dei dati od opposizione al trattamento (compresa la profilazione), o al fine di revocare il consenso prestato e/o proporre reclamo al Garante per la protezione dei dati personali.
- In particolare, il Responsabile è tenuto a:
- a. coordinarsi a tal fine con le funzioni aziendali preposte dal Titolare alle relazioni con i soggetti interessati;
 - b. darne tempestiva comunicazione scritta al Titolare allegando copia della richiesta;
 - c. accertare l'identità del richiedente per verificare la legittimità della richiesta;
 - d. attivare le dovute procedure atte a dare seguito alle richieste per l'esercizio dei diritti degli interessati, senza ingiustificato ritardo, e comunque, al più tardi entro un mese dal ricevimento delle richieste stesse, ai sensi dell'art. 12 GDPR.
- 14. Violazioni di dati personali (cd. "data breach"):** Il Responsabile si impegna ad informare, senza ingiustificato ritardo e comunque entro 48 ore dal momento in cui ne è venuto a conoscenza, il Titolare (inviando una comunicazione a mezzo PEC all'indirizzo domus@pec.ancelle.it) di ogni violazione della sicurezza che comporti 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, ed, ai sensi dell'art. 28.3, lett. f), tenuto conto della natura del trattamento e delle informazioni a disposizione del Fornitore, a prestare ogni necessaria collaborazione al Titolare in relazione all'adempimento degli obblighi sullo stesso gravanti di notifica delle suddette violazioni all'Autorità ai sensi dell'art. 33 e 34 del regolamento (UE) 2016/679 o degli articoli 34 e 35 del regolamento (UE) 2018/1725, ove applicabile, tenuto conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento.
- Violazione riguardante dati trattati dal titolare del trattamento: In caso di una violazione dei dati personali trattati dal titolare del trattamento, il responsabile del trattamento assiste il titolare del trattamento:
- a. nel notificare la violazione dei dati personali alla o alle autorità di controllo competenti, senza ingiustificato ritardo dopo che il titolare del trattamento ne è venuto a conoscenza, se del caso/(a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche);
 - b. nell'ottenere le seguenti informazioni che, in conformità dell'articolo 33, paragrafo 3, del regolamento (UE) 2016/679, devono essere indicate nella notifica del titolare del trattamento e includere almeno:
 - c. la natura 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;
 - d. le probabili conseguenze della violazione dei dati personali;
 - e. le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali, se del caso anche per attenuarne i possibili effetti negativi.
- Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.
- Violazione riguardante dati personali trattati dal responsabile del trattamento: In caso di una violazione dei dati personali trattati dal responsabile del trattamento, quest'ultimo ne dà notifica al titolare del trattamento senza ingiustificato ritardo dopo esserne venuto a conoscenza. La notifica contiene almeno:
- a. una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati in questione);
 - b. i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni sulla violazione dei dati personali;
 - c. le probabili conseguenze della violazione dei dati personali e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione, anche per attenuarne i possibili effetti negativi.
- Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la notifica iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.
- 15. Altri adempimenti:** il Responsabile del trattamento è tenuto altresì a:
- a. cooperare con l'Autorità di Controllo quando richiesto;
 - b. supportare l'attività svolta dal DPO (Data Protection Officer – Responsabile della Protezione dei Dati) per conto del Titolare del trattamento, se nominato (artt. 37,38 GDPR);
 - c. designare per iscritto un Rappresentante che lo rappresenti nell'Unione, se il Responsabile non è stabilito nell'UE e ricorrono i presupposti di cui all'art. 27 GDPR.