CONDIZIONI GENERALI DI SERVIZIO PER GLI SVILUPPATORI

1. PREMESSA

1.1. Le presenti Condizioni Generali di Servizio per gli Sviluppatori (**Condizioni Generali per gli Sviluppatori**) disciplinano il rapporto tra Projectmoon srl, con sede legale in Villorba (TV), Via Roma 4/18, iscritta presso la Camera di commercio di Treviso al n. 04214670269 del Registro delle imprese, REA n. 332105, codice fiscale n. 04214670269 partita IVA n. 04214670269, E-mail info@projectmoon.it PEC projectmoon@pec.projectmoon.it (**Projectmoon** o **Società**), e gli sviluppatori che pubblicano applicazioni sulla piattaforma gestita da Projectmoon.

2. DEFINIZIONI

Nelle presenti condizioni i termini di seguito indicati avranno il seguente significato:

a. **Accordo**: il contratto costituito dalle presenti Condizioni Generali per gli Sviluppatori e da qualsiasi eventuale comunicazione intercorsa tra le Parti.

b. **Amazon**: indica Amazon.com, Inc., Amazon Europe Core SARL, Amazon EU Sarl e/o le società eventualmente affiliate ad esse, nonchè qualsiasi società appartenente al gruppo Amazon o comunque connessa direttamente ad una delle predette società o ad altra società del gruppo Amazon.

c. **API**: Application Program Interface. Set di definizioni e protocolli con i quali vengono realizzati e integrati software applicativi.

d. **Applicazione o App**: singolo programma installabile dall'Utente Venditore gratuitamente o a pagamento, a seconda delle condizioni d'uso della stessa App, accedendo all'Apps Market.

e. **Apps Market**: spazio virtuale allocato presso la piattaforma attraverso il quale l'Utente Venditore può installare sul proprio sito le Applicazioni offerte in vendita dai singoli Sviluppatori oppure installare sul proprio sito i temi grafici offerti a titolo gratuito dai singoli Sviluppatori.

f. **Condizioni Generali per gli Sviluppatori**: il presente documento e qualsiasi sua successiva modifica e integrazione.

g. **Informazioni Amazon o Amazon Information**: indica qualsiasi informazione esposta da Amazon tramite le API del Marketplace, Seller Central o i siti web pubblici di Amazon. Questi dati possono essere pubblici o non pubblici, comprese le informazioni di identificazione personale dei clienti Amazon.

h. **Parti**: la Società e lo Sviluppatore.

i. **PII**: informazioni di identificazione personale. Indica informazioni che possono essere utilizzate da sole o con altre informazioni per identificare, contattare o localizzare un individuo (ad es. cliente o venditore) o per identificare un individuo nel contesto. Ciò include, ma non è limitato a, nome, indirizzo fisico, indirizzo e-mail, numero di telefono, contenuto di un messaggio regalo, risposte a un sondaggio, dettagli di pagamento, acquisti, cookie, impronta digitale (ad es. browser, dispositivo utente), di un cliente o venditore, Indirizzo IP, geolocalizzazione o identificatore del prodotto del dispositivo connesso a Internet.

j. **Sviluppatore**: soggetto giuridico che ha sviluppato l'Applicazione presente nell'Apps Market e/o il Tema presente nel Theme Store.
k. **Tema o tema grafico**: insieme di file che lavorano assieme per creare l'interfaccia grafica di un sito web installabile dall'Utente Venditore gratuitamente o a pagamento, a seconda delle condizioni d'uso dello stesso tema, accedendo al theme store
l. **Theme Store**: spazio virtuale allocato presso la piattaforma attraverso il quale l'Utente Venditore può installare sul proprio sito i temi grafici offerti in vendita dai singoli Sviluppatori oppure installare sul proprio sito i temi grafici offerti a titolo gratuito dai singoli Sviluppatori.
m. **Utente Venditore**: utente che utilizza la piattaforma per offrire in vendita online i propri prodotti e/o servizi.

3. DURATA

3.1. L'Accordo dura a tempo indeterminato. Ciascuna Parte può recedere dall'Accordo dando comunicazione scritta da inviare all'altra Parte con un preavviso di almeno 30 giorni. La comunicazione è efficace quando giunge a destinazione della Parte ricevente.

4. PAGAMENTO

4.1. L'Applicazione o il Tema possono essere disponibili rispettivamente presso l'Apps Market o il Theme Store per essere scaricati dall'Utente Venditore a titolo gratuito oppure oneroso.

4.2. Nell'ipotesi di Applicazione o Tema scaricabile a titolo oneroso, la relativa somma pagata tramite la piattaforma dall'Utente Venditore verrà così suddivisa tra le Parti: 80% allo Sviluppatore (**Importo**) e 20% alla Società. Contestualmente all'acquisto dell'Applicazione o del Tema da parte dell'Utente Venditore, la Società accrediterà direttamente l'Importo sull'account di quest'ultimo in essere sulla piattaforma. Successivamente, lo Sviluppatore potrà disporre il trasferimento dei fondi presso un conto esterno alla piattaforma.

4.3. Qualora l'Importo raggiunga almeno un ammontare pari o superiore ad euro 250,00 (oltre iva), lo Sviluppatore potrà emettere fattura nei confronti della Società per l'importo a lui dovuto, e così di volta in volta per gli Importi successivi. La Società si impegna a saldare la fattura nei successivi 30 giorni, decorrenti dalla ricezione della fattura.

4.4 All'Importo sarà applicata la normativa vigente ai fini Iva che, assieme a qualunque altro onere fiscale derivante dall'esecuzione del Contratto, sarà a carico dello Sviluppatore.

