Ai sensi dell'art. 28 del Regolamento UE 2016/679
Tra
Rocksoil S.p.A, con sede legale Via Simone Elia, 13 - 24020 Torre Boldone (BG) -, CF e P.IVA 01795210168, in persona del legale rappresentante **Martina Lunardi**, il "**Titolare del Trattamento**" qui di seguito "La Società"
e
il "Fornitore" o il "**Responsabile del Trattamento**", in persona del legale rappresentante pro tempore,

sig. .....
di seguito "Il Fornitore" e congiuntamente indicate come "Parti"
Premesso che:
b) Nell'esercizio della sua attività, la Società ha accesso e tratta i dati personali di diversi soggetti (gli "Interessati");
c) Il Fornitore è un soggetto che opera per conto della società, sui dati della stessa o su parte delle commesse e quindi su parte dei dati della stessa;
d) la Società ha stipulato con il Fornitore un contratto di collaborazione ;
e) la Società, quale Titolare del Trattamento, ha determinato le finalità e i mezzi delle attività di trattamento dei predetti dati personali;
f) l'art. 4.8) del GDPR definisce "Responsabile del Trattamento" la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
g) l'art. 28 del GDPR prevede che (i) qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato; (ii) i trattamenti da parte di un responsabile del trattamento siano disciplinati da un contratto o da altro atto giuridico ai sensi del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento;
h) il Fornitore è risultato essere in possesso di idonei requisiti di esperienza, capacità tecnico-economica ed affidabilità e presenta garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate ai sensi delle previsioni del GDPR in materia di protezione dei dati personali e diritti degli interessati;
i) le Parti, pertanto, a seguito della stipulazione del Contratto e ai sensi dell'art. 28 del GDPR, intendono procedere, per mezzo del presente addendum al Contratto (1'"Addendum") a definire le modalità con cui il Responsabile del Trattamento si impegna ad effettuare per conto del Titolare le operazioni di trattamento dei Dati Personali come di seguito definite.

Tutto ciò premesso, tra le Parti si conviene e stipula quanto segue:
Articolo 1— Premesse e Addendum
1.1. Le Premesse al presente Addendum formano parte integrante ed essenziale dello stesso.
1.2. L'Addendum forma parte integrante ed essenziale del Contratto. I termini utilizzati nell'Addendum avranno il significato attribuito loro nell'Addendum stesso. I termini con la lettera maiuscola non altrimenti definiti nell'Addendum avranno il significato loro ascritto nel Contratto.
Articolo 2 — Definizioni
2.1 Nell'Addendum i seguenti termini avranno il significato che segue:
"Data Breach": una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, perdita, modifica, divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, secondo quanto previsto dall'art. 4 (12) del GDPR e il cui verificarsi comporta gli effetti e gli obblighi di cui all'art. 33 del GDPR.
"Dati Personali del Titolare": i dati personali come definiti dal GDPR che formano oggetto delle attività di trattamento da parte del Responsabile del Trattamento per conto del Titolare del Trattamento, ai sensi del e in connessione all'esecuzione del Contratto.
"DPIA": va inteso come data protection impact assessment; ovvero valutazione di impatto sulla protezione dei dati, come disciplinata dall'art. 35 del GDPR. Si tratta di una procedura finalizzata a descrivere le attività di trattamento di dati personali, valutarne necessità e proporzionalità e facilitare la gestione dei rischi che le stesse possono implicare per i diritti e le libertà delle persone fisiche (attraverso una valutazione di tali rischi e la individuazione delle misure idonee ad affrontarli).
"DPO": si intende il data protection officer o responsabile della protezione dei dati, ai sensi dell'art. 37 del GDPR.
"GDPR": il Regolamento Europeo n. 2016/679 sulla protezione dei dati personali.

"Servizi": i servizi e le altre attività che dovranno essere eseguiti dal Fornitore o per suo conto a favore del Titolare ai sensi del Contratto.
"Legge Applicabile": è da intendere come qualsiasi disposizione normativa dell'Unione Europea o dello Stato membro alla cui legge la Società è soggetta, in materia di protezione dei Dati Personali, ivi inclusi i provvedimenti adottati di tempo in tempo, in materia di protezione dei dati personali, dall'Autorità Garante Italiana per la Protezione dei Dati Personali e dal Comitato dei Garanti Europei.
"Soggetto Collegato": qualsiasi soggetto partecipato o controllato da una delle Parti, ovvero in cui una delle Parti detenga una partecipazione o su cui eserciti un controllo o che sia soggetto al comune controllo o partecipazione di una delle Parti, laddove la definizione di controllo dovrà intendersi quella di cui all'art. 2359 c.
"Sub-Responsabile": ciascun soggetto (incluso qualsiasi terzo e qualsiasi Soggetto Collegato al Fornitore ma esclusi i dipendenti del Fornitore o dei suoi sub-contractor) delegato dal Fornitore a effettuare alcune operazioni di trattamento per conto del Titolare in connessione con il Contratto.
I termini "Titolare", "Responsabile", "Interessato", "Stato Membro", "Dati Personali", "Trattamento" ed "Autorità Garante" avranno il significato loro ascritto nel GDPR e dovranno essere interpretati di conseguenza.

