ALLEGATO II

Oggetto: Addendum contrattuale - Responsabile del trattamento dei dati personali ex art. 28 Reg. UE 679/2016 con funzioni di Amministratore di Sistema

La società **ASP Magiera Ansaloni** con sede legale in **Via Carlo Marx 10, 42010 Rio Saliceto (RE), P.IVA 01327630354, dati di contatto Cliente** _____, in persona del legale rappresentante pro-tempore (d'ora in avanti *"il Committente" o "il Titolare del trattamento"*)

PREMESSO

a) che a seguito dell'entrata in vigore del Reg. UE n. 679 del 24 maggio 2016 (GDPR), sono state introdotte all'interno del quadro normativo europeo sulla protezione dei dati personali alcune novità di rilievo;
b) che il committente ha commissionato ad Advenias S.r.l. con sede in Via Lercaro 3 – 40033 Casalecchio di Reno (BO) (d'ora in avanti *"il fornitore"*) la prestazione di servizi relativi alla fornitura, implementazione, parziale gestione e manutenzione di software – oggetto di accordi intercorsi - (**contratto n. 180CA602**) e che tali attività presuppongono per la loro esecuzione il trattamento di dati personali e particolari di interessati verso cui il committente stesso assume la veste di Titolare del trattamento, così come definito dall'art. 4 par. 7 del Reg. UE 679/2016;
c) che il contratto di cui al punto b) disciplina la materia, la durata, la natura e le finalità del trattamento, il tipo di dati personali, le categorie di interessati, gli obblighi e i diritti del titolare del trattamento;
d) che il fornitore tratta tali dati per conto del committente unicamente al fine di dare esecuzione ai servizi oggetto degli accordi suddetti.
e) che il contratto in essere con il Titolare comprende in particolare le seguenti operazioni di trattamento dei dati:
    - Creazione credenziali iniziali di autorizzazione e autenticazione per il primo accesso;
    - Gestione di flussi di dati;
    - Gestione data base;
    - Gestione sistema software
    - Monitoraggio del salvataggio periodico dei dati (backup/recovery);
    - Gestioni aggiornamento dei sistemi;

f) che è stata valutata l'esperienza, capacità e affidabilità del fornitore, anche ai fini di garantire che il trattamento dei dati personali sia svolto nel pieno rispetto delle disposizioni vigenti e delle misure di sicurezza mediante gli elementi indicati nel curriculum aziendale ed in particolare:
    - i servizi svolti;
    - le certificazioni acquisite;
    - gli anni di presenza nel settore;

PREMESSO INOLTRE CHE

- il Provvedimento a carattere generale del Garante per la protezione dei dati personali: "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema – del 27 novembre 2008" estende gli adempimenti previsti per gli amministratori di sistema anche alle funzioni nelle quali alcune operazioni di trattamento comportano particolari e più ampi privilegi per l'accesso ai dati personali, ovvero quando le attività siano esercitate in un contesto che renda tecnicamente

possibile l'accesso, anche fortuito, a dati personali, da ciò derivando la necessità di organizzare una maggiore tutela degli accessi ai dati;
- quali "*amministratori di sistema*" devono essere individuate sia le figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, sia le altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi;
- alcune delle attività tecniche affidate al fornitore elencate alla lettera e) delle premesse di cui sopra possono comportare un'effettiva capacità di azione sulle informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali;
- sono state perciò analizzate le operazioni di trattamento svolte dal fornitore, nel contesto del vigente contratto stipulato con il Titolare;
- alcune delle operazioni di trattamento possono comportare, anche involontariamente, particolari rischi;

TUTTO CIÒ PREMESSO E CONSIDERATO

preso atto che il fornitore presenta garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Reg. UE 679/2016 e garantisca la tutela dei diritti dell'interessato, mediante la firma del presente contratto **la Società ADVENIAS S.r.l. nella veste di Responsabile del trattamento ex art. 28 GDPR, con funzioni di amministratore di sistema dei dati personali oggetto dei servizi di cui in premessa, si impegna a trattare i dati per conto del Titolare in modo lecito, secondo correttezza e nel pieno rispetto di tutte le disposizioni emesse in materia di trattamento dei dati personali, nonché delle seguenti specifiche istruzioni.**

ISTRUZIONI

1. **Persone autorizzate al trattamento**. Prima di iniziare qualsiasi trattamento di dati, il fornitore deve garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza che include altresì il rispetto di eventuali ulteriori istruzioni ricevute ai sensi degli artt. 29 e 32 c.4 del GDPR; tali istruzioni dovranno, ovviamente, essere anche coerenti con quelle indicate nel presente documento. Nei confronti di ciascuna persona dovrà essere effettuato un adeguato piano di formazione.