5. DIRITTI, IMPEGNI E DICHIARAZIONI DELLO SVILUPPATORE

5.1. Lo Sviluppatore:

a. si impegna a manlevare e tenere indenne la Società da qualsiasi reclamo o azione legale, intrapresa innanzi a qualsiasi tipo di autorità, che qualsiasi Utente Venditore, suo cliente o qualsiasi utente di internet abbia promosso in relazione a qualsiasi tipo di danno o pregiudizio subìto in occasione dell'uso dell'Applicazione o del Tema;

b. dichiara che l'Applicazione rispetta il Reg. (UE) 679/2016 in materia di protezione dei dati personali (GDPR), il d. lgs 196/2003 (Codice della Privacy) e il d. lgs 206/2005 (Codice del Consumo), così come qualsiasi normativa applicabile alla prestazione dei servizi o alla vendita dei prodotti cui l'Applicazione si riferisce.
c. si assume ogni responsabilità in ordine al contenuto delle informazioni inserite all'interno della propria Applicazione o che transitano attraverso l'Applicazione o del Tema manlevando espressamente la Società da ogni responsabilità ed onere di accertamento e/o controllo al riguardo. E' pertanto esclusa ogni responsabilità della Società in ipotesi di pubblicazione non autorizzata di informazioni da parte dello Sviluppatore o di un utilizzo dei Servizi non conforme alle presenti Condizioni Generali per gli Sviluppatori e/o alla legge.
d. garantisce che qualunque informazione, immagine, materiale o messaggio, in qualunque formato (sia audio che video o altro), dallo stesso eventualmente immesso in aree pubbliche o private dell'Applicazione o del Tema è e sarà di titolarità dello Sviluppatore e/o nella sua legittima disponibilità.
e. si impegna a tenere indenne la Società ed i terzi eventualmente coinvolti, sostanzialmente e processualmente, da ogni perdita, danno (anche da lucro cessante e danno emergente), responsabilità, costo o spesa, incluse le spese legali, derivanti da ogni violazione di quanto stabilito nelle presenti Condizioni Generali per gli Sviluppatori.

f. si impegna a nominare Projectmoon sub-responsabile del trattamento ai sensi dell'art. 28 del GDPR, come da atto di nomina (**DPA**) che costituisce allegato al presente documento.

5.2. Rispetto delle Policy Amazon Marketplace Web Service:

Lo Sviluppatore si impegna al rispetto di quanto indicato da Amazon Marketplace Web Service (**Amazon MWS**) nella Data Protection Policy di Amazon Marketplace Web Service (Amazon MWS) Documentation , come visionabile al seguente link: https://docs.developer.amazonservices.com/en_US/dev_guide/DG_DataProtectionPolicy.html , così come di volta in volta modificata. In particolare, lo Sviluppatore si impegna a mantenere garanzie amministrative e tecniche nonché ogni altra idonea misura di sicurezza per (i) mantenere la sicurezza e la riservatezza delle Informazioni Amazon accessibili, raccolte, utilizzate, archiviate o trasmesse dallo Sviluppatore o da terzi e (ii) proteggere tali Informazioni Amazon da minacce o pericoli noti o ragionevolmente prevedibili per la loro sicurezza e integrità, perdita accidentale, alterazione, divulgazione e tutte le altre forme illecite di elaborazione . Senza limitazioni, lo Sviluppatore si impegna al rispetto dei seguenti requisiti:

1. **Protezione della rete**: lo Sviluppatore deve implementare controlli di protezione della rete (ad esempio, reti/gruppi di sicurezza AWS VPC, firewall di rete) per negare l'accesso a indirizzi IP non autorizzati; l'accesso pubblico deve essere limitato solo agli utenti approvati.
2. **Gestione degli accessi**: Lo Sviluppatore deve assegnare un ID univoco a ogni persona che acceda da computer a Informazioni Amazon. Lo Sviluppatore non deve creare o utilizzare credenziali di accesso o account utente generici, condivisi o predefiniti. Lo Sviluppatore deve implementare meccanismi di riferimento per garantire che in ogni momento solo gli account utente richiesti accedano a Informazioni Amazon. Lo Sviluppatore deve rivedere su base regolare (almeno trimestralmente) l'elenco di persone e servizi con accesso a Informazioni Amazon e rimuovere gli account che non richiedono più l'accesso. Lo Sviluppatore deve impedire ai propri dipendenti di archiviare i dati di Amazon sui dispositivi personali. Lo Sviluppatore mantiene e applica il "blocco

dell'account" rilevando modelli di utilizzo anomali e tentativi di accesso e disabilitando gli account con accesso alle Informazioni Amazon, se necessario.

3. **Crittografia in transito**: Lo Sviluppatore deve crittografare tutte le informazioni di Amazon in transito (ad esempio, quando i dati attraversano una rete o vengono inviati in altro modo tra host. Ciò può essere ottenuto utilizzando HTTP su TLS (HTTPS). Lo Sviluppatore deve applicare questo controllo di sicurezza su tutti gli endpoint esterni applicabili utilizzati da clienti, nonché i canali di comunicazione interni (es. canali di propagazione dei dati tra i nodi del livello di storage, connessioni a dipendenze esterne) e gli strumenti operativi. Lo Sviluppatore deve disabilitare i canali di comunicazione che non forniscono la crittografia in transito anche se non utilizzati (es., rimuovendo il relativo codice non attivo, configurando le dipendenze solo con canali crittografati e limitando le credenziali di accesso all'uso di canali crittografati), utilizzando AWS Encryption SDK) in cui la crittografia del canale (ad es. utilizzando TLS) termina in hardware multi-tenant non attendibile (ad es. proxy non attendibili).
4. **Piano di risposta agli incidenti di sicurezza**: Lo Sviluppatore deve creare e gestire un piano e/o un runbook per rilevare e gestire gli incidenti di sicurezza. Tali piani devono identificare i ruoli e le responsabilità di risposta agli incidenti, definire i tipi di incidenti che possono avere un impatto su Amazon, definire le procedure di risposta agli incidenti per i tipi di incidenti definiti e definire un percorso e procedure di escalation per inoltrare gli incidenti di sicurezza ad Amazon. Lo Sviluppatore deve rivedere e verificare il piano ogni sei (6) mesi e dopo qualsiasi modifica importante dell'infrastruttura o del sistema. Lo Sviluppatore deve indagare su ogni incidente di sicurezza e documentare la descrizione dell'incidente, le azioni correttive e i relativi controlli di processo/sistema correttivi implementati per prevenire il ripetersi futuro (se applicabile). Lo Sviluppatore deve mantenere la catena di custodia per tutte le prove o i record raccolti,
   Lo Sviluppatore deve informare Amazon (via e-mail a 3p-security@amazon.com) entro 24 ore dal rilevamento di eventuali incidenti di sicurezza. Lo Sviluppatore non può notificare alcuna autorità di regolamentazione, né alcun cliente, per conto di Amazon, a meno che Amazon non richieda espressamente per iscritto che lo sviluppatore lo faccia. Amazon si riserva il diritto di rivedere e approvare la forma e il contenuto di qualsiasi notifica prima che venga fornita a qualsiasi parte, a meno che tale notifica non sia richiesta dalla legge, nel qual caso Amazon si riserva il diritto di rivedere la forma e il contenuto di qualsiasi notifica prima che venga fornito a qualsiasi parte. Lo Sviluppatore deve informare Amazon entro 24 ore quando i loro dati vengono richiesti in risposta a procedimenti legali o dalla legge applicabile.
5. **Richiesta di cancellazione o restituzione**: Lo Sviluppatore deve prontamente (ma entro non più di 72 ore dalla richiesta di Amazon), eliminare in modo permanente e sicuro (in conformità con i processi di sanificazione standard del settore, ad es. NIST 800-88) o restituire le Informazioni Amazon su e in conformità con l'avviso di Amazon che richiede la cancellazione e/o la restituzione. Lo Sviluppatore deve inoltre eliminare in modo permanente e sicuro tutte le istanze live (online o accessibili in rete) inerenti Informazioni Amazon entro 90 giorni dalla notifica di Amazon. Se richiesto da Amazon, lo Sviluppatore certificherà per iscritto che tutte le Informazioni Amazon sono state distrutte in modo sicuro.

