ALLEGATO 2

CONTRATTO DI DESIGNAZIONE A RESPONSABILE ESTERNO PER IL TRATTAMENTO DEI DATI

E CONFERIMENTO DELLE RELATIVE ISTRUZIONI

Tra

Regione Umbria- Giunta regionale, rappresentata dal Dirigente del Servizio dott. Franco Garofalo, domiciliato presso la sede della Regione medesima, che stipula il presente atto in nome e per conto della Regione Umbria – Giunta regionale (C.F. 80000130544)

e

Kolorado SAS di Paolo Marcantonini e C. con sede legale in Via Luigi Rizzo 83 06128 Perugia, P. IVA 02858830546, rappresentata da Paolo Marcantonini domiciliato presso la sede, che stipula il presente atto in nome e per conto di Kolorado SAS P. IVA 02858830546 di seguito, congiuntamente, le "Parti".

Premesso che:

a) tra la Regione Umbria – Giunta regionale e Kolorado SAS intercorre un rapporto di fornitura servizi in forza del contratto principale CIG 7849825882 RdO 2328899 concernente il servizio di supporto alle attività di comunicazione del Programma di Sviluppo Rurale per l'Umbria 2014-2020 stipulato su MEPA in data 03/10/2019;
b) il rapporto contrattuale di cui alla lett. a) implica, necessariamente, il trattamento, da parte di Kolorado SAS, di dati personali di cui la Regione Umbria – Giunta regionale è Titolare;
c) il Regolamento (UE) 679/2016 del 27 aprile 2016 "Regolamento del Parlamento europeo relativo 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)" (di seguito GDPR) "si applica al trattamento dei dati personali effettuato nell'ambito delle attività (...) di un Responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione";

d) ai sensi dell'art. 28, par. 1, del GDPR, "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 Regolamento e garantisca la tutela dei diritti dell'interessato";

e) ai sensi dell'art. 29 del GDPR, "Il Responsabile del trattamento, o chiunque agisca sotto la sua autorità (…), che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal Titolare (...)";

f) ai sensi dell'art. 28, par. 3, del GDPR, inoltre, "I trattamenti da parte di un Responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico, che vincoli il Responsabile del trattamento al Titolare 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";

g) ai sensi dell'art. 31 del GDPR, "il Responsabile del trattamento (...) coopera, su richiesta, con l'Autorità di controllo Garante per la protezione dei dati";

h) ai sensi dell'art. 82, par. 2 del GDPR, il "Responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del (...) Regolamento specificatamente diretti ai Responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del Titolare del trattamento";

i) a seguito delle garanzie offerte e delle dichiarazioni di conformità al GDPR rilasciate da Kolorado SAS (Allegato A), in forza di quanto previsto dall'art. 28, par. 1, del Regolamento suddetto e allegate al presente contratto, Kolorado SAS è stata ritenuta idonea ad assumere la qualifica di Responsabile esterno del trattamento, in quanto dotata di esperienza, competenze tecniche e risorse che gli consentono di mettere in atto misure tecniche e organizzative adeguate, atte a garantire la conformità del trattamento dati alla normativa in materia di tutela dei dati personali.

Tutto ciò premesso e considerato,
che costituisce parte integrante e sostanziale del presente atto,
si conviene quanto segue

Art. 1 Determinazione del Titolare del trattamento dei dati e del Responsabile del trattamento dei dati.

Ai sensi e per gli effetti dell'art. 28 del GDPR, con il presente contratto (di seguito, "Contratto") la Regione Umbria – Giunta regionale (di seguito Regione Umbria), in qualità di "Titolare del trattamento" (di seguito, il "Titolare"), nomina Kolorado SAS, con sede legale in Via Luigi Rizzo 83 06128 Perugia, P. IVA 02858830546 "Responsabile esterno del trattamento" (di seguito, il "Responsabile").

Art. 2 Legge applicabile

Ciascuna Parte si impegna ad adottare tutte le misure necessarie per garantire che i dati personali siano raccolti e trattati in osservanza a quanto richiesto dalle leggi europee, nazionali e dalle prescrizioni della Autorità di controllo in relazione al trattamento dei dati personali e alla libera circolazione di tali dati, tra cui il Regolamento Generale sulla Protezione dei Dati (UE) 2016/679 ("GDPR") e il D.Lgs. 196 del 30 giugno 2003 e s.m.i. ("Codice della Privacy").

