Accordo per il trattamento dei dati personali

(ai sensi dell'art. 28 del Regolamento UE 2016/679 ("GDPR")

Il presente accordo per il trattamento dei dati personali è concluso tra il Fornitore, come di seguito definito, e il Cliente che accetta il presente accordo.

TRA

Il Cliente o Professionista titolare del contratto di servizio CLICKDOC

E

Compugroup Medical S.r.l., con sede in Via Adriano Olivetti, 10 Molfetta (BA), iscritta al registro delle imprese di Bari al n. 05014030729, P. IVA 05014030729, PEC cgmitalia@pcert.postecert.it (di seguito, il "Fornitore")

(di seguito, collettivamente, definite le "Parti" e singolarmente la "Parte")

PREMESSO CHE

a) Il Professionista è un esercente di una professione sanitaria o prestatore di servizi sanitari;

b) Il Fornitore è titolare di una piattaforma resa disponibile tramite il sito www.clickdoc.it, costituita dal software sviluppato dal Fornitore e dai relativi contenuti (di seguito, la "Piattaforma"), che consente agli utenti della Piattaforma (gli "Utenti") la prenotazione online di una o più prestazioni sanitarie (le "Prestazioni") presso i professionisti iscritti alla Piattaforma nonché la fruizione di ulteriori servizi accessori;

c) Il Professionista ha manifestato l'interesse ad avvalersi della Piattaforma al fine di ricevere prenotazioni delle Prestazioni dallo stesso svolte, da parte degli Utenti della Piattaforma, nonché per usufruire degli ulteriori servizi accessori ivi offerti;

d) tra il Fornitore ed il Professionista è stato pertanto concluso un contratto (di seguito, "Contratto") avente ad oggetto l'erogazione, da parte del Fornitore stesso, di servizi (di seguito: "Servizi");

e) lo svolgimento dei suddetti Servizi da parte del Fornitore comporta il trattamento, da parte di quest'ultimo, per conto del Professionista, dei dati personali degli Utenti trattati ai fini dell'erogazione del Servizio al Professionista, di cui lo stesso è Titolare del trattamento (di seguito, i "Dati Personali"), meglio indicati in Allegato 1;

f) il Professionista ha verificato che il Fornitore possiede esperienza, competenze tecniche e risorse che gli consentono di mettere in atto misure tecniche e organizzative adeguate atte a garantire la conformità alla normativa in materia di tutela dei dati personali e la tutela degli interessati;

g) con il presente atto di designazione, le Parti intendono regolare i trattamenti dei Dati Personali da parte del Fornitore ai sensi dell'art. 28.3 del Regolamento (UE) 2016/679 del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali - Regolamento Generale sulla Protezione dei Dati Personali, entrato in vigore il 24 maggio 2016 e applicabile dal 25 maggio 2018 (di seguito, "GDPR" o "Regolamento");

h) il Professionista ed il Fornitore sono qualificati anche, nel prosieguo, rispettivamente, quali Titolare e Responsabile;

Tutto ciò premesso (e costituendo le premesse parte integrante e sostanziale del presente atto di designazione), fra le Parti si conviene e si stipula quanto segue.

1. Oggetto

1.1 Le Parti riconoscono e convengono che il Fornitore agisce quale Responsabile del trattamento dei dati personali. Con la stipula del presente accordo, il Cliente affida al Fornitore l'incarico di trattare i dati personali ai fini della prestazione dei Servizi, così come meglio dettagliato nell'Allegato 1.

1.2 Resta inteso che il Professionista, quale Titolare del trattamento, è l'unico responsabile della correttezza e della legittimità dei Dati Personali acquisiti e raccolti ed è tenuto ad adempiere a tutti gli obblighi di cui al GDPR gravanti sul Titolare.

1.3 Il Fornitore ha nominato un Responsabile della protezione dei dati (DPO) che può essere contattato all'indirizzo dpo.it@cgm.com.

2. Obblighi del Responsabile

2.1 Il Fornitore è tenuto a trattare i Dati Personali solo ed esclusivamente ai fini dell'esecuzione dei Servizi, nel rispetto di quanto disposto dalla normativa applicabile in materia di protezione dei dati personali, nonché delle ragionevoli istruzioni del Titolare riportate nei successivi articoli e di ogni altra indicazione scritta che potrà essergli dallo stesso successivamente fornita.

