ATTO DI DESIGNAZIONE A RESPONSABILE DEL TRATTAMENTO

Tra

ARNAS G. Brotzu, con sede in Cagliari, Piazzale A. Ricchi n. 1, P.IVA 02315520920 in persona del proprio Legale Rappresentante, Dott. Maurizio Marcias (di seguito, la "**Società**" e/o "**Titolare**"),

e

Medigas Italia, con sede in Assago (MI) Via Edison n. 6, P.IVA 11861240155, in persona del suo Legale rappresentate Dott. Giancarlo Fontana (di seguito, il "**Responsabile**" e/o "**Fornitore**")

(di seguito, collettivamente, definite le "**Parti**")

PREMESSO CHE

a) il Fornitore e la Società hanno stipulato in data 03/02/2025 un contratto (di seguito, "**Contratto**"), avente ad oggetto l'erogazione, da parte del Fornitore stesso, del servizio di manutenzione delle apparecchiature e degli impianti appartenenti alla S.S.D. Banca del Sangue Cordonale dell'ARNAS G. Brotzu per la durata di 5 anni (di seguito: "**Servizi**");

b) lo svolgimento dei suddetti Servizi da parte del Fornitore comporta il trattamento, da parte di quest'ultimo, per conto della Società, dei dati personali di interessati di cui la Società stessa è Titolare (di seguito: "**Dati Personali**"), meglio indicati in **Allegato 1**;

c) il Fornitore dichiara di possedere esperienza, competenze tecniche e risorse che gli consentono di mettere in atto misure tecniche e organizzative adeguate atte a garantire la conformità al Regolamento UE 2016/679 ("**GDPR**") e alla normativa di settore applicabile in materia di tutela dei dati personali (di seguito, "**Normativa**");

d) con il presente contratto (di seguito, "**DPA**"), le Parti intendono disciplinare in conformità al GDPR e alla Normativa il trattamento e la protezione dei Dati Personali trattati dal Fornitore in esecuzione dei Servizi. la Società 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, è nominato dal Titolare responsabile del trattamento dei Dati Personali connessi all'erogazione dei Servizi.
1.2 Resta inteso che il Titolare, è l'unico responsabile della correttezza e della legittimità dei Dati Personali acquisiti e raccolti ed è tenuto ad adempiere a tutti i suoi obblighi di cui al GDPR.

2. OBBLIGHI DEL RESPONSABILE

2.1 Il Responsabile è tenuto a trattare i Dati Personali solo ed esclusivamente ai fini dell'esecuzione dei Servizi, nel rispetto di quanto disposto dal GDPR e dalla Normativa, 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, in linea con le previsioni di cui all'art. 32 del GDPR, 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 riservatezza, l'integrità e la disponibilità dei Dati Personali trattati, 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**, tenuto conto anche di eventuali evoluzioni e/o modifiche delle misure di sicurezza dovute a mutate esigenze del Titolare e/o a modifiche ed aggiornamenti della Normativa che saranno adottate ed implementate dal Responsabile e/o suoi eventuali subappaltatori a onere e spese del Titolare e anche sulla base della valutazione di impatto che sarà onere del Titolare condurre.

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 all'indirizzo direzione.generale@pec.aobrotzu.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 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.

4.2 La notifica contiene, ove disponibili, almeno: (i) descrizione dell'evento; (ii) categorie e volume indicativo dei dati; (iii) possibili conseguenze; (iv) misure adottate o proposte; (v) punto di contatto operativo.

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 GDPR, nonché ogni collaborazione nell'effettuazione della eventuale consultazione preventiva al Garante ai sensi dell'art. 36 del GDPR 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 ai quali 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 la Società 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. AMMINISTRATORI DI SISTEMA

7.1 Il Responsabile 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 25 giugno 2009, così come eventualmente modificato o sostituito dallo stesso Garante, e ad ogni altro pertinente provvedimento dell'Autorità, ove applicabile.

7.2 Il Responsabile si impegna, in particolare, a designare, predisporre e conservare l'elenco, comunicare gli eventuali aggiornamenti dello stesso, verificare l'operato e mantenere i file di log degli Amministratori di Sistema in conformità a quanto previsto nel suddetto provvedimento.