Le disposizioni previste dal presente contratto trovano applicazione in tutte le operazioni di trattamento, ivi comprese quelle che siano già state intraprese prima della conclusione del presente accordo.

Ciascuna Parte assume l'obbligo di informare la controparte di qualsiasi modifica della propria legislazione nazionale che potrebbe avere un impatto sul contratto.

Art. 3 Attività di trattamento dei dati personali in esecuzione di un obbligo contrattuale. Autorizzazione al trattamento, categorie e tipologie di dati trattati, categorie di soggetti interessati.

In esecuzione del contratto principale richiamato in premessa in essere fra la Regione Umbria e Kolorado SAS, il Responsabile è autorizzato a trattare per conto del Titolare le seguenti categorie di dati personali: dati comuni ed in particolare le seguenti tipologie di dati personali:

dati anagrafici, residenza, n. telefono, indirizzo di posta elettronica in quanto strumentali alla erogazione dei servizi descritti nel **contratto principale**:

I dati trattati si riferiscono alle seguenti categorie di interessati: **beneficiari e destinatari di contributi del Programma di Sviluppo Rurale dell'Umbria e cittadini che partecipano alle attività di comunicazione e promozione del PSR.**

La Regione Umbria rimane proprietaria e, quindi, Titolare dei dati trattati per suo conto dal Responsabile.

La Regione Umbria comunica per iscritto al Responsabile l'eventuale aggiornamento dei tipi di dati trattati e le categorie di interessati coinvolti nelle attività di trattamento oggetto del contratto principale e del presente contratto.

Art. 4 Comunicazione tra le Parti

Al fine di facilitare la comunicazione tra le Parti, i dati di contatto del Responsabile per la protezione dei dati (Data Protection Officer, "DPO") della Regione Umbria è:

- DPO Regione Umbria Giunta regionale Francesco Nesta – dpo@regione.umbria.it tel. 0755045693 cell. 3371439860

Ciascuna Parte assume l'obbligo di informare la controparte di qualsiasi modifica del rispettivo Responsabile per la protezione dei dati (DPO).

Il Responsabile fornisce a Regione Umbria – Giunta regionale l'elenco dei soggetti preposti al trattamento dei dati personali.

Art. 5 Finalità del trattamento operato in esecuzione di un obbligo contrattuale.

In adempimento alle prestazioni dedotte nel contratto principale, il Responsabile è autorizzato a trattarli esclusivamente per il perseguimento delle seguenti finalità: attività di comunicazione e promozione del PSR 2014-2020, in conformità alle istruzioni impartite dalla Regione Umbria e indicate nel presente contratto o comunque trasmesse per iscritto dalla Regione Umbria escludendo qualsiasi altra finalità.

Il Responsabile non vanta alcun diritto sui dati ed è autorizzato a trattarli nei termini, modi e limiti stabiliti nel presente contratto o comunque trasmesse per iscritto dalla Regione Umbria rispettando in ogni caso i principi generali di liceità, proporzionalità e correttezza.

Art. 6 Istruzioni per il trattamento dei dati personali

Il Responsabile si impegna a trattare i dati personali soltanto su istruzioni documentate del Titolare e indicate nei contratti principali, nel presente contratto o comunque ulteriormente impartite per iscritto dalla Regione Umbria (indicare l'opzione che interessa) ; in particolare, in relazione ai rapporti contrattuali di cui in premessa, il Responsabile potrà trattare i dati esclusivamente per le finalità sopra riportate e potrà effettuare, con strumenti automatizzati, soltanto le seguenti operazioni: registrazione, organizzazione, conservazione, estrazione, consultazione, uso[1].

Qualora la normativa, comunitaria o nazionale, imponesse al Responsabile il trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale, lo stesso Responsabile informerà il Titolare di tale obbligo giuridico prima del relativo trasferimento, salvo che la normativa in questione vieti tale informazione per rilevanti motivi di interesse pubblico.

Il Responsabile informerà immediatamente il titolare qualora, a suo parere, un'istruzione violasse il Regolamento o altre disposizioni, europee o nazionali, relative alla protezione dei dati.

Il Responsabile è consapevole ed accetta che i propri dati personali possano essere pubblicati sul sito istituzionale del Titolare per finalità di trasparenza nei confronti degli interessati.

