

ATTO DI DESIGNAZIONE A RESPONSABILE DEL TRATTAMENTO

Tra

Il Professionista titolare del contratto di servizio CLICKDOC

e

Medicitalia Srl, con sede in Foro Buonaparte, 70 Milano, iscritta al registro delle imprese di Milano al n. MI-2080005, P. IVA 01582700090, PEC medicitalia@pec.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, fra gli altri, l'erogazione, da parte del Fornitore stesso, dei servizi di "gestione calendario prenotazioni online" (di seguito: **"Servizi"**), di cui il presente atto di designazione a responsabile del trattamento costituisce parte integrante e sostanziale;
- 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 Con il presente atto, il Fornitore è nominato dal Professionista Responsabile del trattamento dei Dati Personali connesso all'erogazione dei Servizi.

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.

2. OBBLIGHI DEL RESPONSABILE

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")

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")

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 11 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

Il Responsabile si obbliga ad assistere il Titolare con misure tecniche ed organizzative adeguate, nella misura in cui ciò sia possibile, nell'adempimento dei propri obblighi di dar seguito ad eventuali istanze degli Utenti di cui al capo III del GDPR.

8. ULTERIORI OBBLIGHI

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 atto di designazione e consente al Titolare del trattamento l'esercizio del potere di controllo e ispezione, prestando ogni collaborazione alle attività di audit effettuate dal Titolare stesso o da un altro soggetto da questi incaricato o autorizzato, con lo scopo di controllare l'adempimento degli obblighi e delle istruzioni di cui al presente atto. Resta inteso che qualsiasi verifica condotta ai sensi del presente comma dovrà essere eseguita in maniera tale da non interferire con il normale corso delle attività del Responsabile e fornendo a quest'ultimo un ragionevole preavviso. Il Responsabile si riserva di quantificare e comunicare preliminarmente al Professionista l'eventuale impegno economico necessario per permettere a quest'ultimo le suddette

attività di audit.

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.

9. ULTERIORI RESPONSABILI

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 comunicazione o dalla messa a disposizione di tali informazioni da parte del Responsabile con ogni mezzo da quest'ultimo ritenuto idoneo (pubblicazione dell'elenco dei Sub-Responsabili sul sito internet www.clickdoc.it/doc/sub-responsabili.html, invio di comunicazioni via mail relative ai Servizi, etc.). 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 tramite richiesta via email indirizzata a: dpo.it@cgm.com o al link www.clickdoc.it/doc/sub-responsabili.html.

10. RESPONSABILITÀ

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.

Resta inteso che, laddove il Responsabile abbia adempiuto integralmente i compiti

assegnatigli in forza del presente atto di designazione ed 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

La presente designazione decorre dalla data di conclusione del Contratto, di cui costituisce parte integrante e sostanziale, 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

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.

13. DISPOSIZIONI FINALI

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
AMBITO del TRATTAMENTO

Il presente allegato costituisce parte integrante della nomina a responsabile.

Categorie di interessati

- Utenti della Piattaforma che prenotano una Prestazione presso il Professionista

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

- dati comuni (dati di contatto quali: nome, cognome, indirizzo postale, indirizzo e-mail, numero di telefono, peso, altezza)
- 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 relativa 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, on site e/o da remoto;
- eventuali servizi di hosting;

Durata del trattamento

- esecuzione del Contratto (cfr. artt. 11 e 12 dell'atto di designazione a responsabile del trattamento)

ALLEGATO 2

MISURE DI SICUREZZA

Per garantire la sicurezza dei dati, il Fornitore rivede regolarmente lo stato dell'arte delle tecnologie di sicurezza. Ciò include la determinazione di scenari di danno tipici, le esigenze di sicurezza e i livelli di sicurezza corrispondenti che ne derivano per diversi tipi di dati personali, raggruppati in categorie di possibili danni, nonché l'esecuzione di valutazioni del rischio.

Inoltre, vengono effettuati test di penetrazione dedicati per analizzare, esaminare e valutare regolarmente l'efficacia di queste misure tecniche e organizzative che devono garantire la sicurezza del trattamento.

I seguenti orientamenti disciplinano l'attuazione di misure tecniche e organizzative appropriate:

- **Backup dei dati (servizi SaaS)**

Per evitare perdite, i dati vengono regolarmente sottoposti a backup veicolati dalle procedure di sicurezza IT della capogruppo tedesca CGM SE.

- **"Privacy by design"**

Il Fornitore garantisce che i principi di protezione / privacy dei dati e di sicurezza dei dati siano presi in considerazione durante i processi di progettazione e sviluppo dei sistemi IT.

L'obiettivo è quello di prevenire un'attività di programmazione aggiuntiva, dispendiosa in termini di costi e di tempo, che sarebbe necessaria se i requisiti di privacy e sicurezza dei dati dovessero essere attuati dopo l'installazione dei sistemi IT. All'inizio del processo di sviluppo vengono prese in considerazione misure come la disattivazione di alcune funzionalità software, l'autenticazione o la crittografia.

- **"Privacy by default"**

I prodotti CGM sono dotati di impostazioni di fabbrica ottimizzate per la privacy dei dati, in modo che vengano trattati solo i dati personali necessari per il relativo scopo.

- **Comunicazione via e-mail (Cliente / Fornitore)**

Nel caso in cui si desideri contattare il Fornitore tramite e-mail, tenere presente che la privacy delle informazioni trasmesse non può essere garantita, poiché il contenuto delle e-mail può essere visualizzato anche da terzi. Si consiglia di contattare il Fornitore ogni volta che si desidera trasmettere informazioni riservate.

- **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.

- **Misure di sicurezza IT**

Firewall o sicurezza perimetrale

Le reti informatiche di 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

Protezione Anti-virus

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.