Accordo integrativo per il trattamento dei dati per conto del Committente

tra

_____

(“**Committente**”)

e

Brainlab Italia s.r.l., Via Monte di Pietá 21, 20121 Milano, Italia
(„**Appaltatore**”, congiuntamente definiti “**Parti**”)

Premessa

Il presente accordo disciplina le attività dell’Appaltatore in relazione all’installazione di componenti hardware e software, nonché alla manutenzione, riparazione, formazione, all’accesso remoto, alla diagnostica e a tutti gli altri lavori di assistenza ai prodotti dell’Appaltatore forniti al Committente a sostegno dell’erogazione di servizi sanitari e nell’ambito dei quali i dipendenti dell’Appaltatore o terzi da quest’ultimo incaricati possano entrare in contatto con dati personali del Committente. L'accordo di base riguardante tali attività o prestazioni viene di seguito denominato Contratto principale.

Il presente Accordo integrativo viene stipulato in conformità al Contratto principale e vale per lo stesso periodo di quest’ultimo.

1. Definizioni

Ai fini del presente Accordo valgono le seguenti definizioni:

Con “**Paese terzo con livello adeguato di protezione dei dati**” s’intende ogni Stato al di fuori del SEE riconosciuto dalla Commissione Europea in grado di fornire un livello adeguato di protezione dei dati in virtù della propria legislazione nazionale o di impegni internazionali da esso assunti;

Con “**GDPR**” s’intende il Regolamento (UE) 2016/679 del 27 aprile 2016 emanato dal Parlamento europeo e dal Consiglio relativamente alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);

Con “**Istruzione**” s’intende una disposizione scritta del Committente relativamente ad una determinata modalità di trattamento dei dati personali volta alla loro protezione (ad esempio anonimizzazione, blocco, cancellazione, diffusione) da parte dell’Appaltatore.

“Dati personali”, “Titolare del trattamento”, “Incaricato del trattamento”, “Trattamento/elaborazione”, “Interessato”, “Misure tecnico-organizzative”, “Autorità di controllo” o **“Trattamento per conto di un responsabile”** sono definizioni rilevabili dal GDPR.

2. Oggetto e responsabilità

L’Appaltatore tratterà i dati personali per conto del Committente. Oggetto dell’incarico saranno le attività descritte nel Contratto principale e nei relativi allegati, e in particolare nella Descrizione delle prestazioni. Nell’ambito del presente Accordo integrativo, spetta unicamente al Committente assicurare il rispetto delle leggi in materia di protezione dei

dati personali, in particolare la liceità della trasmissione dei dati all'Appaltatore, nonché la liceità del trattamento degli stessi da parte dell'Appaltatore.

3. Specificazione del contenuto dell'incarico

3.1 Finalità, tipologia e portata della raccolta, del trattamento e/o dell'utilizzo dei dati personali nell'ambito dell'incarico sono descritti nel Contratto principale, al quale si fa esplicito riferimento in materia.

3.2 Le tipologie di categorie dei dati personali raccolti e/o trattati, nonché le categorie degli Interessati dal trattamento dei dati personali nell'ambito del presente incarico, sono descritti nell'Allegato 1 e/o nel Contratto principale, al quale si fa esplicito riferimento in materia.

4. Potere di istruzione del Committente

4.1 Il Committente si riserva, nell'ambito di quanto specificato nel presente Accordo, il diritto di decidere tipologia, portata e procedure per il trattamento dei dati, che lo stesso potrà concretizzare attraverso specifiche istruzioni. Qualsiasi modifica all'oggetto del trattamento e alle procedure andrà concordata e documentata di comune accordo.

4.2 L'Appaltatore informerà il Committente qualora ritenga che un'istruzione violi le disposizioni in materia di protezione dei dati personali. L'Appaltatore ha il diritto di sospendere la messa in atto dell'istruzione in questione fino a quando questa non verrà confermata o modificata dal Committente.

5. Doveri dell'Appaltatore

5.1 Se non consentito per legge o per effetto di altre disposizioni (ad es. per consenso dell'Interessato), l'Appaltatore provvederà a raccogliere, elaborare o utilizzare i dati solo per conto del Committente e in conformità alle istruzioni di quest'ultimo, ma non per i propri scopi. L'Appaltatore provvederà a rettificare, cancellare, correggere o bloccare i dati personali da esso trattati su ordine del Committente soltanto dietro istruzioni di quest'ultimo. Nel caso in cui un Interessato contatti direttamente l'Appaltatore chiedendo la rettifica o cancellazione dei propri dati, l'Appaltatore inoltrerà immediatamente tale richiesta al Committente.