5.3. Requisiti di sicurezza aggiuntivi specifici per le informazioni di identificazione personale.

Lo Sviluppatore si impegna al rispetto dei seguenti requisiti di sicurezza aggiuntivi, con riferimento a quanto richiesto da Amazon MWS. I seguenti requisiti di sicurezza aggiuntivi devono essere soddisfatti per tutte le PII. Se un'API di Marketplace contiene PII o le PII sono combinate con non PII, l'intero archivio dati deve soddisfare i seguenti requisiti:

1. **Conservazione e recupero dei dati**. Lo Sviluppatore conserva le PII solo allo scopo e per il tempo necessario per evadere gli ordini (non oltre 30 giorni dopo la spedizione dell'ordine) o per calcolare/rimettere le tasse. Se uno Sviluppatore è obbligato per legge a conservare copie di archivio delle PII per scopi fiscali o regolamentari simili, queste Informazioni Amazon archiviate devono essere archiviate come backup "freddo" o offline (ad esempio, non disponibile per uso immediato o interattivo) archiviato in una struttura sicura e tutti i dati archiviati sui supporti di backup devono essere crittografati. Nel caso in cui le PII vengano perse, lo Sviluppatore deve essere in grado di recuperare tutte le PII perse (ovvero, i dati vengono cancellati o non sono disponibili per l'elaborazione a causa di un arresto anomalo del sistema o ransomware).
2. **Governance dei dati**: Lo Sviluppatore deve creare, documentare e rispettare una politica sulla privacy e sulla gestione dei dati per le loro applicazioni o servizi che regolino la condotta appropriata e i controlli tecnici da applicare nella gestione e protezione delle risorse informative. Lo Sviluppatore deve tenere un inventario di software e risorse fisiche (ad es. computer, dispositivi mobili) con accesso alle PII e aggiornarlo regolarmente. Dovrebbe essere mantenuto un registro delle attività di elaborazione dei dati come campi di dati specifici e come vengono raccolti, elaborati, archiviati, utilizzati, condivisi e smaltiti per tutte le informazioni PII per stabilire la responsabilità e la conformità alle normative. Lo Sviluppatore deve stabilire e rispettare la loro politica sulla privacy per il consenso del cliente e i diritti sui dati per accedere, rettificare, cancellare,
3. **Crittografia e archiviazione**: Lo Sviluppatore deve crittografare tutte le PII non in uso (ad esempio, quando i dati sono persistenti) utilizzando gli standard di best practice del settore (ad esempio utilizzando AES-128, AES-256 o RSA con chiave di 2048 bit (o superiore). I materiali crittografici (ad esempio chiavi di crittografia/decrittografia) e capacità crittografiche (ad es. daemons che implementano Trusted Platform Module virtuali e forniscono API di crittografia/decrittografia) utilizzate per la crittografia delle PII a riposo devono essere accessibili solo ai processi e servizi dello Sviluppatore. Lo Sviluppatore non deve memorizzare le PII in supporti rimovibili (ad es. USB) o applicazioni cloud pubbliche non protette (ad es. collegamenti pubblici resi disponibili tramite Google Drive) Lo Sviluppatore deve smaltire in modo sicuro tutti i documenti stampati contenenti PII.
4. **Principio del minimo privilegio**: Lo Sviluppatore deve implementare adeguati meccanismi di controllo per consentire la concessione di diritti a qualsiasi parte che utilizza l'Applicazione (ad esempio, l'accesso a uno specifico set di dati a sua custodia) e agli operatori dell'Applicazione (ad esempio, l'accesso a specifiche API di configurazione e manutenzione come kill switch) seguendo il principio del privilegio minimo. Le sezioni o le funzionalità dell'applicazione che vendono PII devono essere protette da un ruolo di accesso univoco e l'accesso deve essere concesso in base alla "necessità di sapere".

5. **Registrazione e monitoraggio**: Lo Sviluppatore deve raccogliere i log per rilevare eventi relativi alla sicurezza (ad es. accesso e autorizzazione, tentativi di intrusione, modifiche alla configurazione) nelle proprie applicazioni e sistemi. Lo Sviluppatore deve implementare questo meccanismo di registrazione su tutti i canali (ad es. API di servizio, API a livello di storage, dashboard amministrative) che forniscono l'accesso alle informazioni di Amazon. Tutti i registri devono avere controlli di accesso per impedire qualsiasi accesso non autorizzato e manomissione durante il loro ciclo di vita. I log stessi non devono contenere PII e devono essere conservati per almeno 90 giorni come riferimento in caso di incidente di sicurezza. Lo Sviluppatore deve creare meccanismi per monitorare i registri e tutte le attività di sistema per attivare allarmi investigativi su azioni sospette (ad es. chiamate multiple non autorizzate, tasso di richieste impreviste e volume di recupero dei dati e accesso ai record di dati canary). Lo Sviluppatore dovrebbe eseguire indagini quando vengono attivati gli allarmi di monitoraggio e questo dovrebbe essere documentato nel Piano di risposta agli incidenti dello sviluppatore.