1 Si ricorda che l'art. 4, per. 1, n.2del GDPR fornisce la seguente definizione di "trattamento": "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione".

In ogni fase e per ogni operazione del trattamento, il Responsabile dovrà garantire il rispetto dei principi comunitari e nazionali in ambito di protezione dei dati personali e, in particolare, quelli di cui agli artt. 5 e 25 del Regolamento. In particolare, il Responsabile dovrà:

a) rispettare la normativa vigente in materia di trattamento dei dati personali, ivi comprese le norme che saranno emanate nel corso della durata del contratto;
b) trattare i dati personali per le sole finalità specificate e nei limiti dell'esecuzione delle prestazioni contrattuali così come previsto dai contratti principali;
c) trattare i dati conformemente alle istruzioni impartite dal Titolare e di seguito indicate, che il Responsabile si impegna a far osservare anche alle persone da questi autorizzate ad effettuare il trattamento dei dati personali oggetto del presente contratto, d'ora in poi "persone autorizzate";
d) garantire che le persone che trattano dati personali siano state specificamente autorizzate, adeguatamente istruite e si siano impegnate alla riservatezza o siano sottoposti ad un obbligo legale appropriato di segretezza;
e) valutare i rischi inerenti il trattamento dei dati personali e adottare tutte le misure tecniche ed organizzative che soddisfino i requisiti del Regolamento UE anche al fine di assicurare un adeguato livello di sicurezza dei trattamenti, in modo tale da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, modifica, divulgazione non autorizzata, nonché di accesso non autorizzato, anche accidentale o illegale, o di trattamento non consentito o non conforme alle finalità della raccolta;
f) provvedere, qualora previsto dall'art. 30 del GDPR, alla predisposizione e aggiornamento del Registro delle attività di trattamento oggetto dei contratti principali, secondo quanto disposto dalla Giunta regionale con D.G.R. 515/2018 e s.m.i., rendendolo tempestivamente disponibile al Titolare, o all'Autorità di controllo, in caso di relativa richiesta.

Il Responsabile si impegna a fare in modo che i dati personali oggetto di trattamento siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati») e vengano:

g) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
h) mantenuti aggiornati, laddove e per quanto previsto dal contratto, adottando tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
i) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;

La Regione Umbria – Giunta regionale si impegna a fornire per iscritto al Responsabile del trattamento, ove ritenuto opportuno, ulteriori istruzioni rispetto a quelle previste dal presente contratto e dai contratti principali.

Art. 7 Diritti degli Interessati

CASO 1: La Regione Umbria – Giunta regionale raccoglie direttamente i dati personali e li trasmette al Responsabile per il trattamento

La Regione Umbria, in qualità di Titolare del trattamento dei dati, predispone l'informativa da rendere agli interessati ai sensi dell'art. 13 del GDPR e provvede a fornirla ai medesimi spiegando i loro diritti e raccogliendone, se necessario, il consenso.

Detta informativa è comunicata al Responsabile del trattamento.

La Regione Umbria, in qualità di Titolare del trattamento dei dati, risponde alle richieste di esercizio dei diritti di cui agli artt. da 15 a 22 del GDPR che dovessero essere avanzate dagli Interessati qualora sussistano le condizioni di legge (diritto di informazione, accesso, rettifica, cancellazione, revoca del consenso, restrizione, portabilità dei dati, obiezione, diritto di non essere valutato sulla base del trattamento automatizzato,…).

In ogni caso il Responsabile si obbliga ad assistere il Titolare ed a fornire ogni informazione e/o documento utile o opportuno per consentire al Titolare di evadere eventuali istanze degli

interessati, nonché informare tempestivamente il Titolare dei reclami eventualmente presentati dagli interessati.

CASO 2 Il Responsabile raccoglie direttamente i dati

In occasione del primo atto di raccolta delle informazioni, il Responsabile fornisce agli interessati l'informativa di cui all'art. 13 del GDPR sul trattamento dei dati che esegue in nome e per conto del Titolare, e li rende edotti dei loro diritti, acquisendo, se necessario, la loro positiva manifestazione di volontà al trattamento.

Il contenuto e la forma dell'informativa e della formula per la raccolta del consenso devono essere concordati con il Titolare prima di raccogliere i dati.