3. Misure di sicurezza

3.1 Il Responsabile, previa effettuazione dell'analisi dei rischi (e tenendo conto, in particolare, dei rischi che derivano dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, ai Dati Personali trasmessi, conservati o comunque trattati), si impegna ad adottare e a mantenere misure tecniche ed organizzative adeguate per proteggere la sicurezza, la riservatezza e l'integrità dei Dati Personali, tenendo conto, fra l'altro,

della tipologia di trattamento, delle finalità perseguite, del contesto e delle specifiche circostanze in cui avviene il trattamento, nonché della tecnologia applicabile e dei costi di attuazione.

3.2 Fermo restando quanto sopra, il Responsabile si obbliga ad adottare, in particolare, le misure di sicurezza fisiche, logiche e organizzative di cui all'Allegato 2.

3.3 Eventuali evoluzioni e/o modifiche delle misure di sicurezza dovute a mutate esigenze del Professionista e/o a modifiche ed aggiornamenti della normativa in materia di protezione dei dati personali saranno adottate ed implementate dal Fornitore e/o suoi eventuali subappaltatori a onere e spese del Professionista e su espressa richiesta ed indicazione da parte di quest'ultimo e anche sulla base della valutazione di impatto che sarà suo onere condurre in qualità di Titolare del trattamento, se del caso con la collaborazione del Fornitore.

3.4 Il Responsabile si impegna, altresì, ad assistere il Professionista in relazione all'obbligo del Titolare di mettere in atto misure tecniche ed organizzative adeguate ai sensi dall'art. 32 del GDPR, tenuto conto della natura del trattamento e delle informazioni a disposizione del Fornitore. Il Fornitore si riserva di quantificare e comunicare preliminarmente al Professionista l'eventuale impegno economico necessario per l'implementazione di servizi non inclusi nel Contratto.

4. Violazioni di dati personali (cd. "Data Breach")

4.1 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) 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 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 del GDPR o di comunicazione della stessa agli interessati ai sensi dell'art. 34 del GDPR.

5. Valutazione d'impatto (cd. "Data Protection Impact Assessment")

5.1 Il Responsabile s'impegna fin da ora 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 ai sensi dell'art. 36 del Regolamento stesso.

6. Soggetti autorizzati al trattamento

6.1 Fatto salvo quanto previsto all'articolo 9 che segue, il Responsabile garantisce che l'accesso ai Dati Personali sarà limitato ai soli propri dipendenti e collaboratori il cui accesso ai Dati Personali sia necessario per l'esecuzione dei Servizi.

6.2 Il Responsabile si impegna a fornire ai propri dipendenti e collaboratori deputati a trattare i Dati Personali di cui è Titolare il Professionista le istruzioni necessarie per garantire un corretto, lecito e sicuro trattamento, vincolandoli alla riservatezza su tutte le informazioni acquisite nello svolgimento della loro attività.

7. Istanze degli interessati

7.1 Il Responsabile si obbliga ad avvertire prontamente il Titolare, entro tre (3) giorni lavorativi, in merito alle eventuali richieste degli interessati che dovessero pervenire al Responsabile inviando copia delle istanze ricevute all'indirizzo PEC del Professionista e collaborare al fine di garantire il pieno esercizio da parte degli interessati di tutti i diritti previsti dalla normativa applicabile.

8. Ulteriori obblighi

8.1 Il Responsabile mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui alla normativa in materia di protezione dei dati personali e/o delle istruzioni del Titolare di cui al presente accordo sul trattamento dei dati personali.

Il Responsabile si impegna altresì a:

a) realizzare quant'altro sia ragionevolmente utile e/o necessario al fine di garantire l'adempimento degli obblighi previsti dalla normativa applicabile in materia di protezione dei dati, nei limiti dei compiti affidati con il presente atto di designazione;

b) informare prontamente il Titolare di ogni questione rilevante ai fini di legge, in particolar modo, a titolo esemplificativo e non esaustivo, nei casi in cui abbia notizia, in qualsiasi modo, che risulti violata la normativa in materia di protezione dei dati personali, ovvero che il trattamento presenti rischi specifici per i diritti, le libertà fondamentali e/o la dignità dell'interessato, nonché qualora, a suo parere, un'istruzione violi la normativa, nazionale o comunitaria, relativa alla protezione dei dati.

c) non diffondere o comunicare a terzi i dati trattati attraverso l'attività;

d) procedere alla nomina del proprio/i amministratore/i di sistema, in adempimento di quanto previsto dal provvedimento del Garante del 27.11.08, pubblicato in G.U. n. 300 del 24.12.2008, ove ne ricorrano i presupposti, comunicandolo prontamente al Titolare, curando, altresì, l'applicazione di tutte le ulteriori prescrizioni contenute nel suddetto provvedimento.