2. **Clausola di riservatezza.** I dati sono da considerarsi quali informazioni riservate del committente. Su questa base:
   a. il fornitore non potrà in alcun caso comunicare i dati a terzi, a meno che ciò sia necessario per l'assolvimento di un obbligo derivante da una legge;
   b. nel caso in cui il fornitore riceva richiesta o intimazione di comunicare informazioni personali o particolari del processo di trattamento di dati qui regolato, da parte di una pubblica autorità o da parte dell'autorità giudiziaria, dovrà provvedere a dare di ciò pronta notizia al committente e si impegna a seguire le istruzioni del committente;
   c. non deve in alcun modo trasferire dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il fornitore. In tal caso, il fornitore informa il committente circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

3. **Finalità.** Il trattamento dei dati deve essere effettuato dal fornitore ai soli fini di dare esecuzione ai servizi commissionatogli. Esso si dovrà configurare, quindi, come strettamente necessario per effettuare il servizio.

4. **Privacy by design & Privacy by default.** Il fornitore deve rispettare i principi di protezione dei dati fin dalla progettazione (*privacy by design*) e protezione dei dati per impostazione predefinita (*privacy by default*) di cui all'art. 25 GDPR comunicando al committente le soluzioni individuate ed adottate per rispettare tali principi (vedi successivo punto 6).

5. **Diritto di accesso**. Deve essere garantito agli interessati l'effettivo esercizio dei diritti loro riconosciuti dal GDPR, con particolare riguardo al diritto di accesso ai dati a cui occorrerà dare riscontro nelle modalità ed entro i termini di legge anche in conformità alle procedure emesse al riguardo dal committente. Il fornitore deve supportare il committente con ogni mezzo adeguato per garantire la conformità alle disposizioni relative ai diritti dell'interessato; deve inoltre assistere il committente con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo dei titolari del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato.

6. **Misure di sicurezza**. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il fornitore deve adottare idonee ed adeguate misure necessarie ai fini della sicurezza dei dati personali ai sensi dell'articolo 32 del GDPR, fra le quali, ad esempio:
   a. la pseudonimizzazione e la cifratura dei dati personali;
   b. la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
   c. la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
   d. una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento, comunicando al committente le soluzioni individuate ed adottate per rispettare tale obbligo.

7. **Assistenza al committente.** Il fornitore deve assistere il committente ai fini del rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR, tenendo conto della natura del trattamento e delle informazioni a sua disposizione.

8. **Violazione di dati personali (data breach).** Il fornitore deve implementare soluzioni atte a rilevare eventuali violazioni dei dati personali (ossia le violazioni di sicurezza che comportano 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) e, al verificarsi di tali violazioni, comunicarle tempestivamente al committente. Il fornitore s'impegna, altresì, a collaborare attivamente con il committente ai fini delle conseguenti comunicazioni all'Autorità Garante per la protezione dei dati personali e, eventualmente, agli interessati ai sensi degli artt. 33 e 34 del GDPR.

9. **Verifiche del fornitore.** Il fornitore dovrà mantenere un costante controllo in merito al fatto che i dati siano trattati in modo lecito, secondo correttezza e comunque nel rispetto delle leggi, delle disposizioni in materia di trattamento compreso il profilo relativo alla sicurezza oltre che delle istruzioni impartite. A tale proposito dovrà anche condurre verifiche periodiche da effettuare in conformità alla normativa e nel rispetto minimo delle scadenze di legge. Il fornitore si impegna inoltre a informare immediatamente il committente segnalando ogni situazione di cui venga a conoscenza che possa esporre il committente a violazioni di legge o possa generare un trattamento illecito o porre in pericolo la riservatezza e l'integrità dei dati.

10. **Verifiche del committente**. Il fornitore deve mettere a disposizione del committente tutte le informazioni necessarie per dimostrare la conformità con il GDPR e contribuire alle attività di revisione, comprese le verifiche realizzate dal committente o da un altro soggetto da questi incaricato.

11. **Restituzione dei dati.** Al termine del servizio oggetto del contratto il fornitore deve restituire e anonimizzare tutti i dati personali del committente e cancellare le eventuali copie esistenti in suo possesso.

12. **Dovere di informazione.** Il fornitore deve informare immediatamente il committente qualora, a suo parere, un'istruzione violi il regolamento europeo o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati.