8. RAPPORTI CON LE AUTORITÀ

8.1 Il Responsabile, su richiesta del Titolare, si impegna a coadiuvare quest'ultimo nella difesa in caso di procedimenti dinanzi all'autorità di controllo o all'autorità giudiziaria che riguardino il trattamento dei Dati Personali.

9. ISTANZE DEGLI INTERESSATI

9.1 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 interessati di cui al capo III del GDPR.

10. ULTERIORI OBBLIGHI

10.1 Il Responsabile mette a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente atto, al GDPR e alla Normativa, consentendo e contribuendo alle attività di revisione, comprese le ispezioni, condotte dal Titolare o da altro soggetto da questi incaricato. A tale scopo il Responsabile riconosce al Titolare, e/o agli incaricati dal medesimo, il diritto di accedere ai locali di sua pertinenza ove hanno svolgimento le operazioni di trattamento o dove sono custoditi dati e/o documentazione relativa al presente atto. In ogni caso il Responsabile si impegna, per sé e per i terzi incaricati, a che le informazioni raccolte durante le operazioni di verifica siano utilizzate solo per tali finalità.

10.2 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 preavviso di almeno 15 (quindici) giorni lavorativi.

10.3 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 nomina;

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, 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.

11. ULTERIORI RESPONSABILI

11.1 Il Responsabile è autorizzato sin da ora a ricorrere ad altri responsabili (di seguito, "**Sub-responsabili**") per l'esecuzione di specifiche attività di trattamento solo a condizione che imponga ai Sub-Responsabili, mediante accordo scritto, obblighi di protezione dei dati non meno rigorosi di quelli previsti nel presente DPA, in particolare in materia di sicurezza (art. 32 GDPR).

11.2 Il Responsabile si impegna espressamente ad informare il Titolare per iscritto con un preavviso di almeno 15 giorni di ogni eventuale modifica riguardante l'aggiunta o la sostituzione dei Sub-Responsabili, indicando almeno: identità, contatti, attività affidate e localizzazione del trattamento. Il Titolare avrà il diritto di opporsi per iscritto entro tale termine e 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.

11.3 Resta espressamente inteso che il Responsabile rimarrà direttamente responsabile nei confronti del Titolare in ordine alle azioni e alle omissioni dei propri Sub-Responsabili.

12. RESPONSABILITÀ

12.1 Il Fornitore sarà responsabile per i danni conseguenti a inadempimenti o inosservanze delle istruzioni di cui al presente atto o di quelle successive eventualmente trasmesse per iscritto dalla Società.

12.2 Resta inteso che, laddove il Responsabile abbia adempiuto integralmente ai compiti assegnatigli in forza del presente DPA ed alle obbligazioni del GDPR specificatamente dirette ai Responsabili, la Società risponderà comunque dei danni cagionati dal trattamento effettuato in violazione di legge, se ingiustificatamente rifiuta di effettuare i necessari interventi segnalati dal Responsabile e/o di adottare le misure dallo stesso suggerite anche ai sensi del precedente art. 10.2, b).

13. DURATA

13.1 L'efficacia del presente DPA decorre dalla data in cui viene sottoscritta dalle Parti ed è valida fino alla cessazione per qualunque motivo del Contratto e/o, comunque, dei Servizi ovvero fino alla revoca anticipata per qualsiasi motivo da parte del Titolare, fermo restando che, anche successivamente alla cessazione del Contratto o dei Servizi o alla revoca, 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.

14. RESTITUZIONE E CANCELLAZIONE DEI DATI PERSONALI

14.1 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.

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

15. DISPOSIZIONI FINALI

15.1 Per tutto quanto non previsto dalla presente DPA si rinvia alle disposizioni generali vigenti ed applicabili in materia protezione dei dati personali.

15.2 In caso di conflitto tra il presente DPA e quanto previsto da qualsiasi altro accordo vigente tra le Parti in materia di dati personali, ivi incluso il Contratto, il presente DPA è destinato a prevalere.