5.2 In singoli casi l'Appaltatore ha il diritto di utilizzare i dati, di cui è entrato in possesso nell'ambito dei servizi di assistenza forniti, in forma tale da prevenire, da parte dei propri dipendenti, ogni riconduzione alla persona dell'Interessato (a titolo d'esempio, un paziente, un medico o un dipendente dell'ospedale). L'utilizzo avverrà allo scopo di: 1) adempiere ad obblighi di legge (ad es. l'obbligo di monitoraggio dei prodotti e di rendicontazione) oppure di: 2) garantire gli interessi legittimi dell'Appaltatore e del Committente, in particolare ai fini del miglioramento della qualità e della funzionalità dei prodotti dell'Appaltatore attraverso l'uso di dati di assistenza selezionati (ad es. immagini di TAC o RM spersonalizzate), tra l'altro per le verifiche di nuove versioni di prodotti. Sono escluse le ulteriori restrizioni contenute nel presente Accordo per il trattamento dei dati personali nell'ambito dell'incarico.

5.3 Il trattamento avverrà soltanto su indicazione del Committente, tranne qualora l'Appaltatore non vi sia costretto in base al diritto dell'Unione Europea o di uno Stato membro cui egli sia soggetto, nel qual caso l'Appaltatore informerà il Committente di tale obbligo di legge prima del trattamento stesso, a meno che non sia la legge stessa a vietare tale comunicazione per motivi importanti di interesse pubblico (cfr. Art. 28 c. 3 lett. a) GDPR).

5.4 A meno che non sia vietato dalle leggi in vigore o da una richiesta ufficiale, l'Appaltatore è tenuto a notificare immediatamente al Committente qualsiasi richiesta di accesso o

sequestro dei dati personali del Committente da parte di uffici pubblici, autorità preposte alla protezione dei dati o forze dell'ordine.

5.5 Prima di accordare l'accesso ai dati personali, l'Appaltatore obbligherà al segreto e alla riservatezza dei dati i soggetti incaricati del trattamento dei dati personali e provvederà a formarli sulle norme disciplinanti in materia di protezione dei dati valide per l'Appaltatore stesso. Tra le stesse rientra, in caso di necessità, anche l'obbligo degli Interessati di osservare l'eventuale segreto professionale (derivato) esistente (ad es. in caso di trattamento di dati provenienti da ospedali o da medici di base), oppure la riservatezza delle telecomunicazioni, nella misura in cui siano state concordate nel Contratto principale prestazioni di questo tipo. Il Committente adotterà tutte le misure necessarie in misura conforme al diritto etico e professionale, provvedendo ad informare e istruire adeguatamente l'Appaltatore.

5.6 Qualora previsto dalla legge, l'Appaltatore nominerà un Responsabile della protezione dei dati, mettendo a disposizione del Committente i dati per contattarlo per tutto il periodo di validità del Contratto principale.

5.7 L'Appaltatore provvederà ad informare il Committente in caso di violazioni delle istruzioni o disposizioni a tutela dei dati personali del Committente da parte dell'Appaltatore o di persona assunta dallo stesso.

Qualora i dati personali vadano persi, siano trasmessi illecitamente o divulgati a terzi in altro modo illecito ai sensi degli Artt. 33 e 34 del GDPR, il Committente va informato immediatamente di tali evenienze. L'Appaltatore provvederà, d'accordo con il Committente, ad adottare adeguate misure atte a proteggere i dati e a mitigare eventuali conseguenze negative a danno degli Interessati.

Inoltre, l'Appaltatore informerà immediatamente il Committente in caso di gravi malfunzionamenti nel normale svolgimento dell'attività, nonché in caso di sospetta violazione dei dati o di altre anomalie nel trattamento dei dati personali.

L'Appaltatore è a conoscenza che il Committente è tenuto a documentare eventuali violazioni alla protezione dei dati personali e, se del caso, ad informarne le autorità di controllo e/o l'Interessato. Nel caso e nella misura in cui si siano verificate tali violazioni, l'Appaltatore sosterrà il Committente in maniera adeguata come previsto dall'Art. 28 c. 3 lett. f) del GDPR nell'assunzione delle proprie responsabilità, affinché il Committente possa adempiere puntualmente ai propri obblighi. L'Appaltatore informerà il Committente della violazione e fornirà i seguenti dati qualora ne sia in possesso:

a) una descrizione della natura della violazione della protezione di dati personali, per quanto possibile con indicazione delle categorie e del numero approssimativo di Interessati coinvolti, nonché delle categorie interessate e del numero approssimativo di record di dati personali coinvolti;

b) nome e recapito del Responsabile della protezione dei dati o di altro ufficio competente per ulteriori informazioni;

c) una descrizione delle conseguenze presunte della violazione della protezione di dati personali;

d) una descrizione delle misure adottate o proposte dal Committente al fine di risolvere la violazione della protezione dei dati personali ed eventualmente delle misure volte a mitigare le possibili conseguenze avverse.