5.4. Audit.

Lo Sviluppatore deve conservare tutti i libri e i registri appropriati ragionevolmente necessari per verificare la conformità con la AWS Acceptable Use Policy (https://aws.amazon.com/it/aup/), con la Data Protection Policy di Amazon MWS di cui al punto 5.2, e con l'Accordo per gli sviluppatori di Amazon Marketplace durante il periodo di questo contratto e per i 12 mesi successivi. Su richiesta scritta di Amazon o di Projectmoon, lo Sviluppatore deve certificare per iscritto ad Amazon e/o Projectmoon di essere conforme a queste politiche.

Su richiesta, Amazon e/o Projectmoon può, o può far sì che una società di contabilità pubblica certificata indipendente selezionata da Amazon e/o Projectmoon, controlli e ispezioni i libri, i registri, le strutture, le operazioni e la sicurezza di tutti i sistemi coinvolti nell'applicazione di uno Sviluppatore nel recupero, nell'archiviazione o elaborazione delle informazioni di Amazon e/o Projectmoon. Lo Sviluppatore deve cooperare con Amazon e/o Projectmoon o il revisore di Amazon e/o Projectmoon in relazione alla verifica, che può avvenire presso le strutture dello Sviluppatore e/o delle strutture del subappaltatore. Se l'audit rivela carenze, violazioni e/o mancato rispetto dei nostri termini, condizioni o politiche, lo Sviluppatore deve, a proprie spese e spese, e intraprendere tutte le azioni necessarie per rimediare a tali carenze entro un periodo di tempo concordato.

5.5. Policy di Amazon AWS

Lo Sviluppatore si impegna al rispetto della AWS Acceptable Use Policy dei servizi web offerti da Amazon Web Service, Inc. (**Amazon AWS**), visionabile al seguente link: https://aws.amazon.com/it/aup/ . A titolo esemplificativo, ma non esaustivo, lo Sviluppatore si impegna quindi a non porre in essere:

- **Nessun uso o contenuto illegale, dannoso o offensivo**, a non utilizzare, incoraggiare, promuovere, facilitare o istruire altri a utilizzare i servizi o il sito AWS per usi illegali, dannosi, fraudolenti, illeciti o offensivi, o per trasmettere, archiviare, visualizzare, distribuire o altrimenti rendere disponibile contenuto che è illegale, dannoso, fraudolento, illecito o offensivo;
- **Nessuna violazione della sicurezza**. Le attività vietate includono: accesso non autorizzato (accedere o utilizzare qualsiasi sistema senza autorizzazione, incluso il tentativo di sondare, scansionare o testare la vulnerabilità di un sistema o di violare qualsiasi misura di sicurezza o autenticazione utilizzata da un sistema), Intercettazione (monitoraggio dei dati o del traffico su un sistema senza autorizzazione), falsificazione dell'origine (falsificazione di intestazioni di pacchetti

TCP-IP, intestazioni di posta elettronica o qualsiasi parte di un messaggio che ne descriva l'origine o il percorso. L'uso legittimo di alias e remailer anonimi non è vietato da questa disposizione);

- **Nessun abuso di rete**. Le attività vietate includono: monitoraggio o scansione di un sistema che compromette o interrompe il sistema monitorato o sottoposto a scansione, Denial of Service (DoS) ("spammare" un target con richieste di comunicazione in modo che il target non possa rispondere al traffico legittimo o risponda così lentamente da diventare inefficace), interferenza intenzionale (interferire con il corretto funzionamento di qualsiasi sistema, incluso qualsiasi tentativo deliberato di sovraccaricare un sistema tramite mail bombing, news bombing, attacchi broadcast o tecniche di flooding;
- **Nessun abuso di e-mail o altri messaggi**

6. DIRITTI DELLA SOCIETA'

6.1. La Società si riserva il diritto di sospendere, anche a tempo indeterminato, la pubblicazione dell'Applicazione sull'Apps Market o del Tema nel Theme Store qualora lo Sviluppatore abbia violato qualsiasi norma delle presenti Condizioni Generali per gli Sviluppatori oppure qualora qualsiasi garanzia o dichiarazione prestata dallo Sviluppatore ai sensi delle presenti Condizioni Generali per gli Sviluppatori si sia rivelata non corretta o falsa, anche parzialmente.

6.2. Salvo il diritto al risarcimento del danno, la Società si riserva il diritto di risolvere l'Accordo ai sensi dell'art. 1453 c.c. qualora lo Sviluppatore abbia violato uno o più impegni previsti dalle presenti Condizioni Generali per gli Sviluppatori.

6.3. Lo sviluppatore rinuncia a promuovere qualsiasi tipo di azione giudiziale per qualsiasi ipotesi di danno o pregiudizio subìto a seguito della sospensione della pubblicazione dell'Applicazione sull'Apps Market o del Tema nel Theme Store effettuata ai sensi dell'articolo 6.1 e/o per la risoluzione dell'Accordo ai sensi dell'articolo 6.2 ovvero per la risoluzione a qualsiasi titolo dell'Accordo effettuata dalla Società.

7. CONTENUTO VIETATO

7.1. Fermo restando quanto indicato all'articolo 8 in tema di diritti di privativa, è vietata la pubblicazione sull'Apps Market e nel Theme Store di Applicazioni e Temi che abbiano un contenuto o che rimandino, in qualsiasi modo e forma, a un contenuto che:

a. abbia riferimenti sessuali, pornografici e/o pedopornografici;
b. inciti all'odio, alla discriminazione di genere, religiosa o politica o alla violenza;
c. favorisca la vendita o l'uso di prodotti pericolosi per la salute degli utenti, o di prodotti la cui vendita è vietata dalla legge italiana o da provvedimenti o sentenze assunti da qualsiasi tipo di autorità;
d. favorisca o promuova qualsiasi tipo di attività vietata dalla legge italiana o da provvedimenti o sentenze assunti da qualsiasi tipo di autorità.