Articolo 3 — Oggetto delle prestazioni del Responsabile del Trattamento

3.1. Il Responsabile del Trattamento è autorizzato a trattare per conto del Titolare del Trattamento i Dati Personali necessari per fornire i Servizi.
3.2. I Dati Personali oggetto di trattamento sono i dati anagrafici identificativi o di contatto dei Clienti finali della Società.
3.3. La natura delle operazioni realizzate sui dati personali è sia automatizzata che non automatizzata.
3.3. La finalità o le finalità del trattamento sono finalità operative per lo svolgimento di un contratto;
3.4. Le categorie di interessati sono Clienti finali della Società, tra cui Clienti privati, Clienti business e Pubbliche Amministrazioni.

Articolo 4 — Obblighi del Responsabile del Trattamento

4.1 Ai sensi dell'art. 28, comma terzo, del GDPR, il Fornitore quale Responsabile del Trattamento (così come chiunque svolga operazioni di trattamento sotto le sue istruzioni) sarà tenuto all'osservanza dei seguenti obblighi.
a) **Rispetto della normativa.** Attenersi scrupolosamente a e rispettare, nel trattamento dei Dati Personali, la Legge Applicabile.
b) **Rispetto delle finalità.** Trattare i Dati Personali esclusivamente per la finalità o le finalità specificate all'articolo 3 che precede e per l'esecuzione delle prestazioni dedotte nel Contratto, nonché conformemente alle istruzioni documentate in forma scritta da parte del Titolare. Il Responsabile del Trattamento dovrà, quindi, astenersi dal fare uso dei Dati Personali per finalità diverse da quelle specificate dal Titolare del Trattamento. I Dati Personali trattati dal Responsabile del Trattamento rimarranno di proprietà del Titolare e/o degli Interessati. Il Responsabile del Trattamento non dovrà assumere decisioni unilaterali concernenti le attività di trattamento per finalità diverse da quelle previste, ivi inclusa la decisione di comunicare tali dati a soggetti terzi e quella relativa ai tempi di conservazione dei Dati Personali del Titolare.
c) **Dovere di cooperazione.** Informare immediatamente il Titolare (i) se ritenga che un'istruzione impartita dal Titolare del Trattamento comporti una violazione delle disposizioni del GDPR o, più in generale, della Legge Applicabile e (ii) dell'esistenza dell'obbligo giuridico di procedere ad un trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, a meno che la normativa vigente vieti tale informazione per rilevanti motivi di interesse pubblico.
d) **Riservatezza.** Garantire la riservatezza dei Dati Personali trattati e, in particolare, che (i) l'accesso ai Dati Personali sia limitato alle sole persone che hanno necessità di conoscere e/o accedere a tali dati per le finalità di cui al Contratto (i c.d. "Soggetti Autorizzati al Trattamento") e (ii) i Soggetti Autorizzati al trattamento dei Dati Personali si siano previamente impegnati alla riservatezza o siano, comunque, assoggettati ad un adeguato obbligo legale di riservatezza e abbiano ricevuto un'adeguata formazione in materia di protezione dei dati personali.
e) **Sicurezza.** Tenuto conto dello stato delle conoscenze tecniche, dei costi di realizzazione e della natura, della finalità, del contesto e dello scopo del trattamento nonché dei diversi livelli di rischio (in termini di gravità e probabilità) che il trattamento comporta per i diritti e le libertà fondamentali degli Interessati, adottare le misure di sicurezza tecnica e organizzativa adeguate ad assicurare un livello di sicurezza appropriato rispetto al rischio di perdita, alterazione o illegittimo trattamento dei Dati Personali gestiti per conto del Titolare, ivi incluse, ove applicabili, le misure di cui all'art. 32 (1) del GDPR. Nel valutare il livello di sicurezza appropriato in relazione al rischio, il Fornitore dovrà tenere in considerazione in particolare i rischi implicati dalle specifiche attività di trattamento dallo stesso compiute, ivi inclusi i rischi implicati dalla Violazione dei Dati Personali. In ogni caso il Responsabile del Trattamento dovrà garantire almeno l'adozione delle seguenti misure di sicurezza tecnica e organizzativa:

- implementazione e gestione degli opportuni profili di accesso ai sistemi ed alle funzionalità applicative che consentono agli incaricati di gestire i dati personali dei clienti e, ove applicabili, funzionalità di cifratura delle informazioni presenti sull'HD dei laptop in uso al personale ed utilizzo di funzionalità di cifratura delle chiavette USB, al fine di assicurarne su base permanente riservatezza;
- implementazione dei controlli di qualità necessari a validare le procedure operative in uso con riguardo anche alle procedure di gestione di eventuali documenti cartacei contenenti dati personali dei clienti ed altri controlli di qualità in ambito tecnologico atti a validare i software in uso in modo da garantirne l'integrità;
- utilizzo delle opportune procedure di backup insieme all'implementazione di eventuali architetture di alta affidabilità dei sistemi, atti a garantirne la disponibilità;
- implementazione ed aggiornamento di sistemi a protezione di dati ed applicazioni per far fronte a violazioni e attacchi mirati, azioni di pirateria, minacce del Web ed uso a distanza di vulnerabilità, atti a garantirne riservatezza, integrità e disponibilità.

In generale si richiede al Fornitore di adottare tutte quelle misure tecniche ed organizzative che garantiscono un livello di sicurezza adatto al rischio, capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico e l'implementazione di un procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

f) **Sub-Responsabili**.

Selezionare l'opzione prescelta in base al tipo di attività da svolgere:

☐ Procedere, se necessario, alla nomina di un altro Responsabile del trattamento (il c.d. "Sub-Responsabile del trattamento") per gestire attività di trattamento specifiche, qualora il Contratto preveda la possibilità di subappalto e nei termini di cui al Contratto. In questo caso, il Responsabile del Trattamento dovrà informare previamente la Società, mediante una comunicazione scritta, di eventuali modifiche comportanti l'aggiunta o la sostituzione di eventuali Sub-Responsabili del trattamento e, in particolare, dovrà indicare chiaramente le attività di trattamento delegate, l'identità e i dati di contatto del Sub-Responsabile del trattamento ed i contenuti del contratto sottoscritto con quest'ultimo, dando così al Titolare del Trattamento l'opportunità di opporsi a tali modifiche entro e non oltre 5 giorni dalla ricezione di tale comunicazione. Il Titolare del Trattamento dovrà quindi sommariamente indicare al Responsabile del Trattamento le ragioni della sua opposizione e le Parti coopereranno in buona fede in vista della selezione di un Sub-Responsabile del trattamento che sia ritenuto idoneo dal Titolare del Trattamento. In difetto di un'intesa nei successivi 5 giorni, e qualora il Responsabile del Trattamento ritenga di non essere in grado di eseguire le prestazioni di cui al

☐ Contratto senza l'apporto del Sub-Responsabile del Trattamento, il Titolare del Trattamento avrà diritto di risolvere il Contratto, ai sensi e per gli effetti di cui all'art. 1456 c.c.

In ogni caso, le Parti convengono che, nel caso di nomina di un Sub-Responsabile del trattamento:
- Prima che il Sub-Responsabile del trattamento cominci a svolgere le attività di trattamento dei Dati Personali delegategli, il Responsabile del Trattamento dovrà svolgere un'accurata due diligence volta ad assicurarsi che il Sub-Responsabile del trattamento sia in grado di garantire il livello di protezione dei Dati Personali richiesto dal Contratto e dall'Addendum;
- al predetto Sub-Responsabile del trattamento dovranno essere imposti, mediante la stipulazione di un contratto o di un altro atto giuridico vincolante, i medesimi obblighi in materia di protezione dei dati personali stabiliti in questo Addendum e, in particolare, garanzie sufficienti a mettere in atto misure tecniche e organizzative adeguate affinché il trattamento soddisfi i requisiti del GDPR;
- qualora il Sub-Responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile del Trattamento sarà integralmente responsabile nei confronti del Titolare dell'adempimento degli obblighi da parte del Sub-Responsabile.