5.8 L'Appaltatore informerà prontamente il Committente di qualsiasi attività di monitoraggio e misura intrapresa dalle autorità di controllo in relazione al trattamento dei dati personali del Committente stesso.

5.9 Qualora il Committente sia tenuto, in base alle vigenti disposizioni di legge in materia di protezione dei dati, a fornire informazioni sulla raccolta, sul trattamento o sull'utilizzo di dati, l'Appaltatore dovrà mettere a disposizione del Committente tutte le informazioni relative.

5.10 L’Appaltatore provvederà al monitoraggio del rispetto degli obblighi suddetti durante l’espletamento del trattamento dei dati oggetto di incarico.

5.11 L’Appaltatore terrà un elenco scritto di tutte le categorie di attività di trattamento svolte per conto del Committente così come previsto dall’Art. 30 c. 2 del GDPR.

5.12 In caso di necessità, l’Appaltatore fornirà il supporto previsto dall’Art. 28 c. 3 lett. f) del GDPR nella redazione di una valutazione delle conseguenze in relazione alla protezione dei dati come previsto dall’Art. 35 del GDPR nonché, ove opportuno, nella consultazione preventiva delle autorità di controllo come previsto dall’Art. 36 del GDPR. Su richiesta del Committente, l’Appaltatore metterà a disposizione di quest’ultimo le necessarie informazioni e documentazioni. I costi supplementari derivanti da tali prestazioni saranno rimborsati all'Appaltatore.

5.13 L’Appaltatore adotterà misure appropriate in caso di abuso, perdita e ripristino dei dati (ad es. tramite la predisposizione di backup come previsto dagli standard industriali), nella misura prevista dal Contratto principale.

6. Sicurezza del trattamento dei dati

6.1 Nell’ambito delle proprie responsabilità, l’Appaltatore doterà la propria organizzazione interna in conformità con tutti i requisiti applicabili in materia di protezione e sicurezza dei dati. L’Appaltatore provvederà a mettere in atto, aggiornare e monitorare le misure tecnico-organizzative affinché sia garantita un’adeguata protezione dei dati del Committente contro abusi e perdite, in conformità con quanto previsto dalle leggi in vigore.

6.2 L’Appaltatore metterà in atto tutte le misure tecnico-organizzative conformi ai requisiti di cui all’Art. 32 del GDPR, in modo da garantire un livello di protezione adeguato al rischio e da sostenere il Committente nell’adempimento degli obblighi previsti dall’Art. 32 del GDPR (Art. 28 c. 3 lett. c), f) GDPR).

6.3 In questo contesto, l’Appaltatore dovrà tenere conto dello stato dell'arte, dei costi di attuazione, nonché di natura, portata, circostanze e finalità del trattamento, oltre che della diversa probabilità di accadimento e gravità dei rischi per i diritti e le libertà delle persone fisiche. Tra questi rientrano adeguate misure, ad esempio per il controllo di ingressi, utenti, accessi, trasmissioni, inserimenti, ordini, disponibilità e separazione a seconda delle finalità, nonché:

a) la pseudonimizzazione e la crittografia dei dati personali;

b) la capacità di garantire a lungo termine riservatezza, integrità, disponibilità e resilienza dei sistemi e servizi associati al trattamento;

c) la capacità di pronto ripristino della disponibilità dei dati personali e dell’accesso agli stessi in caso di incidenti fisici o tecnici;

d) una procedura che consenta di esaminare, verificare e valutare regolarmente l'efficacia delle misure tecnico-organizzative a garanzia della sicurezza del trattamento.

6.4 L’Allegato 2 contiene una descrizione e le specifiche delle misure tecnico-organizzative indispensabili che l’Appaltatore dovrà attuare nell’ambito del presente Accordo. Esse potranno essere integrate con ulteriore documentazione.

6.5 Le misure tecnico-organizzative sono soggette al progresso e all’evoluzione della tecnologia. L’Appaltatore potrà intraprendere adeguate misure alternative che non dovranno tuttavia essere inferiori al livello di sicurezza delle misure previste. Ogni modifica sostanziale andrà documentata.