7.2. E' vietata la pubblicazione nell'Apps Market e nel Theme Store di Applicazioni e di Temi che carpiscono qualsiasi tipo di dato, monitorino in segreto o danneggiano gli Utenti Venditori o i loro clienti o comunque gli utenti di internet o che siano in qualsiasi modo dannose.

8. DIRITTI DI PRIVATIVA

8.1. Lo Sviluppatore dichiara che l'Applicazione e il Tema:

a. non ha violato e non vìola nessun diritto d'autore di terzi, sia in base alla legge 633/1942 sul diritto d'autore, sia in base a qualsiasi altra normativa italiana o straniera posta a tutela del diritto d'autore;
b. non ha violato e non vìola nessun diritto di proprietà industriale, sia in base al Codice della Proprietà Industriale, sia in base a qualsiasi altra normativa italiana o straniera posta a tutela della proprietà intellettuale ed industriale.

8.2. Lo Sviluppatore riconosce e accetta, pertanto, che è vietata la pubblicazione sull'Apps Market e nel Theme Store di Applicazioni e Temi che violano i diritti di proprietà intellettuale di altri (inclusi i diritti relativi a marchi, copyright, brevetti, segreti industriali e altri diritti di proprietà). Sono inoltre vietate le Applicazioni e i Temi che istigano o inducono alla violazione di diritti di proprietà intellettuale. Allo Sviluppatore potrebbe essere chiesto dalla Società di fornire prove a dimostrazione dei suoi diritti di utilizzo dei contenuti protetti da copyright.

8.3. Lo Sviluppatore dichiara di aver ottenuto qualsiasi tipo di autorizzazione da qualsiasi titolare del diritto d'autore e/o del diritto industriale eventualmente necessaria per creare l'Applicazione e/o per pubblicarla sull'Apps Market nonchè per creare il Tema e/o pubblicarlo nel Theme Store. La Società non è responsabile nei confronti degli Utenti Venditori e dei terzi per l'eventuale mancanza di tali autorizzazioni.

8.4. Lo Sviluppatore si impegna a tenere indenne e manlevare la Società da qualsiasi responsabilità connessa alla violazione delle dichiarazioni contenute in questo articolo 8.

9. RISERVATEZZA

9.1. Ciascuna delle Parti riconosce e prende atto che essa e/o i suoi rispettivi incaricati potrebbero venire a conoscenza di Informazioni Confidenziali (come infra definite) relative all'altra Parte (ovvero, ove applicabile e rilevante, a società facenti parti del Gruppo a cui appartiene l'altra Parte) che, se rivelate, potrebbero causare un danno all'altra Parte e/o a terzi. Per tale motivo, ciascuna Parte si obbliga a mantenere ed a far sì che i propri dipendenti, collaboratori, anche esterni, e/o incaricati mantengano riservate tali Informazioni Confidenziali. Queste restrizioni non saranno applicabili a: (i) comunicazioni e/o dichiarazioni richieste per ordine dell'autorità giudiziaria, o di altra autorità competente; (ii) qualsiasi informazione che sia o sia divenuta di pubblico dominio, senza che si siano verificate violazioni del presente articolo; (iii) informazioni riguardanti una Parte, che vengano richieste all'altra da legali di terzi, i quali minaccino un'azione giudiziaria nei confronti di una delle Parti, laddove la minaccia sia ragionevolmente fondata e argomentata; (iv) informazioni rispetto alle quali la Parte interessata ha dato il proprio preventivo, espresso consenso scritto a che siano rivelate a terzi.

9.2. Per "Informazioni Confidenziali" si intendono, in particolare:

- qualsiasi elemento di conoscenza, dato o informazione che includa o riguardi dati tecnici o non-tecnici, algoritmi, logiche, formule, composizioni, devices, metodi, segreti aziendali, know-how, tecniche, progetti (cc.dd. blueprints), bozze, modelli, materiale mock-up, procedure, presentazioni, miglioramenti, sviluppi, strutture, schemi, disegni, manuali, dati finanziari, concepts, business plans, roadmaps;

- dati relativi alla piattaforma che non siano di pubblico dominio, siano essi sottoforma di scritto, di materiale video, audio e/o verbale;

- ricerche, statistiche, indagini e approfondimenti, nonché il relativo materiale verbale o scritto;

- documentazione inviata tramite posta, email, ambienti, sistemi condivisi, online e/o tramite accesso riservato con login/password;

- eventuali codici login o password;

- qualsiasi elemento di conoscenza, dato o informazione che includa o riguardi i servizi, l'ambito di competenza e/o di operatività, l'azienda, i clienti e/o il personale di ciascuna delle Parti.

9.3. La Parte che venga a conoscenza di un'Informazione Confidenziale si impegna a custodirla, mantenerla strettamente riservata, trattarla con la medesima cura con cui tratterebbe una propria informazione confidenziale, rivelarla, al proprio interno, esclusivamente ai soggetti che ne debbano necessariamente venire a conoscenza per ragioni di cui alla presente scrittura e nei limiti dello stesso (fatti salvi i casi in cui l'informazione debba essere rivelata, per ragioni di servizio, a consulenti esterni della Parte, quali legali, commercialisti, fiscalisti, etc.), non usarla, nemmeno in parte, per scopi diversi da quelli previsti dalla presente scrittura nonché in base al progetto descritto in premessa, e comunque a non rivelarla a terzi per tutta la durata dell'Accordo, nonché successivamente alla cessazione, per qualsiasi causa, di tale Accordo. In ogni caso, qualsiasi Informazione Confidenziale comunicata da una Parte all'altra rimarrà di proprietà della Parte che l'ha comunicata e potrà essere riconsegnata, previa sua esplicita richiesta, a quest'ultima alla cessazione, per qualsiasi causa, della collaborazione e non dovrà essere interpretata nel senso che essa conferisca, direttamente o indirettamente, alla Parte che la riceve qualsivoglia diritto in relazione a dati, informazioni, diritti, materiali o altri contenuti in genere che siano di proprietà della Parte che ha comunicato tale informazione.