Il Responsabile ha l'obbligo di fornire l'informativa e raccogliere il consenso anche dei soggetti interessati da attività di trattamento iniziate prima della conclusione del presente contratto.

Il Responsabile, qualora riceva delle richieste di esercizio dei diritti da parte degli interessati per le attività che gli sono state autorizzate dal presente contratto, provvede tempestivamente, entro un massimo di 5 giorni, mediante PEC o raccomandata A/R, ad informare il Titolare e fornisce, se necessario, supporto per la gestione della richiesta.

Art. 8 Hosting di dati personali

Il Responsabile si impegna ad archiviare e conservare i dati del Titolare su server situati all'interno dell'Unione europea e ad informare il Titolare prima di spostare l'ubicazione del Data Center.

Il Responsabile non è autorizzato a modificare la posizione fisica dei suoi server al di fuori dell'Unione europea senza l'esplicita autorizzazione del Titolare. La violazione di questo obbligo è giusta causa di risoluzione contrattuale.

Art. 9 Ricorso del Responsabile ad un sub-Responsabile del trattamento

Il Responsabile non ricorrerà ad altro ulteriore Responsabile del trattamento (di seguito "sub-Responsabile") senza previa autorizzazione scritta, specifica o generale, del Titolare. Nel caso

di autorizzazione generale, il Responsabile informerà il Titolare di eventuali modifiche riguardanti l'aggiunta o la sostituzione di ulteriori sub-Responsabili, dando così al Titolare l'opportunità di opporsi a tali modifiche.

In ogni caso qualora il Responsabile ricorresse ad un sub-Responsabile per l'esecuzione di specifiche attività di trattamento per conto del Titolare, dovrà sottoscrivere, con tale sub-Responsabile, un contratto (o altro atto giuridico) analogo al presente Contratto — stipulato in forma scritta, anche in formato elettronico — imponendo a quest'ultimo gli stessi obblighi in materia di protezione dei dati contenuti nel presente Contratto (e in ogni altro atto giuridico o addendum intervenuto tra le Parti) e prevedendo, in particolare, garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR, nonché della relativa disciplina nazionale.

Resta inteso che, laddove il sub-Responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile conserva nei confronti del Titolare l'intera responsabilità dell'inadempimento degli obblighi del sub-Responsabile.

Art. 10 Obbligo di garantire la sicurezza dei dati trattati

Il Responsabile del trattamento si impegna a garantire la riservatezza, l'integrità e la disponibilità dei dati trattati e ad assicurare che le persone autorizzate a trattare tali dati ne garantiscano parimenti la tutela, siano vincolate da un obbligo di riservatezza e ricevano un'appropriata formazione sulla protezione dei dati.

Art. 11 Misure di sicurezza

Il Responsabile del trattamento si impegna a garantire uno standard di sicurezza adeguato al livello di rischio e comunque non inferiore al livello M ("Minimo"), delle misure minime di sicurezza ICT per le Pubbliche Amministrazioni come da Circolare AgID 2/2017 (Misure minime di sicurezza ICT per le pubbliche amministrazioni).

Il Responsabile del trattamento prende in considerazione, in termini di strumenti, prodotti, applicazioni o servizi, i principi della protezione dei dati fin dalla progettazione (*privacy by design*) e per impostazione predefinita (*privacy by default*).

A tal fine, il Responsabile del trattamento si impegna ad attuare le opportune misure di sicurezza in funzione della natura dei dati trattati e dei trattamenti effettuati, tra cui, se del caso:

- la crittografia dei dati;
- la capacità di garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di elaborazione in corso;
- la possibilità di ripristinare la disponibilità e l'accesso ai dati personali in modo tempestivo in caso di incidente fisico o tecnico;
- un processo per testare e valutare con regolarità l'efficacia delle misure tecniche e organizzative per garantire la sicurezza del trattamento.

Art. 12 Obbligo di gestione e segnalazione in caso di violazione dei dati (data breach)

Il Responsabile si impegna a garantire uno standard di sicurezza adeguato al livello di rischio.
In caso di violazione dei dati, il Responsabile si impegna a informare il Titolare entro 24 ore dalla accertata violazione secondo la procedura approvata dalla Giunta regionale con deliberazione del 14 maggio 2018, n. 485 allegata al presente contratto e assiste il Titolare ai fini degli adempimenti previsti dal GDPR.