6.6 L’Appaltatore sosterrà il Committente come previsto dall’Art. 28 c. 3 lett. e) del GDPR con adeguate misure tecnico-organizzative, per quanto possibile e ragionevole, ai fini dell’adempimento dell’obbligo del Committente verso gli Interessati di cui al comma 3 del GDPR, ad es. per quanto riguarda l’informazione e il diritto di informazione degli Interessati, la rettifica e la cancellazione dei dati, la limitazione del trattamento o del diritto

alla portabilità dei dati e di quello di opposizione al trattamento. I costi supplementari derivanti da tali prestazioni saranno rimborsati all'Appaltatore.

7 Accesso remoto e per l'assistenza

7.1 Per gli interventi di accesso remoto e finalizzati all'assistenza valgono le seguenti norme integrative, sempre che le attività di trattamento riguardino determinate categorie di dati personali o il Committente sia soggetto al segreto professionale.

7.2 Sempre che nel caso particolare non sia possibile escludere l'accesso a dati personali, gli interventi in modalità remota avverranno esclusivamente col consenso del personale preposto del Committente.

7.3 Il personale dell'Appaltatore ricorrerà a adeguate procedure di identificazione e cifratura.

7.4 Gli interventi in modalità remota saranno documentati e registrati. Il Committente è autorizzato a controllare i lavori di verifica e manutenzione prima, durante e dopo la loro esecuzione. In questo caso egli dovrà osservare le disposizioni di cui al paragrafo 9. In caso di interventi in modalità remota, il Committente – sempre che ciò sia tecnicamente possibile e realizzabile in considerazione della natura delle prestazioni effettuate – è autorizzato a seguirle da un monitor di controllo e a sospenderle in qualsiasi momento.

7.5 L'accesso remoto ai relativi sistemi avverrà solo in base al principio della necessità di sapere.

7.6 Le attività di individuazione e risoluzione dei problemi per cui sia necessario l'accesso ai dati personali richiederanno il previo consenso del personale preposto del Committente. Qualora a tal fine fossero effettuate delle copie, l'Appaltatore provvederà a modificarle dopo l'eliminazione del problema in modo tale da non poter più produrre alcun riferimento personale, ovvero a cancellarle, sempre che non sia necessaria la conservazione (immutata) dei relativi dati per altri motivi (ad es. quali prove degli interventi effettuati e della loro conformità). I dati personali potranno essere utilizzati soltanto allo scopo di individuare e risolvere eventuali problemi e pertanto non potranno essere copiati su dispositivi di archiviazione mobili (palmari, chiavette USB o dispositivi simili) senza opportuna crittografia. Ai fini di cui sopra resta inalterato il paragrafo 5.2.

7.7 In singoli casi può accadere che gli interventi di individuazione e risoluzione dei problemi avvengano senza che sia stato preventivamente ottenuto il consenso, quando ciò si renda necessario per la prestazione di servizi contrattuali (in particolare allo scopo di effettuare riparazioni). Il Committente rilascia con il presente il proprio consenso generico a tali interventi.

7.8 L'accesso remoto nonché qualsiasi attività necessaria in quest'ambito, e in particolare operazioni quali cancellazione, trasferimento di dati o individuazione e risoluzione dei problemi, saranno condotti nel rispetto di misure tecnico-organizzative volte alla protezione dei dati personali.

8. Diritti e doveri del Committente

8.1 Per quanto riguarda i dati oggetto di trattamento, Committente e Appaltatore sono responsabili del rispetto delle leggi vigenti per ciascuno di essi in materia di protezione dei dati.

8.2 Il Committente determinerà le misure per la restituzione dei supporti informatici affidati e/o per la cancellazione dei dati memorizzati al termine dell'incarico. Qualora non si proceda ad alcuna determinazione in tal senso, i dati verranno riconsegnati al Committente oppure cancellati. Qualora, sulla base di particolari decisioni, si dia corso alla cancellazione dei dati, questa va confermata al Committente da parte dell'Appaltatore con indicazione della data. La restituzione o cancellazione dei dati memorizzati sarà possibile soltanto qualora non sussistano obblighi di legge o normativi che vincolino l'Appaltatore alla conservazione. Ai fini di cui sopra resta inalterato il paragrafo 5.2.

9. Diritti di controllo

9.1 Su richiesta, l'Appaltatore metterà a disposizione del Committente la prova documentale dell'attuazione delle misure tecnico-organizzative e degli ulteriori obblighi previsti dall'Art. 28 del GDPR.