9.4. Ciascuna Parte si impegna a non rivelare a terzi alcun tipo di informazioni relative ai clienti dell'altra Parte.

10. RUOLO DELLA SOCIETA'. LIMITAZIONI DI RESPONSABILITA'

10.1. Resta espressamente inteso che la Società non controlla né sorveglia come gli utenti utilizzano o hanno intenzione di utilizzare l'Applicazione o il Tema dello Sviluppatore.

10.2. La Società:

a. non controlla né sorveglia le informazioni e/o i dati e/o i contenuti immessi dagli utenti attraverso l'Applicazione o il Tema dello Sviluppatore;

b. ha la facoltà di offrire in vendita sull'Apps Market e nel Theme Store applicazioni e temi anche di terze parti, ancorché concorrenti dello Sviluppatore;

c. non può essere ritenuta responsabile nel caso di ritardi, malfunzionamenti e/o interruzioni nell'erogazione dei servizi offerti dalla Applicazione o dal Tema dipesi da guasti o malfunzionamenti dipendenti da causa di forza maggiore,caso fortuito o fatto non riconducibile alla Società.

10.3 Lo Sviluppatore si impegna a tenere indenne e manlevata Projectmoon da qualsiasi contestazione, violazione, danno, richiesta di risarcimento e/o responsabilità derivante

dalla violazione degli impegni dello sviluppatore di cui agli artt. 5 e 7 delle presenti Condizioni Generali per gli Sviluppatori.

11. MODIFICHE

11.1. La Società si riserva il diritto di modificare in qualsiasi momento il contenuto delle Condizioni Generali per gli Sviluppatori. In questa circostanza, la Società trasmetterà per e-mail allo Sviluppatore il contenuto delle nuove Condizioni Generali per gli Sviluppatori e lo Sviluppatore avrà tempo 10 giorni per comunicare di non voler accettare le modifiche effettuate dalla Società: in questo caso, l'Accordo si riterrà sciolto a far data dalla comunicazione dello Sviluppatore. Se lo Sviluppatore non trasmette la comunicazione entro i 10 giorni le modifiche si intenderanno accettate.

11.2. Fermo quanto sopra, la Società si riserva il diritto di variare le caratteristiche tecniche, i sistemi, le risorse ed i servizi della piattaforma in conseguenza della normale evoluzione tecnologica delle componenti hardware e software.

12. AUTONOMIA DELLE PARTI

12.1. La Società e lo Sviluppatore agiscono in piena autonomia ed indipendenza. Il presente Accordo non fa sorgere tra loro alcun rapporto di collaborazione, joint-venture, agenzia, associazione, intermediazione o lavoro subordinato o qualsiasi altro rapporto diverso da quello specificatamente disciplinato dal presente Accordo.

13. RECAPITI

13.1. Ogni comunicazione alla Società da parte dello Sviluppatore dovrà essere effettuata ai seguenti recapiti: (a) Projectmoon s.r.l., Via Roma 4/18, 31020 - Villorba (TV); (b) e-mail: info@projectmoon.it; PEC: projectmoon@pec.projectmoon.it.

14. LEGGE APPLICABILE E FORO COMPETENTE.

14.1 Le presenti Condizioni Generali per gli Sviluppatori sono disciplinate dalla legge italiana. Per qualsiasi causa derivante dalla loro applicazione e/o interpretazione è esclusivamente e inderogabilmente competente il Foro di Treviso.

Data Protection Agreement (DPA) o Nomina a Sub-Responsabile del Trattamento o Addendum

Ai sensi dell'art. 5.1 f. delle Condizioni Generali per gli Sviluppatori le Parti si impegnano a quanto previsto dalla presente

DPA

o

NOMINA A SUB-RESPONSABILE ESTERNO DEL TRATTAMENTO AI SENSI DELL'ART. 28 DEL REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO DEL 27.4.2016 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 - "GDPR") (**Nomina a Sub-Responsabile del Trattamento** o **Addendum**)

stipulata tra

Projectmoon s.r.l., con sede in Via Roma 4/18, 31020 - Villorba (TV) (partita iva 04214670269), in qualità di Sub-Responsabile del Trattamento dei dati personali (**Sub-Responsabile del Trattamento**), in persona del suo legale rappresentante

e

la diversa parte del presente Addendum**,** di seguito **Responsabile del Trattamento** o **Sviluppatore**, in persona del suo legale rappresentante

(il Responsabile del Trattamento e il Sub-Responsabile del Trattamento congiuntamente, le "**Parti**").

I. Oggetto

Le presenti clausole hanno come oggetto la definizione delle condizioni alle quali il Sub-Responsabile del Trattamento si impegna a effettuare per conto del Responsabile del Trattamento le operazioni di Trattamento dei Dati Personali qui di seguito definite.

Nell'ambito delle loro relazioni contrattuali le Parti si impegnano a rispettare la Normativa sulla Protezione dei Dati Personali di tempo in tempo applicabile e, in particolare, il GDPR.

II. Definizioni

"**Accordo**": le Condizioni Generali per gli Sviluppatori in essere tra il Responsabile del Trattamento e il Sub-Responsabile del Trattamento e di cui il presente documento costituisce un addendum. Le definizioni presenti nelle Condizioni Generali per gli Sviluppatori devono intendersi qui integralmente riprese.

"**Addendum**": il presente documento, incluso ogni suo eventuale allegato.

"**Dati Personali**": i dati personali, come definiti dall'art. 4.1 del GDPR, oggetto del presente Addendum.

"**GDPR**": il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 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).

"**Interessato**": ha il significato di cui all'art. 4.1 del GDPR.

"**Normativa sulla Protezione dei Dati Personali"**: significa qualsiasi legge o regolamento, inclusi le leggi e i regolamenti dell'Unione europea, degli Stati membri e di UK, applicabile al trattamento dei Dati Personali, incluso il GDPR.

"**Sub-Responsabile del Trattamento**": ha il significato di cui all'art. 4.8 del GDPR.

"**Responsabile del Trattamento**": ha il significato di cui all'art. 4.7 del GDPR.

"**Trattamento**": ha il significato di cui all'art. 4.2 del GDPR.

"**Violazione dei Dati Personali**": ha il significato di cui all'art. 4.12 del GDPR.