g) **Trasferimento dei Dati Personali gestiti per conto del Titolare**. Il Responsabile del Trattamento potrà trattare i Dati Personali in paesi siti al di fuori dell'Unione Europea nonché trasferirli in tali paesi a condizione che i suddetti paesi garantiscano il livello di protezione dei dati e il rispetto degli altri obblighi previsti dalla normativa europea nonché da questo Addendum. Il Responsabile del Trattamento è tenuto ad informare il Titolare del Trattamento in merito ai paesi in cui i Dati Personali saranno trattati o trasferiti.

h) **Diritti degli Interessati**. Tenuto conto della natura del trattamento, assistere il Titolare con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare del Trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'Interessato di cui al capo III del GDPR (il diritto di accesso, di rettifica, di cancellazione e di opposizione, alla limitazione del trattamento, alla portabilità dei dati, di non essere oggetto di una decisione individuale automatizzata). Nell'ipotesi in cui gli Interessati presentino richiesta per l'esercizio

dei suddetti diritti al Responsabile del Trattamento, quest'ultimo dovrà inoltrare immediatamente, e comunque entro 72 ore dalla ricezione, detta richiesta per posta elettronica al Titolare del Trattamento.

i) **Cooperazione in caso di Data Breach e redazione di DPIA**. Assistere il Titolare nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR e, pertanto, nella elaborazione e nell'attuazione delle misure di sicurezza, nella notifica e nella comunicazione dei Data Breach, nella redazione della DPIA e nella consultazione preventiva, tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile del Trattamento.

In particolare:

- **nel caso di Data Breach**, il Responsabile del Trattamento dovrà notificare al Titolare del Trattamento ogni violazione riscontrata, a prescindere da qualsiasi valutazione circa l'impatto e le conseguenze attese della violazione stessa, senza indugio e, in ogni caso, entro il tempo massimo di 24 ore dal momento in cui ne sia venuto a conoscenza utilizzando l'indirizzo email del TITOLAREITOLARE, corredando detta comunicazione con ogni documentazione utile a consentire al Titolare, quale Titolare del Trattamento, di notificare tale violazione al Garante e agli Interessati, ove necessario, nel rispetto delle tempistiche di cui all'art. 33 del GDPR. La comunicazione dovrà, in ogni caso, contenere quantomeno i seguenti dettagli:
  - (i) l'indicazione della probabile causa della violazione;
  - (ii) le conseguenze note o attese di tale violazione;
  - (iii) la soluzione proposta;
  - (iv) le misure che siano state già adottate per contenere e limitare le conseguenze della violazione.

Il Responsabile del Trattamento garantisce sin d'ora che ogni informazione fornita a tal fine sarà completa, corretta e accurata;

- **nella redazione della DPIA e nella consultazione preventiva**, il Responsabile del trattamento, dovrà assistere il Titolare nella realizzazione delle analisi di impatto relative alla protezione dei dati ai sensi dell'art. 35 del GDPR e nella consultazione preventiva al Garante ai sensi dell'art. 36 del GDPR.

i) **Cancellazione dei Dati Personali del Titolare**. Cancellare/distruggere o restituire alla società Titolare (secondo quanto la stessa deciderà e comunicherà al Responsabile del Trattamento di volta in volta) tutti i dati personali dopo la cessazione della prestazione dei Servizi relativi al trattamento e cancellare / distruggere le copie esistenti, documentandone per iscritto l'intervenuta cancellazione / distruzione, salvo che la normativa applicabile preveda la conservazione dei dati.

k) **Audit**. Mettere a disposizione del Titolare, dietro semplice richiesta dello stesso, tutta la documentazione e le informazioni necessarie per dimostrare il rispetto degli obblighi stabiliti dall'art. 28 del GDPR e da questo Addendum e consentire e contribuire allo svolgimento delle attività di revisione, comprese le ispezioni, realizzate dal Titolare del Trattamento o da un altro soggetto da questi incaricato. L'audit sarà condotto dal Titolare del Trattamento cercando di limitare al massimo le interferenze con la normale attività di business del Responsabile del Trattamento. Le risultanze dell'audit saranno discusse in buona fede tra le Parti e il Responsabile del Trattamento si impegna sin d'ora ad attuare i cambiamenti ritenuti necessari dal Titolare del Trattamento in seguito all'audit, al fine di garantire la conformità alla Legge Applicabile e all'Addendum.

l) **DPO**. Comunicare al Titolare del trattamento il nome ed i dati del proprio Responsabile della Protezione dei dati, qualora ne abbia designato uno ai sensi dell'art. 37 del GDPR.

m) **Registro delle attività di trattamento**. Tenere per iscritto un registro di tutte le categorie di attività di trattamento svolte per conto del Titolare, contenente
  - i) il nome e i dati di contatto del Fornitore quale Responsabile del trattamento, di ogni titolare del trattamento per conto del quale agisce, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del Responsabile della protezione dei dati;
  - ii) le categorie dei trattamenti effettuati per conto del Titolare e per altri titolari del trattamento;
  - iii) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49 del GDPR, i documenti che attestano l'esistenza di garanzie adeguate;
  - iv) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1, del GDPR.