9.2 Il Committente potrà, d'intesa con l'Appaltatore, effettuare un controllo dell'incarico oppure incaricare supervisori di effettuarlo prima dell'inizio del trattamento dei dati e con modalità ragionevoli durante l'intera durata dell'incarico. L'Appaltatore potrà ottemperare a tali richieste in qualsiasi momento prima dell'inizio e durante la durata del trattamento mediante opportune autodichiarazioni, certificazioni in corso di validità, rapporti o estratti di organi indipendenti (ad es. da parte di revisori esterni, attività di revisione interne, responsabili della protezione dei dati, ufficio addetto alla sicurezza informatica, revisori della protezione dei dati o della qualità), o mediante un'adeguata certificazione nell'ambito di un'ispezione sulla sicurezza informatica o sulla protezione dei dati.

9.3 Qualora il Committente nutra ragionevoli dubbi circa l'autodichiarazione o la valutazione presentata dall'Appaltatore, esso ha il diritto di effettuare, a proprie spese, un'adeguata ispezione presso la sede dell'Appaltatore al fine di verificare il rispetto delle misure tecnico-organizzative e degli altri obblighi di cui all'Art. 28 del GDPR. Tale ispezione andrà annunciata perlomeno con due settimane di anticipo e potrà essere condotta solo durante il normale orario di ufficio, senza interferire con l'attività aziendale. Il Committente dovrà sostenere tutti i costi supplementari risultanti all'Appaltatore da una tale ispezione.

9.4 Su richiesta scritta del Committente, l'Appaltatore metterà a disposizione di quest'ultimo, entro un opportuno lasso di tempo, le informazioni e documentazioni necessarie per l'ispezione.

10. Subappaltatori

10.1 L'Appaltatore è autorizzato a incaricare subappaltatori e altre imprese dell'esecuzione dei propri obblighi contrattuali.

10.2 L'Appaltatore si assicurerà, stipulando accordi coi subappaltatori, che ad essi siano imposti perlomeno sostanzialmente gli stessi obblighi assunti dall'Appaltatore in base al presente Accordo integrativo prima che sia loro concesso l'accesso ai dati personali del Committente per l'esecuzione dell'incarico. Qualora un subappaltatore svolga le prestazioni concordate al di fuori dell'UE o del SEE e di un Paese terzo con adeguato livello di protezione dei dati, l'Appaltatore si assicurerà mediate opportune misure del rispetto delle disposizioni EU in materia di protezione dei dati.

10.3 Su richiesta, l'Appaltatore metterà a disposizione un elenco dei subappaltatori coinvolti nelle attività di trattamento dei dati effettuate ai sensi del presente Accordo. L'Appaltatore informerà il Committente di qualsiasi modifica prevista riguardante l'aggiunta o la sostituzione di altri subappaltatori, dandogli la possibilità di contestare tali modifiche, purché con obiezioni giustificate. Ove il Committente non approvi un nuovo subappaltatore, Committente e/o Appaltatore potranno recedere tramite semplice comunicazione scritta, cioè senza rispettare un termine di preavviso, dalle prestazioni interessate dal trattamento in questione per le quali debba essere nominato un ulteriore subappaltatore, nonché da ogni altro obbligo di risarcimento danni o rimborso spese.

10.4 Il Committente è autorizzato a verificare i subappaltatori dell'Appaltatore come previsto al par. 9, previa consultazione e d'accordo con lo stesso, incaricando sin d'ora l'Appaltatore della verifica a proprio nome, confermando il proprio consenso affinché la stessa possa essere condotta soltanto dall'Appaltatore e possa risultare effettuata anche mediante presentazione di certificazioni in corso di validità, rapporti o estratti di enti indipendenti (ad es. revisori esterni, ispezioni interne, Responsabili della protezione dei dati, ufficio sicurezza informatica, revisori della protezione dei dati o della qualità), o mediante un'adeguata certificazione nell'ambito di un'ispezione sulla sicurezza informatica o sulla

protezione dei dati. Prima della trasmissione dei relativi documenti e informazioni del subappaltatore, il Committente dovrà eventualmente stipulare uno o più accordi di riservatezza col subappaltatore e/o con l'Appaltatore in questione.

10.5 Quanto specificato al paragrafo 10 non vale qualora l'Appaltatore affidi a terzi servizi accessori; tali servizi accessori comprendono, tra l'altro, servizi postali, di spedizione e di installazione.