Art. 13 Assistenza e supporto

Il Responsabile del trattamento supporta la Regione Umbria – Giunta regionale nella realizzazione di valutazioni d'impatto sulla protezione dei dati (DPIA), nel rispetto degli obblighi di cui agli articoli 35 e 36 del Regolamento.
Il Responsabile fornisce al Titolare la documentazione necessaria per dimostrare l'adempimento dei propri obblighi e per consentire al medesimo o a qualsiasi soggetto autorizzato di svolgere attività di audit.

Art. 14 Responsabilità

Il Responsabile può svolgere attività di trattamento solo in ossequio delle istruzioni ricevute dal Titolare e può essere ritenuto responsabile per qualsiasi inadempienza ai propri obblighi e per i danni conseguenti causati da fatto proprio. Se il sub-responsabile non adempie ai propri obblighi, il responsabile del trattamento risponde nei confronti di Regione Umbria di tale inadempimento. Il responsabile del trattamento informa la Regione Umbria prontamente nel caso in cui sia stata intrapresa nei suoi confronti un'azione giudiziaria per violazione della normativa in materia di protezione dei dati personali.

I Responsabili devono inoltre tenere indenne la Regione Umbria da qualsiasi azione giudiziaria (incluse le spese legali e di risarcimento danni) intentata da terze parti per inadempimento degli obblighi in materia di protezione dei dati personali loro imputabili.

In caso azione di risarcimento civile, o responsabilità amministrativa, promossa nei confronti del Titolare per i danni provocati, o violazioni commesse dal Responsabile per inadempimento degli obblighi previsti dal regolamento o dal codice privacy specificatamente diretti ai Responsabili del trattamento o azioni difformi o contrarie rispetto alle legittime istruzioni del Titolare, il Responsabile stesso manleva integralmente il Titolare, salvo dimostrazione di avere adottato tutte le misure idonee a evitare il danno. Analogamente, il Responsabile manleva integralmente il Titolare in caso di applicazione di sanzioni da parte dell'Autorità di controllo per inadempienze normative o contrattuali commesse dallo stesso Responsabile, salvo dimostrazione di avere adottato tutte le misure idonee a evitare il danno e aver rispettato gli obblighi previsti dagli art. 28 e 82. Nei casi previsti dal presente articolo, il Titolare potrà risolvere il contratto, salvo il risarcimento del maggior danno.

Art. 15 Periodo di conservazione dei dati personali e metodi di cancellazione

Al termine del rapporto contrattuale, il Responsabile si impegna a cancellare/ restituire in modo sicuro, tutti i dati che ha trattato in nome e per conto di Regione Umbria e a fornire, su

richiesta della medesima, una dichiarazione scritta della avvenuta cancellazione/restituzione, senza conservare alcuna copia dei dati.

Qualora fosse stabilito l'obbligo di restituire i dati, il medesimo, i medesimi devono essere inviati in un formato leggibile elettronicamente in modo che Regione possa riutilizzarli e archiviarli correttamente.

La cancellazione deve essere eseguita con una soluzione tecnica che rispetti lo stato di avanzamento tecnologico e riguardi tutti i dati personali che sono stati elaborati per conto del Titolare.

Il Responsabile garantisce che, su richiesta del Titolare e senza costi aggiuntivi, prima di effettuare la cancellazione predetta potrà procedere alla trasmissione sicura dei dati personali ad altro soggetto, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, beninteso qualora il destinatario sia attrezzato a riceverli.

Art. 16 Attività di vigilanza

Durante l'esecuzione del contratto il Titolare del trattamento vigila sul rispetto degli obblighi previsti dai contratti principali e dal presente contratto, dal GDPR e dal codice della privacy 196/2003 da parte del Responsabile, nonché controlla l'attività di trattamento dei dati personali effettuando audit, ispezioni e verifiche periodiche sull'attività posta in essere dal Responsabile.

Il Responsabile mette a disposizione del Titolare tutta la documentazione e le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente contratto, consentendo e contribuendo alle attività di revisione, comprese le ispezioni, realizzate dal Titolare, dal suo Data Privacy Officer, o da un altro soggetto a ciò deputato.

Luogo e data

Perugia, 18 giugno 2020

Il Titolare del trattamento

_____

(firmare digitalmente)

Per accettazione

Il Responsabile esterno per il trattamento dei dati

Paolo Marcantonini