Cagliari, 02/02/2026

IL TITOLARE DEL TRATTAMENTO

Dott. Maurizio Marcias

Per accettazione

IL RESPONSABILE DEL TRATTAMENTO

Dott. Giancarlo Fontana

ALLEGATO 1

AMBITO del TRATTAMENTO

FINALITÀ DEL TRATTAMENTO

- Gestione dei dati relativi ai campioni biologici, tutti nulla escluso, ai fini della tracciabilità di stoccaggio degli stessi all'interno di criocontenitori e ultrafreezer

CATEGORIE DI INTERESSATI

- Personale (dipendenti, collaboratori, tirocinanti, stagisti)
- Pazienti

TIPO DI DATI PERSONALI OGGETTO DI TRATTAMENTO

Dati Personali comuni

- Dati anagrafici
- Dati di contatto

Dati Personali particolari

- Dati relativi alla salute

DURATA DEL TRATTAMENTO

Durata pari alla durata del Contratto, fatti salvi gli obblighi di conservazione e le tempistiche di cancellazione dei Dati Personali previste contrattualmente.

ALLEGATO 2

MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

Il Responsabile, tenuto conto che i Dati Personali oggetto di trattamento includono dati relativi alla salute (Allegato 1), adotta e mantiene almeno le seguenti misure tecniche e organizzative, idonee a garantire un livello di sicurezza adeguato al rischio ai sensi dell'art. 32 GDPR.

1. account individuali per l'accesso a sistemi e caselle e-mail che trattano dati (divieto di account condivisi);

2. autenticazione multi-fattore (MFA) attiva almeno su e-mail professionale, accessi remoti (se presenti) e account con privilegi elevati/gestionali;

3. password robuste e gestione delle credenziali che preveda il cambio immediato in caso di sospetta compromissione e il divieto di riuso sistematico e l'uso di password manager ove possibile;

4. accesso ai dati limitato al personale strettamente necessario e revoca/aggiornamento degli accessi alla cessazione o cambio mansione e verifica almeno annuale delle abilitazioni;

5. blocco automatico dello schermo e logout dalle applicazioni al termine dell'uso su postazioni accessibili ad altri (es. banco/retro);

6. sistemi operativi e software (browser, client mail, gestionali) aggiornati con update automatici attivi dove possibile;

7. antimalware attivo e aggiornato su tutte le postazioni che trattano dati;

8. cifratura dei dispositivi mobili (laptop/PC portatili) e dei dischi che possono contenere o accedere a dati;

9. accessi remoti consentiti solo in modalità sicura e con MFA con divieto di esporre servizi di accesso remoto non protetti su Internet;

10. uso di canali cifrati (TLS/HTTPS) e, se si inviano documenti con dati sanitari via e-mail, utilizzo di file protetti da password comunicata su canale separato e controllo dei destinatari prima dell'invio;

11. uso di chiavette USB solo se necessario e divieto di utilizzare supporti personali non controllati;

12. backup regolare dei dati/gestionali rilevanti con almeno una copia separata e conservazione coerente con le esigenze operative ed esecuzione di una prova di restore almeno su base annuale;

13. controllo accessi alle aree dove sono presenti postazioni di lavoro e/o archivi, e archivi cartacei con dati in armadi chiusi a chiave;

14. triturazione (shredder) o servizio equivalente per carta e supporti dismessi;

15. istruzioni operative minime e vincolo di riservatezza (contrattuale o legale) per chiunque tratti dati;

16. awareness e formazione (anche breve e documentata) su phishing, gestione credenziali, invio documenti, errori frequenti (es. destinatario errato) e segnalazione incidenti;

17. obbligo di comunicare al Titolare senza ingiustificato ritardo (nei termini del DPA) qualsiasi violazione o sospetto evento (furto device, ransomware, invio errato, accessi anomali);

18. registro minimo dei fornitori IT (se presenti) che possono accedere ai dati (es. assistenza gestionale/cloud);

19. verifica periodica dell'efficacia delle misure, almeno su base annuale e adozione di azioni correttive in caso di gap.