11. Trasferimento dei dati al di fuori del SEE

11.1 Il trattamento avverrà di regola in uno Stato membro dell'Unione europea, in uno Stato dello Spazio Economico Europeo oppure in uno Stato terzo con adeguato livello di protezione dei dati (compresi gli Stati Uniti, purché in presenza di una relativa certificazione Privacy Shield). I trattamenti in altro Stato ("**Stato terzo**") sono ammessi, purché nel rispetto dei requisiti per la trasmissione internazionale di dati personali come previsto dall'Art. 44 e segg. del GDPR.

11.2 Se e nella misura in cui: 1) Committente e Appaltatore si trovino all'interno dello Spazio Economico Europeo ("**SEE**") mentre il subappaltatore dell'Appaltatore è situato in uno Stato terzo e 2) l'Appaltatore stipuli accordi con i subappaltatori sulla base delle clausole contrattuali standard dell'UE per gli Appaltatori ("**SCC**"), il Committente autorizza sin d'ora l'Appaltatore a concludere tali accordi sul trattamento in subappalto con i subappaltatori, purché ciò sia possibile per l'Appaltatore, anche in nome e per conto dello stesso Committente. Su richiesta, l'Appaltatore dovrà informare il Committente nonché le parti interessate dell'esistenza e dello stato dei contratti con clausole contrattuali tipo stipulati nelle circostanze suddette. La conclusione dei relativi contratti è a discrezione dell'Appaltatore.

12. Responsabilità

12.1 Il Committente dovrà manlevare e tenere indenne l'Appaltatore da qualsiasi pretesa di terzi o da altri danni e responsabilità derivanti da: 1) qualsiasi violazione degli obblighi del Committente ai sensi del presente Accordo e/o altre violazioni delle leggi applicabili in materia di protezione dei dati, e/o 2) qualsiasi violazione da parte dell'Appaltatore delle leggi applicabili in materia di protezione dei dati nella misura in cui tali violazioni riguardino l'esecuzione dei termini del presente Accordo o altre istruzioni del Committente. Ciò non vale nel caso in cui il Committente non sia responsabile delle circostanze all'origine di tali responsabilità. Resta invariato l'Art. 82 (5) del GDPR.

12.2 Qualora il Contratto principale preveda limitazioni o esclusioni di responsabilità o obbligo di indennizzo dell'Appaltatore, tali limitazioni o esclusioni valgono anche per eventuali pretese avanzate nei confronti dell'Appaltatore in relazione al presente Accordo integrativo.

12.3 Le norme sulla responsabilità o sulla liberatoria previste nel Contratto principale restano invariate per quanto non specificato.

13. Riservatezza

Le Parti s'impegnano a trattare con riservatezza qualsiasi conoscenza di segreti commerciali e aziendali acquisita nell'ambito del rapporto contrattuale. Tale obbligo continuerà ad avere effetto anche oltre il termine dei singoli incarichi e/o della relazione commerciale.

14. Dovere di informazione, requisito della forma scritta, scelta del diritto applicabile

14.1 Qualora presso l'Appaltatore fossero messi a rischio i dati personali del Committente a causa di un pignoramento o sequestro di beni, di una procedura d'insolvenza o di

concordato o altri eventi o misure intraprese da terzi, l'Appaltatore dovrà informarne immediatamente il Committente. L'Appaltatore informerà altresì tutte le parti interessate che la sovranità e la proprietà dei dati sono esclusivo appannaggio del Committente.

14.2 Eventuali modifiche e integrazioni al presente Accordo integrativo necessitano della forma scritta e della dicitura espressa che si tratta di modifiche ovvero integrazioni al presente Accordo integrativo. La modifica stessa del requisito della forma deve avvenire per iscritto.

14.3 Il presente Accordo integrativo e qualsiasi controversia relativa alla sua conclusione ed esecuzione sono disciplinati esclusivamente dal diritto della Repubblica federale tedesca, con esclusione della Convenzione di Vienna delle Nazioni Unite sulla compravendita internazionale di merci dell'11/04/1980. Foro competente per eventuali controversie tra le Parti in relazione al presente Accordo integrativo è il Tribunale regionale di Monaco di Baviera I *(Landgericht München I)*.