13. **Valutazione d'impatto sulla protezione dei dati personali (DPIA).** Il fornitore deve assistere il committente con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di agevolare la realizzazione di valutazioni d'impatto sulla protezione dei dati personali, ai sensi dell'art. 35 del GDPR, per il trattamento in questione.

14. **Sub-responsabile.** Il fornitore può ricorrere a un altro responsabile solo previa autorizzazione scritta, specifica o generale, del committente. La presente vale quale autorizzazione scritta generale. Il fornitore è comunque sempre tenuto ad informare il committente in merito alla scelta, aggiunta o sostituzione di qualsiasi responsabile del trattamento, dando così al committente l'opportunità di valutarla, e se del caso opporvisi. Se il fornitore ricorre a un altro responsabile (sub-responsabile) per l'esecuzione di specifiche attività di trattamento per conto del committente, deve imporgli, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel presente contratto. In particolare, il fornitore deve prevedere in quest'ultimo caso garanzie sufficienti affinché il sub-responsabile metta in atto misure tecniche e organizzative adeguate al fine di soddisfare i requisiti normativi previsti. Qualora il sub-responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il fornitore conserva l'intera responsabilità dell'adempimento degli obblighi del sub-responsabile.

15. **Registro delle attività dei trattamenti.** Il fornitore deve tenere un registro delle attività dei trattamenti ai sensi dell'art. 30 c.2 del GDPR.

16. **Responsabile della protezione dei dati (DPO).** Il fornitore deve procedere, se del caso, alla designazione del responsabile della protezione dei dati (DPO) ai sensi dell'art. 37 del GDPR. Qualora il fornitore ritenga di non doversi dotare di tale figura ne fornisce adeguata e documentata motivazione al committente.

17. **GDPR Governance.** Ulteriori specificazioni tecniche e operative legate ai punti in oggetto sono consultabili all'interno del documento *GDPR Governance*, presente all'interno del software ed in constante miglioramento: una copia aggiornata del documento può sempre essere richiesta al fornitore scrivendo all'indirizzo assistenza@advenias.it

PRESCRIZIONI PARTICOLARI PER IL RISPETTO DEL PROVVEDIMENTO DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI DEL 27 NOVEMBRE 2008 SUGLI AMMINISTRATORI DI SISTEMA.

Il fornitore si impegna inoltre a:

1. designare puntualmente tutte le persone fisiche che individuerà, per lo svolgimento delle predette attività, quali "amministratori di sistema" in ogni caso previa verifica della capacità, esperienza ed affidabilità delle stesse anche ai fini di garantire che il trattamento dei dati personali sia svolto nel pieno rispetto delle disposizioni vigenti e delle misure di sicurezza;

2. predisporre ed aggiornare tempestivamente un elenco degli amministratori di sistema che agiscono sui sistemi del Titolare, completo di estremi identificativi e funzioni attribuite, e metterlo a disposizione del Titolare secondo le indicazioni del medesimo;

3. rendere operativi sistemi informatici per la registrazione delle autenticazioni informatiche (access log) degli amministratori di sistema designati, con conservazione almeno semestrale delle stesse. Anche tali registrazioni potranno essere oggetto dell'attività di verifica periodica da parte del Titolare;

4. verificare con cadenza almeno annuale, anche eventualmente con il supporto di auditor esterni, l'operato degli amministratori di sistema in modo da controllare la loro rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti;

5. documentare adeguatamente lo svolgimento delle attività di cui sopra, fornendo un report scritto almeno annuale al Titolare.

In caso di inosservanza degli obblighi previsti nel presente documento il committente si riserva il diritto di risolvere il contratto per inadempimento da parte del fornitore. Resta inteso che la nomina a Responsabile del trattamento decadrà in qualunque caso di cessazione del servizio, con effetto dalla data di tale cessazione.

Qualora il fornitore determini autonomamente le finalità e i mezzi di trattamento, in violazione delle precedenti istruzioni, si assume i conseguenti oneri, rischi e responsabilità come se fosse un autonomo titolare relativamente al trattamento in questione.

In funzione di quanto sopra Vi preghiamo di restituirci il presente documento firmato nell'apposito spazio posto in calce e siglato su ogni singola pagina per conferma e accettazione.

18/06/2018

Il Titolare del Trattamento
Timbro/Firma del Committente

……..…..……..

Per conferma e accettazione

Il Responsabile del Trattamento
ADVENIAS s.r.l.
Ing. U. Brighetti