9. Ulteriori responsabili e limitazioni al trasferimento dei dati al di fuori dello Spazio Economico Europeo (SEE)

9.1 Il Responsabile è autorizzato sin da ora a ricorrere ad altri responsabili (di seguito, "Sub-responsabili") per l'esecuzione di specifiche attività di trattamento di Dati Personali per conto del

Titolare, imponendo agli stessi, per iscritto, attraverso appositi accordi vincolanti, i medesimi obblighi in materia di protezione dei dati cui è soggetto il Responsabile in virtù del presente atto di designazione, in particolare in relazione agli obblighi in materia di sicurezza.

9.2 Il Responsabile si impegna espressamente ad informare di eventuali modifiche riguardanti l'aggiunta o la sostituzione degli ulteriori Sub-responsabili il Titolare, che avrà il diritto di opporsi a tali modifiche, comunicando la propria opposizione per iscritto, da inviare all'indirizzo dpo.it@cgm.com, entro 10 giorni dalla messa a disposizione di tali informazioni da parte del Responsabile sul sito internet www.clickdoc.it/doc/sub-responsabili.html. Il Responsabile non ricorrerà ai Sub-responsabili nei cui confronti il Titolare abbia manifestato la propria opposizione. Resta inteso che, in mancanza di opposizione, la modifica si intenderà accettata.

9.3 Resta espressamente inteso che il Responsabile rimarrà direttamente responsabile nei confronti della Società in ordine alle azioni e alle omissioni dei propri Sub-responsabili.

9.4 L'elenco dei Sub-responsabili è disponibile al link www.clickdoc.it/doc/sub-responsabili.html.

9.5 Il Cliente acconsente espressamente sin d'ora che alcune operazioni di trattamento di dati personali siano affidate dal Fornitore ad altre società del Gruppo CGM, il cui elenco è disponibile al link indicato al precedente punto 9.4.

9.6 Il Fornitore si astiene dal trasferire i dati personali trattati per conto del Cliente al di fuori dello Spazio Economico Europeo senza il previo consenso scritto di volta in volta del Cliente; in caso di consenso, il Fornitore dovrà assicurarsi che il trattamento avvenga verso Paesi terzi e Organizzazioni internazionali che garantiscano un livello di sicurezza e protezione adeguato adottando tutte le misure previste dagli artt. 44 e ss. del GDPR.

10. Responsabilità

10.1 Il Fornitore sarà responsabile per i danni conseguenti a inadempimenti o inosservanze delle istruzioni di cui al presente atto di designazione o di quelle successive eventualmente trasmesse per iscritto dal Professionista, nei limiti della clausola sulla limitazione di responsabilità contenuta nel Contratto.

10.2 Resta inteso che, laddove il Responsabile abbia adempiuto integralmente i compiti assegnatigli in forza del presente atto di designazione e le obbligazioni del GDPR specificatamente dirette ai Responsabili, il Professionista risponderà integralmente di eventuali danni cagionati dal trattamento dei Dati Personali effettuato in violazione di legge, tanto nei confronti del Fornitore che degli Utenti.

11. Durata

11.1 La presente designazione decorre dalla data di attivazione dei Servizi che comportano un trattamento di dati per conto del Cliente ed è valida fino alla cessazione per qualunque motivo del Contratto e/o, comunque, dei Servizi, fermo restando che, anche successivamente alla cessazione del Contratto o dei Servizi, il Responsabile dovrà mantenere la massima riservatezza sui dati e le

informazioni relative al Titolare delle quali sia venuto a conoscenza nell'adempimento delle sue obbligazioni.

12. Restituzione e cancellazione dei dati personali

12.1 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.

