ALLEGATO A

Descrizione del trattamento di dati personali

Il trattamento dei dati ha per oggetto XXXXXXXX

Finalità per le quali i dati personali sono trattati

I dati forniti vengono trattati al solo fine dell'esecuzione del contratto

Categorie di interessati i cui dati personali sono trattati (Inserire la spunta solo per le categorie oggetto del servizio)

☐ *Pazienti*
☐ *Assistiti del SSN/SSR*
☐ *Studenti*
☐ *Collaboratori*
☐ *Consulenti*
☐ *Dipendenti*
☐ *Docenti*
☐ *Minori*
☐ *Utenti del servizio*
☐ *Altro (se sì, specificare: _____)*

Categorie di dati personali trattati (Inserire la spunta solo per le categorie oggetto del servizio)

☐ *Dati comuni: identificativi diretti (es: nominativi, documenti di identità, foto e videoriprese, codice fiscale, etc.)*
☐ *Dati comuni: identificativi indiretti (es: indirizzo ip, n. matricola, targa, etc.)*
☐ *Dati comuni: dati di contatto (es: n. cellulare, indirizzo mail, fax, etc.)*
☐ *Dati comuni: attività economiche, commerciali, finanziarie e assicurative (dati contabili, ordini, buoni di spedizione, fatture; articoli, prodotti, servizi; contratti accordi transazioni; identificativi finanziari; redditi beni patrimoniali, investimenti*
☐ *Dati altamente personali: relativi ai familiari (stato civile, minori, figli soggetti a carico, consanguinei, altri appartenenti al nucleo familiare)*
☐ *Dati altamente personali: lavoro (occupazione attuale, precedente; informazione sul reclutamento, sul tirocinio o sulla formazione professionale; informazione sulla sospensione o interruzione del rapporto di lavoro o sul passaggio ad altra occupazione; CV)*
☐ *Dati altamente personali: Economici/finanziari (es: inquadramento, carta di credito, bancari, Regolarità fiscale/ contributiva, etc.)*
☐ *Categorie particolari di dati personali: origine razziale o etnica*
☐ *Categorie particolari di dati personali: convinzioni filosofiche o religiose*
☐ *Categorie particolari di dati personali: condizioni di salute attuali*
☐ *Categorie particolari di dati personali: condizioni di salute pregresse*
☐ *Categorie particolari di dati personali: appartenenza sindacale e/o opinioni politiche*
☐ *Categorie particolari di dati personali: stato di salute dei familiari*
☐ *Categorie particolari di dati personali: dati genetici*
☐ *Categorie particolari di dati personali: dati biometrici*
☐ *Categorie particolari di dati personali: dati genetici*
☐ *Dati relativi a reati e condanne penali*
☐ *Altro (se sì, specificare: _____)*

Durata del trattamento

A far data dall'avvio dei servizi (inserire data) fino alla scadenza del contratto (inserire data)

ALLEGATO B

Misure tecniche e organizzative, comprese misure tecniche e organizzative per garantire la sicurezza dei dati (ove applicabile in relazione alla natura del servizio/incarico)