III. Descrizione del Trattamento demandato al Sub-Responsabile del Trattamento

Il Sub-Responsabile del Trattamento è autorizzato a trattare per conto del Responsabile del Trattamento i Dati Personali necessari per adempiere all'Accordo ("**Servizi**").

Le operazioni di Trattamento demandate al Sub-Responsabile del Trattamento sono le seguenti:

- Conservazione
- Consultazione
- Uso
- Organizzazione
- Estrazione
- Raccolta

La finalità del Trattamento demandato al Sub-Responsabile del Trattamento è unicamente quella di dare esecuzione all'Accordo, prestando i Servizi.

Le categorie di Dati Personali il cui Trattamento è demandato al Sub-Responsabile del Trattamento sono le seguenti:

- Nome
- Cognome
- Indirizzo di residenza
- Indirizzo di domicilio
- CAP
- E-mail
- Numero di telefono
- Nazione
- Codice fiscale
- PII
- Informazioni Amazon.

Le categorie di Interessati a cui si riferiscono i Dati Personali il cui trattamento è demandato al Sub-Responsabile del Trattamento sono i clienti o potenziali clienti del Responsabile del Trattamento.

IV. Durata dell'Addendum

Il presente Addendum produce effetti a partire dalla sua sottoscrizione e per tutta la durata dell'Accordo, sicché, cessato l'Accordo, per qualsiasi causa, cesseranno anche, immediatamente, gli effetti del presente Addendum. Gli obblighi relativi alla riservatezza e i divieti di diffusione e/o comunicazione dovranno essere osservati dal Sub-Responsabile del Trattamento anche dopo la cessazione dell'Accordo e del presente Addendum.

V. Obbligazioni del Sub-Responsabile del Trattamento nei confronti del Responsabile del Trattamento

Il Sub-Responsabile del Trattamento si obbliga:

- a trattare i Dati Personali unicamente per la finalità di cui al presente Addendum e, in particolare, come indicato al punto III che precede, solo ed esclusivamente ai fini della corretta esecuzione dell'Accordo e della corretta prestazione dei Servizi, conseguentemente;

- a non comunicare, diffondere, rivelare, in qualsiasi modo, i Dati Personali a terzi, ad eccezione dei responsabili ulteriori del trattamento, qualora designati dal Sub-Responsabile del Trattamento conformemente all'art. 28 GDPR e all'art. VI che segue, e delle persone autorizzate al trattamento dei dati personali sotto l'autorità del Sub-Responsabile del Trattamento ("**Incaricati**"), qualora essi siano istruiti in tal senso dal Sub-Responsabile del Trattamento, conformemente a quanto indicato dall'art. 29 GDPR, e siano formalmente designati dallo stesso, a norma del presente articolo;
- trattare i Dati Personali conformemente alle istruzioni eventualmente fornite dal Responsabile del Trattamento ("**Istruzioni**"), anche in caso di trasferimento di Dati Personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o il diritto nazionale cui è soggetto il Sub-Responsabile del Trattamento; in tal caso, il Sub-Responsabile del Trattamento informa il Responsabile del Trattamento di tale obbligo giuridico prima del Trattamento, a meno che il diritto dell'Unione o dello Stato membro in questione vietino tale informazione per rilevanti motivi di interesse pubblico. Se il Sub-Responsabile del Trattamento ritiene che un'istruzione costituisca una violazione del GDPR e/o di un'altra disposizione del diritto dell'Unione o del diritto di uno degli Stati membri relativa alla protezione dei dati personali, il Sub-Responsabile del Trattamento ne dovrà dare immediata comunicazione al Responsabile del Trattamento.

VI. Ulteriori responsabili del Trattamento

Autorizzazione generale

Il Responsabile del Trattamento autorizza il Sub-Responsabile del Trattamento, in via generale, a ricorrere a un altro Sub-Responsabile del Trattamento ("**Responsabile Ulteriore del Trattamento**" o "**Sub-Responsabile**") per l'esecuzione di specifiche attività di trattamento, ai sensi dell'art. 28.2 del GDPR.

VII. Informativa da fornire all'interessato

Spetta al Responsabile del Trattamento fornire agli Interessati le informazioni di cui agli artt. 13 e 14 del GDPR, nei casi, con le modalità e con le tempistiche di cui a tali articoli e all'art. 12 del GDPR.

VIII. Conservazione dei Dati Personali durante la vigenza dell'Addendum e loro cancellazione o restituzione dopo la sua cessazione

Durante la vigenza dell'Addendum, il Sub-Responsabile del Trattamento si obbliga a conservare i Dati Personali solo ed esclusivamente per il tempo strettamente necessario al conseguimento delle finalità del Trattamento e per il corretto adempimento degli obblighi di cui all'Addendum, come indicato dal Responsabile del Trattamento nelle Istruzioni, fatta salva la necessità di conservare i Dati Personali in ragione di obblighi imposti al Sub-Responsabile del Trattamento dal diritto dell'Unione o dello Stato membro cui è soggetto.

In caso di cessazione, per qualsiasi causa, dell'Addendum, il Sub-Responsabile del Trattamento si obbliga a:

a) cessare il Trattamento; e

b) fatti salvi gli obblighi di conservazione dei Dati Personali imposti al Sub-Responsabile del Trattamento dal diritto dell'Unione o dello Stato membro cui è soggetto, a scelta del Responsabile del Trattamento, nel termine di 90 giorni lavorativi:

- distruggere e/o cancellare tutti i Dati Personali, in modo irreversibile e permanente e, comunque, sulla base delle Istruzioni; o
- restituire tutti i Dati Personali; o
- inviare i Dati Personali a un Sub-Responsabile del Trattamento indicato dal Responsabile del Trattamento.

La restituzione o l'invio devono essere accompagnati dalla cancellazione e/o distruzione di tutte le copie esistenti nei sistemi informativi del Sub-Responsabile del Trattamento, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione di tali dati. Una volta distrutti, il Sub-Responsabile del Trattamento dovrà giustificare per iscritto la distruzione.

IX. Responsabile per la protezione dei dati personali (o *Data Protection Officer* - "DPO")

Il Sub-Responsabile del Trattamento informare il Responsabile del Trattamento che ha nominato un DPO.