13. Verifiche e controlli

13.1 Il Fornitore sottopone ad audit periodici la sicurezza dei sistemi e degli ambienti di elaborazione dei dati personali dallo stesso utilizzati per l'erogazione dei Servizi e le sedi in cui avviene tale trattamento. Il Fornitore avrà la facoltà di incaricare dei professionisti indipendenti selezionati dal Fornitore per lo svolgimento di audit secondo standard internazionali e/o best practice, i cui esiti saranno riportati in specifici report. Tali report, che costituiscono informazioni confidenziali del Fornitore, potranno essere resi disponibili al Professionista per consentirgli di verificare la conformità del Fornitore agli obblighi di sicurezza di cui al presente accordo.
13.2 Nei casi previsti dall'art. 13.1, il Professionista concorda che il proprio diritto di verifica sarà esercitato attraverso la verifica dei report messi a disposizione dal Fornitore.
13.3 Il Fornitore riconosce il diritto del Professionista, con le modalità e nei limiti di seguito indicati, ad effettuare audit indipendenti per verificare la conformità del Fornitore agli obblighi previsti nel presente Accordo e di quanto previsto dalla normativa. Il Professionista potrà avvalersi per tali attività di proprio personale specializzato o di revisori esterni, purché tali soggetti siano previamente vincolati da idonei impegni alla riservatezza.
13.4 Nel caso di cui al precedente punto 13.2, il Cliente dovrà previamente inviare richiesta scritta al Responsabile della Protezione dei Dati (DPO) del Fornitore. Successivamente alla richiesta di audit o ispezione il Fornitore e il Cliente concorderanno, prima dell'avvio delle attività, i dettagli di tali verifiche (data di inizio e durata), le tipologie di controllo e l'oggetto delle verifiche, i vincoli di riservatezza a cui devono essere vincolati il Cliente e coloro che effettuano le verifiche e i costi che il Fornitore potrà addebitare per tali verifiche e che saranno determinati in relazione all'estensione e alla durata delle attività di verifica.
13.5 Il Fornitore potrà opporsi per iscritto alla nomina da parte del Cliente di eventuali revisori esterni che siano, ad insindacabile giudizio del Fornitore, non adeguatamente qualificati o indipendenti, siano concorrenti del Fornitore o che siano evidentemente inadeguati. In tali circostanze il Cliente sarà tenuto a nominare altri revisori o a condurre le verifiche in proprio.
13.6 Il Cliente si impegna a corrispondere al Fornitore gli eventuali costi calcolati dal Fornitore e comunicati al Cliente nella fase di cui al precedente punto 13.4, con le modalità e nei tempi ivi concordati. Restano a carico esclusivo del Cliente i costi delle attività di verifica dallo stesso commissionate a terzi.

14. Disposizioni finali

14.1 Per tutto quanto non previsto dal presente atto di designazione si rinvia alle disposizioni generali vigenti ed applicabili in materia protezione dei dati personali.

ALLEGATO 1

Il presente allegato costituisce parte integrante della nomina a responsabile.

Categorie di interessati

- Utenti della Piattaforma e Utenti non iscritti che fruiscono dei Servizi presso il Professionista.
    - Operatori individuati dal Professionista.

Tipo di Dati Personali oggetto di trattamento (indicare se dati comuni, categorie particolari, dati relativi a condanne penali e reati)

- dati comuni (dati anagrafici quali a titolo esemplificativo e non esaustivo: nome, cognome; dati di contatti quali indirizzo postale, indirizzo e-mail, numero di telefono).

- categorie particolari di dati personali (dati sanitari) che l'Utente dovesse inserire sulla Piattaforma o comunque deducibili delle Prestazioni prenotate dall'Utente tramite la Piattaforma nonché ulteriori dati sanitari relativi all'Utente che il Professionista dovesse raccogliere direttamente dall'Utente ed inserire sulla Piattaforma.

Natura e finalità del trattamento

- attività preliminari e/o ancillari all'erogazione dei Servizi (es. backup, importazione e download di dati etc.);

- erogazione dei Servizi Agenda base e prenotazioni nonché delle attività di assistenza on site e/o da remoto;

- eventuali servizi di hosting;