Per l'Appaltatore:

[*Nome*]
[*Funzione*]
[*Luogo e data*]

_____

Per il Committente:

[*Nome]*
[*Funzione*]
[*Luogo e data*]

_____

<u>Allegato 1</u>: Tipologie di categorie di dati e categorie di Interessati nell'ambito della raccolta, del trattamento e/o dell'uso di dati personali

1. Tipologie di dati personali raccolti e/o utilizzati

- Dati anagrafici personali (ad es. nome e cognome, data di nascita, sesso, codice identificativo paziente)
- Dati di contatto (ad es. telefono, e-mail)
- Dati anagrafici contrattuali (ad es. relazione contrattuale, interesse a prodotti o contratti)
- Storico cliente
- Dati di fatturazione e pagamento (ad es. conto corrente bancario)
- Dati di pianificazione e gestione (ad es. informazioni sull'infrastruttura del cliente)
- Dati di valutazione (di terzi, ad es. agenzie di rating, o da elenchi pubblici)
- Informazioni di carattere medico e fotografie dei pazienti

2. Categorie di persone soggette al trattamento di dati personali

- Clienti
- Clienti potenziali
- Abbonati
- Pazienti del cliente

<u>Allegato 2</u>: Sicurezza del trattamento dei dati

Il presente allegato descrive le misure tecnico-organizzative e le procedure minime da rispettare a cura dell'Appaltatore al fine di tutelare la sicurezza dei dati personali creati, raccolti, ricevuti o ottenuti in altro modo e garantire la costante riservatezza, integrità, disponibilità e resilienza dei sistemi e servizi di trattamento.

Misure tecnico-organizzative

I. Riservatezza, Art. 32 c. 1 lett. b) GDPR

1. Controllo degli accessi fisici

Misure atte a vietare alle persone non autorizzate di accedere alle apparecchiature per il trattamento dei dati con le quali vengono elaborati o utilizzati dati personali

- ☒ Definizione di una cerchia ristretta di persone autorizzate all'accesso
- ☒ Lucchetti di sicurezza
- ☒ Sistema di chiusura manuale (ad es. stanza che può essere chiusa a chiave, armadio) - applicabile specificamente per l'home office
- ☒ Sistemi di chiusura mediante chip card/ transponder
- ☒ Videosorveglianza degli accessi

2. Controllo dell'accesso informatico

Misure atte ad impedire l'utilizzo dei sistemi di trattamento dei dati da parte di persone non autorizzate

- ☒ Concessione di autorizzazioni utente funzionali e/o limitate nel tempo
- ☒ Politica sulle password comprendente lunghezza, assegnazione e modifica delle stesse
- ☒ Autenticazione con nome utente e password
- ☒ Utilizzo di sistemi anti-intrusione e per la prevenzione delle intrusioni
- ☒ Utilizzo di software antivirus
- ☒ Utilizzo di un firewall hardware
- ☒ Utilizzo di filtri e-mail anti-spam
- ☒ Creazione di profili utente
- ☒ Allocazione di profili utente ai sistemi informatici
- ☒ Utilizzo della tecnologia VPN
- ☒ Utilizzo di software centralizzati di gestione smartphone (ad es. per l'eliminazione esterna dei dati)
- ☒ Utilizzo di un firewall software
- ☒ Crittografia del disco rigido dei portatili
- ☒ Sistema di log-in supplementare per le diverse applicazioni

3. Controllo degli accessi

Misure atte a garantire che le persone autorizzate a utilizzare un sistema di trattamento dei dati possano accedere esclusivamente ai dati per cui è loro consentito l'accesso e che i dati personali non possano essere letti, copiati, modificati o rimossi senza autorizzazione durante la loro elaborazione e il loro utilizzo e successivamente al salvataggio

- ☒ Definizione delle autorizzazioni all'accesso
- ☒ Gestione dei diritti tramite amministratore di sistema
- ☒ Rilascio restrittivo delle autorizzazioni di amministratore
- ☒ Requisito dell'identificazione della password
- ☒ Eliminazione fisica dai supporti dati prima del riutilizzo
- ☒ Conservazione sicura dei supporti dati
- ☒ Registrazione dei trasferimenti di dati
- ☒ Registrazione degli accessi alle diverse applicazioni
- ☒ Eliminazione sicura dei supporti dati
- ☒ Definizione di processi per il rilascio, il controllo e la revoca delle autorizzazioni

4. Controllo della gestione separata

Misure atte a garantire che i dati raccolti per finalità diverse possano essere trattati separatamente

- ☒ Archiviazione fisicamente separata su sistemi o supporti dati specifici
- ☒ Separazione logica dei client (da parte del software)
- ☒ Creazione di una logica delle autorizzazioni
- ☒ Separazione dei sistemi di produzione da quelli di verifica

II. Pseudonimizzazione e crittografia, Art. 32 c. 1 lett. a) GDPR

Misure per la pseudonimizzazione e la crittografia dei dati personali (se non già presenti al par. I)

- ☒ Utilizzo di tecniche di pseudonimizzazione e anonimizzazione anche in ambito R&S
- ☒ Crittografia secondo gli standard previsti per i dati particolarmente sensibili (at rest) nei singoli servizi
- ☒ Presenza di un insieme di regole per la cifratura dei dati