Articolo 5 — Obblighi del Titolare del trattamento

5.1 La società Titolare, quale Titolare del trattamento, è tenuta a:

1) Fornire agli Interessati l'informativa di cui agli articoli 13 e 14 del GDPR;

2) Fornire al Fornitore le informazioni ed i dati elencati nel presente Addendum, nonché ogni altra informazione utile per l'esecuzione delle attività di trattamento illustrate nello stesso;

3) Documentare per iscritto tutte le istruzioni impartite al Responsabile del Trattamento per il trattamento dei Dati Personali del Titolare;

4) Vigilare, in via preventiva e per tutta la durata del trattamento, sul rispetto degli obblighi previsti dal GDPR;
5) Svolgere un'attività di supervisione sul trattamento dei dati personali, ivi incluse le revisioni e le ispezioni di cui al presente Addendum.

Articolo 6 — Conseguenze della violazione delle disposizioni della Legge Applicabile da parte del Responsabile del Trattamento

6.1 Nel caso in cui dovesse violare le disposizioni della Legge Applicabile, determinando le finalità e i mezzi del trattamento, il Fornitore sarà considerato un autonomo titolare del trattamento in questione, fatte salve le disposizioni del GDPR di cui all'art. 82 in tema di diritto al risarcimento e responsabilità, all'art. 83 in tema di condizioni generali per infliggere sanzioni amministrative pecuniarie e all'art. 84 in tema di sanzioni.

Articolo 7 — Clausola di manleva

7.1 Il Fornitore si impegna a manlevare e tenere indenne la società Titolare da qualsiasi danno, pregiudizio, costo, spesa, onere che la stessa dovesse subire e/o dover risarcire a terzi a causa della violazione, da parte del Responsabile del Trattamento, o degli eventuali Sub-Responsabili da esso nominati, delle disposizioni della Legge Applicabile e delle istruzioni impartite dal Titolare del Trattamento.
A tale riguardo, il Responsabile del Trattamento dichiara di avere contratto specifica polizza assicurativa la quale dovrà essere esibita al Titolare dietro semplice richiesta.

Articolo 8 — Clausola risolutiva espressa

8.1 Nel caso in cui il Fornitore si rendesse inadempiente ad uno degli obblighi stabiliti all'articolo 4 che precede, il presente Addendum si intenderà risolto ai sensi e per gli effetti di cui all'art. 1456 c.c. dopo che la società Titolare avrà comunicato per iscritto al Fornitore che intende avvalersi della clausola risolutiva espressa, fatto salvo il diritto del Titolare del Trattamento alla manleva ed al risarcimento dei danni conseguenti all'inadempimento.

Articolo 9 — Durata

9.11 Il presente Addendum avrà la stessa durata del Contratto. Lo stesso si intenderà pertanto cessato e/o risolto laddove il Contratto venga a cessare o sia risolto per qualsiasi ragione o causa.

Articolo 10- Miscellanea

10.1. Per quanto concerne i trattamenti che il Responsabile esegue per conto del Titolare in esecuzione del Contratto, Il Titolare ha facoltà di modificare unilateralmente e discrezionalmente il presente addendum e le istruzioni ivi contenute, mediante apposita comunicazione scritta ....
10.2. Le Parti si impegnano a prestare la loro massima cooperazione per modificare o integrare l'Addendum nel caso ciò si renda necessario in virtù di intervenute modifiche nella Legge Applicabile.
10.3. Il presente Addendum e la sua interpretazione ed esecuzione sono regolate dalla Legge Italiana.
10.4. Qualsiasi controversia che dovesse sorgere in connessione o in relazione all'Addendum sarà devoluta alla cognizione esclusiva del Foro previsto nel Contratto.

Milano, li .....

Il Titolare del Trattamento
Rocksoil S.p.A. - Amministratore Delegato
Martina Lunardi
X .....

Per il Responsabile del Trattamento

.....

Ai sensi e per gli effetti di cui all'art. 1341 c.c., il Fornitore dichiara di avere letto e di approvare espressamente le seguenti clausole:
art. 7 (Clausola di Manleva);
art. 8 (Clausola Risolutiva Espressa);
art. 10 (Miscellanea, Foro esclusivo).