ALLEGATO 2

MISURE DI SICUREZZA

Misure di sicurezza organizzative	**Policy e Disciplinari utenti**: il Fornitore applica dettagliate policy e disciplinari, ai quali tutta l'utenza con accesso ai sistemi informativi ha l'obbligo di conformarsi e che sono finalizzate a garantire comportamenti idonei ad assicurare il rispetto dei principi di riservatezza, disponibilità ed integrità dei dati nell'utilizzo delle risorse informatiche. **Autorizzazione accessi logici**: il Fornitore definisce i profili di accesso nel rispetto del least privilege necessari all'esecuzione delle mansioni assegnate. I profili di autorizzazione sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento. Tali profili sono oggetto di controlli periodici finalizzati alla verifica della sussistenza delle condizioni per la conservazione dei profili attribuiti. **Gestione interventi di assistenza:** gli interventi di assistenza sono regolamentati allo scopo di garantire l'esecuzione delle sole attività previste contrattualmente e impedire il trattamento eccessivo di dati personali la cui titolarità è in capo al Cliente. **Data Breach:** il Fornitore ha implementato un'apposita procedura finalizzata alla gestione degli eventi e degli incidenti con un potenziale impatto sui dati personali che definisce ruoli e responsabilità, il processo di rilevazione (presunto o accertato), l'applicazione delle azioni di contrasto, la risposta e il contenimento dell'incidente / violazione nonché le modalità attraverso le quali effettuare le comunicazioni delle violazioni di dati personali al Cliente. **Formazione:** il Fornitore eroga periodicamente ai propri dipendenti coinvolti nelle attività di trattamento corsi di formazione sulla corretta gestione dei dati personali.
Misure di sicurezza tecniche	**Firewall:** le reti informatiche del Fornitore sono protette da sistemi di sicurezza perimetrale (c.d. Firewall) e da altre apparecchiature all'uopo destinate mantenute aggiornate allo stato dell'arte.

	Antivirus: ogni postazione di lavoro del Fornitore è protetta da sistemi di sicurezza contro le minacce informatiche (antivirus) e ne è consentito l'utilizzo unicamente mediante appositi sistemi di autenticazione e profilazione. **Monitoraggio dei sistemi:** il Fornitore effettua verifiche di monitoraggio e scansioni di vulnerabilità giornalieri. **Credenziali di autenticazione:** i sistemi sono configurati con modalità idonee a consentirne l'accesso unicamente a soggetti dotati di credenziali di autenticazione che ne consentono la loro univoca identificazione. Fra questi, codice associato a una parola chiave, riservata e conosciuta unicamente dallo stesso; dispositivo di autenticazione in possesso e uso esclusivo dell'utente, eventualmente associato a un codice identificativo o a una parola chiave. **Sicurezza canali di comunicazione:** per quanto di propria competenza, sono adottati dal Fornitore protocolli di comunicazione sicuri e in linea con quanto la tecnologia rende disponibile . **Logging:** i sistemi sono configurabili con modalità che consentono il tracciamento degli accessi e, ove appropriato, delle attività svolte in capo alle diverse tipologie di utenze (Amministratore, Super Utente, etc.) protetti da adeguate misure di sicurezza che ne garantiscono l'integrità. **Backup:** per evitare perdite, i dati vengono regolarmente sottoposti a backup veicolati dalle procedure di sicurezza IT della capogruppo tedesca CGM SE. **Amministratori di Sistema:** relativamente a tutti gli utenti che operano in qualità di Amministratori di Sistema, il cui elenco è mantenuto aggiornato e le cui funzioni attribuite sono opportunamente definite in appositi atti di nomina, è gestito un sistema di log management finalizzato al puntuale tracciamento delle attività svolte ed alla conservazione di tali dati con modalità inalterabili idonee a consentirne ex post il

	monitoraggio. L'operato degli Amministratori di Sistema è sottoposto ad attività di verifica in modo da controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previsti dalle norme vigenti. **Amministrazione da remoto:** dipendenti o subappaltatori del Fornitore potrebbero dover accedere ai dati dei pazienti o dei clienti e occasionalmente ai dati del Cliente. Tale accesso è disciplinato dalle regole generali del Fornitore: o l'accesso all'amministrazione da remoto è chiuso per impostazione predefinita e viene autorizzato solo dal Cliente, il quale avrà la possibilità di monitorare gli interventi; o le password per accedere ai sistemi IT del Cliente vengono rilasciate da quest'ultimo solo per le finalità di cui all'Allegato 1; o gli interventi critici sono garantiti da una procedura "4-eyes" (principio del doppio controllo) con ulteriore presenza dell'interessato; o l'accesso all'amministrazione da remoto viene registrato nel sistema CRM. Vengono registrati i seguenti dati: persona responsabile, data e ora, durata, sistema di destinazione, breve descrizione dell'attività svolta e, in caso di interventi critici, i nominativi del personale qualificato aggiuntivo consultato nell'applicazione della procedura "4-eyes ; o la registrazione delle sessioni di amministrazione da remoto è vietata, salvo i casi in cui sia necessaria per la risoluzione dei problemi segnalati dal cliente.