III. Integrità, Art. 32 c. 1 lett. b) GDPR

1. Controllo della diffusione

Misure volte a garantire che i dati personali, durante la trasmissione elettronica o durante il trasporto o l'archiviazione su supporti dati, non possano essere letti, copiati, modificati o rimossi senza autorizzazione e che si possa verificare e constatare in quali punti è previsto un trasferimento dei dati personali tramite dispositivi di trasmissione dati

- ☒ Installazioni di linee dedicate e/o tunnel VPN
- ☒ Formazione dei dipendenti sulla protezione dei dati
- ☒ Documentazione dei destinatari dei dati
- ☒ Una direttiva disciplina chiaramente come reagire in caso di smarrimento di un supporto dati
- ☒ Crittografia del disco rigido dei portatili

2. Controllo degli input

Misure volte a garantire la possibilità di verificare e confermare a posteriori se e da chi sono stati inseriti, modificati o rimossi i dati personali nei relativi sistemi di trattamento

- ☒ Assegnazione dei diritti di inserimento, modifica e cancellazione di dati sulla base di una logica delle autorizzazioni
- ☒ Registrazione di inserimenti, modifiche e cancellazioni dei dati, per quanto consentito dai sistemi

IV. Disponibilità e resilienza, Art. 32 c. 1 lett. b) e c) GDPR

1. Controllo della disponibilità

Misure volte a garantire la protezione dei dati personali contro la distruzione o la perdita accidentali, incluse quelle per il ripristino in caso di incidenti fisici o tecnici

- ☒ Gruppo di continuità (UPS)
- ☒ Climatizzazione nei locali del server
- ☒ Impianti antincendio e antifumo
- ☒ Programma di backup e ripristino
- ☒ Predisposizione di un piano di emergenza
- ☒ Utilizzo di firewall e scanner antivirus
- ☒ Gestione delle patch
- ☒ Sistema adeguato di spegnimento incendi nei locali del server
- ☒ Test di recupero dati
- ☒ Conservazione esternalizzata dei backup in luogo sicuro

V. Procedure di valutazione e accertamento periodici, Art. 32 c. 1 lett. d) GDPR

1. Gestione della protezione dei dati

Altre misure, in particolare quelle organizzative ai fini della protezione dei dati personali

- ☒ Descrizione delle prescrizioni vigenti in materia di protezione dei dati delle direttive e istruzioni vincolanti
- ☒ Revisioni periodiche dei provvedimenti in materia di protezione dei dati e delle norme quadro esistenti
- ☒ Costituzione di informazioni aggiornate in materia di sicurezza e falle informatiche
- ☒ Eventuale coinvolgimento del Responsabile della protezione dei dati nelle nuove procedure rilevanti in materia di trattamento dei dati

2. Incident Response Management

Altre misure di gestione in caso di incidenti associati alla protezione dei dati

- ☒ Norma quadro di comportamento in caso di incidenti di sicurezza informatica e di protezione dei dati
- ☒ Procedura di notifica di eventuali incidenti
- ☒ Procedure di Business Continuity Management

3. Preimpostazioni per la protezione dei dati, Art. 25 c. 2 GDPR

Misure atte a garantire che le preimpostazioni siano conformi ai diritti dell'Interessato (privacy by default)

- ☒ Implementazione di preimpostazioni in materia di protezione dei dati
- ☒ Limitazione alla raccolta dei dati
- ☒ Utilizzo della pseudonimizzazione o anonimizzazione dei dati personali anche in ambito R&S

4. Controllo dell'incarico

Misure atte a garantire che i dati personali trattati nell'ambito dell'incarico possano essere elaborati solo in conformità alle istruzioni del Committente

- ☒ Scelta dell'Appaltatore secondo criteri di *due diligence* (in particolare in materia di sicurezza dei dati)
- ☒ Istruzioni documentate all'Appaltatore (ad es. tramite contratto di esecuzione dell'incarico)
- ☒ L'Appaltatore ha nominato, se necessario, un Responsabile della protezione dei dati
- ☒ Formazione del personale
- ☒ Controlli preventivi dell'Incaricato del trattamento, in particolare verifica preventiva della documentazione sulle misure di sicurezza adottate dall'Appaltatore
- ☒ Dovere dell'Incaricato del trattamento di impegnare i propri dipendenti alla riservatezza sui dati
- ☒ Accordo con l'Appaltatore sull'efficacia dei diritti di controllo
- ☒ Elenco delle attività di esecuzione dell'incarico