- *Mezzi che permettono di garantire la confidenzialità, l'integrità, la disponibilità e la resilienza costante dei sistemi e dei servizi di trattamento;*
- *Mezzi che permettono di ristabilire la disponibilità dei dati a carattere personale e l'accesso a questi nei tempi appropriati in caso di incidente fisico o tecnico;*
- *La nomina di un DPO;*
- *Adozione di una procedura per la gestione degli incidenti di sicurezza c.d. "Data Breach";*
- *Sottoscrizione di polizze assicurative che tengano conto dei risarcimenti danni di cui all'art. 82 del GDPR con massimali adeguati;*
- *I provvedimenti del Garante applicabili, in particolare:*
  - *Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008;*
  - *Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali - 13 ottobre 2008;*
  - *Linee guida cookie e altri strumenti di tracciamento - 10 giugno 2021;*
- *Le Linee Guida del Garante in materia di Posta elettronica e internet – 01.03.2007 e Trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati – 15.05. 2014;*
- *Misure minime di sicurezza ICT per le pubbliche amministrazioni;*
- *Rispetto delle ISO 27001 e relative estensioni (es. 27017, 27018, 27701, etc.);*
- *Al termine della prestazione dei servizi relativi al trattamento dei dati personali, il responsabile del trattamento ha l'obbligo di restituire tutti i dati personali al titolare del trattamento e cancellare le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati. Il Titolare ha il diritto di verificare che il Responsabile abbia completato in modo appropriato la restituzione o la cancellazione dei dati. Il Titolare può effettuare tale verifica tramite una terza parte, a condizione che la terza parte non abbia una relazione competitiva con il Responsabile stesso. Il Responsabile deve conservare la riservatezza di tutti i dati che gli sono stati resi noti oltre la fine delle presenti clausole che rimarranno valide oltre la fine dell'Accordo principale e fintanto che il Responsabile ha dati personali forniti o raccolti per il Titolare;*
- *In caso di incidente di sicurezza, di una violazione o sospetta violazione dei dati personali, il responsabile del trattamento ne dà notifica al titolare del trattamento senza ingiustificato ritardo dal momento in cui ne è venuto a conoscenza. La notifica del responsabile del trattamento al titolare del trattamento avviene, se possibile, entro 24 ore dal momento in cui è venuto a conoscenza della violazione o presunta violazione dei dati personali per permettere al titolare del trattamento di rispettare il suo obbligo di notifica della violazione stessa all'autorità di controllo competente, cfr. articolo 33, RGPD;*
- *Il Responsabile deve mantenere un Registro degli incidenti di sicurezza e Data Breach, anche qualora non vi siano violazioni, per coadiuvare il Titolare nel suo obbligo relativo al paragrafo 5 dell'art. 33 del GDPR. A seguito del verificarsi di detti incidenti il Titolare potrà:*
  - *fare attività di Audit, anche senza preavviso e avvalendosi di soggetti terzi;*
  - *prescrivere ulteriori misure di sicurezza anche apportando modifiche a quelle in essere con particolare riferimento al presente accordo;*
  - *attivare azioni di rivalsa nei confronti del Responsabile;*
  - *applicare le penali contrattuali;*
  - *risolvere il contratto.*
- *Il Responsabile del Trattamento, qualora non rientri nelle casistiche definite dall' art. 30, par 2 e 5, del Regolamento tiene per iscritto un Registro delle attività relative al trattamento svolte per conto del Titolare e delle applicazioni informatizzate utilizzate, nel pieno rispetto del GDPR;*
- *Il Responsabile del Trattamento si impegna a produrre ed aggiornare in caso di modifiche l'elenco degli operatori autorizzati singolarmente ed opportunamente formati in materia di privacy (ivi inclusi gli opportuni aggiornamenti normativi), impartendo per iscritto specifiche istruzioni per trattare i dati degli utenti nell'ambito della propria attività e con i limiti di legge, curando, in particolare, il profilo della sicurezza di accesso e dell'integrità dei dati ai sensi dell'art.29 del Regolamento. Inoltre, il Responsabile del Trattamento si impegna a stabilire le modalità di accesso ai dati e l'organizzazione del lavoro degli autorizzati al trattamento, avendo cura di adottare preventivamente misure organizzative adeguate al rischio per diritti e libertà delle persone fisiche. Inoltre, deve garantire che le persone autorizzate siano state istruite sulla procedura di gestione degli incidenti di sicurezza e la gestione delle violazioni di dati personali. Il Titolare può richiedere una prova documentata al fine di verificare tali adempimenti;*
- *Il Responsabile, qualora siano presenti Amministratori di Sistema, si impegna a conformarsi al Provvedimento generale del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", così come modificato dal Provvedimento del Garante del 25 giugno 2009 "Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento", così come eventualmente modificato o sostituito dallo stesso Garante, e ad ogni altro pertinente provvedimento dell'Autorità. Il Titolare può richiedere una prova documentata al fine di verificare tali adempimenti;*

ALLEGATO C - ELENCO DEI SUB-RESPONSABILI DEL TRATTAMENTO

Il Responsabile del trattamento nell'esecuzione del servizio e/o della fornitura oggetto del presente affidamento prevede di ricorrere ai seguenti sub-responsabili del trattamento:

Elenco dei sub-responsabili del trattamento		
(Nome, ragione sociale, sede legale)	*Attività svolte per conto del Responsabile del trattamento principale*	*Durata del trattamento*

ALLEGATO D

Contatti/punti di contatto del titolare e del responsabile del trattamento

Le parti possono mettersi in contatto tra di loro utilizzando i seguenti contatti/punti di contatto:

Titolare del trattamento: ASST Mantova

Referente Privacy	*Struttura Affari Generali e Controlli Interni -* *riferimento: dott. ssa Matilde Di Lecce – tel 0376 464805*
DPO	*Dott. Nicola Faravelli*
Direttore dell'Esecuzione del Contratto	*Dott. XXXX*
PEC	*protocollogenerale@pec.asst-mantova.it*

Responsabile del trattamento: XXXXXXXXXXX

Referente Privacy	*Dott. XXXX*
DPO	*XXXX*
Referente contratto	*Dott. XXXX*
PEC	*XXXX*