X. Documentazione

Il Sub-Responsabile del Trattamento mette a disposizione del Responsabile del Trattamento tutte le informazioni e la documentazione necessarie per dimostrare il rispetto degli obblighi di cui al GDPR, compreso l'art. 28 dello stesso, e di cui al presente Addendum, consentendo e contribuendo alle attività di revisione, comprese le ispezioni, realizzate dal Responsabile del Trattamento o da un altro soggetto dallo stesso incaricato.

XI. Obbligazioni del Responsabile del Trattamento nei confronti del Sub-Responsabile del Trattamento

Il Responsabile del Trattamento si impegna a fornire al Sub-Responsabile del Trattamento i Dati Personali nel caso in cui, in ragione dell'Accordo e/o dei Servizi, essi non siano raccolti e/o acquisiti direttamente dal Sub-Responsabile del Trattamento, per conto del Responsabile del Trattamento.

Il Responsabile del Trattamento vigilerà, per tutta la durata dell'Addendum, sull'osservanza degli obblighi imposti al Sub-Responsabile del Trattamento dalle Istruzioni, dall'Addendum e dalla Normativa sulla Protezione dei Dati Personali, compreso il GDPR. Il Responsabile del Trattamento si riserva la facoltà di chiedere al Sub-Responsabile del Trattamento, con le medesime modalità e con la medesima tempistica, di effettuare audit e/o ispezioni presso i Sub-Responsabili, congiuntamente al Sub-Responsabile del Trattamento, impegnandosi quest'ultimo a dare evidenza di tale facoltà nel contratto o altro atto giuridico relativo con il Sub-Responsabile.

XII. Obbligazioni del Responsabile del Trattamento nei confronti del Sub-Responsabile del Trattamento con riferimento ai rapporti con Amazon

XII a. Lo Sviluppatore si impegna al rispetto di quanto indicato da Amazon Marketplace Web Service (**Amazon MWS**) nella Data Protection Policy di Amazon Marketplace Web Service (Amazon MWS) Documentation , come visionabile al seguente link: https://docs.developer.amazonservices.com/en_US/dev_guide/DG_DataProtectionPolicy.html , così come di volta in volta modificata. In particolare, lo Sviluppatore si impegna al rispetto degli obblighi e delle direttive di cui all'art. 5.2 delle Condizioni Generali per gli Sviluppatori.

XII b. Lo Sviluppatore si impegna al rispetto dei requisiti di sicurezza aggiuntivi, con riferimento a quanto richiesto da Amazon MWS. I requisiti di sicurezza aggiuntivi devono essere soddisfatti per tutte le PII. Se un'API di Marketplace contiene PII o le PII sono combinate con non PII, l'intero archivio dati deve soddisfare i requisiti di cui all'art. 5.3 delle Condizioni Generali per gli Sviluppatori.

XII c. Come previsto dall'art. 5.4 delle Condizioni Generali per gli Sviluppatori, Lo Sviluppatore deve conservare tutti i libri e i registri appropriati ragionevolmente necessari per verificare la conformità con la AWS Acceptable Use Policy (https://aws.amazon.com/it/aup/), con la Data Protection Policy di Amazon MWS di cui al punto 5.2, e con l'Accordo per gli sviluppatori di Amazon Marketplace durante il periodo di questo contratto e per i 12 mesi successivi. Su richiesta scritta di Amazon o di Projectmoon, lo Sviluppatore deve certificare per iscritto ad Amazon e/o Projectmoon di essere conforme a queste politiche.

Su richiesta, Amazon e/o Projectmoon può, o può far sì che una società di contabilità pubblica certificata indipendente selezionata da Amazon e/o Projectmoon, controlli e ispezioni i libri, i registri, le strutture, le operazioni e la sicurezza di tutti i sistemi coinvolti nell'applicazione di uno Sviluppatore nel recupero, nell'archiviazione o elaborazione delle informazioni di Amazon e/o Projectmoon. Lo Sviluppatore deve cooperare con Amazon e/o Projectmoon o il revisore di Amazon e/o Projectmoon in relazione alla verifica, che può avvenire presso le strutture dello Sviluppatore e/o delle strutture del subappaltatore. Se l'audit rivela carenze, violazioni e/o mancato rispetto dei nostri termini, condizioni o politiche, lo Sviluppatore deve, a proprie spese e spese, e intraprendere tutte le azioni necessarie per rimediare a tali carenze entro un periodo di tempo concordato.

XII d. Come previsto dall'art. 5.5 delle Condizioni Generali per gli Sviluppatori, Lo Sviluppatore si impegna al rispetto della AWS Acceptable Use Policy dei servizi web offerti da Amazon Web Service, Inc. (**Amazon AWS**), visionabile al seguente link: https://aws.amazon.com/it/aup/.

XII e. Lo Sviluppatore si impegna a tenere indenne e manlevata Projectmoon da qualsiasi contestazione, danno, richiesta di risarcimento e/o responsabilità derivante dalla violazione da parte dello Sviluppatore degli impegni di cui agli artt. XII a., XII b., XII c., XII d., della presente DPA.

XIII. Trasferimento dei Dati Personali in un Paese terzo

Nel caso in cui il Sub-Responsabile del Trattamento intenda trasferire i Dati Personali in un Paese non appartenente alla UE, il Sub-Responsabile del Trattamento si impegna a: (i) comunicare tale intenzione preventivamente al Responsabile del Trattamento, per e-mail, indicando il Paese terzo di destinazione, il destinatario e le garanzie adeguate che, a norma del capo V del GDPR, consentono il trasferimento; (ii) effettuare il trasferimento solo ed esclusivamente in assenza di opposizione da parte del Responsabile del Trattamento, comunicata per iscritto ed entro il termine di 15 giorni lavorativi dal ricevimento di tale comunicazione ovvero una volta scaduto tale termine.

XIV. Comunicazioni

Tutte le comunicazioni previste dal presente Addendum dovranno avvenire ai contatti indicati in epigrafe.

XV. Manleva

Lo Sviluppatore si impegna a tenere indenne e manlevata Projectmoon da qualsiasi contestazione, danno, risarcimento e /o responsabilità derivante dalla violazione degli

impegni assunti nei confronti di Projectmoon e/o di terzi, tra cui gli obblighi di cui all'art. XII della presente DPA.

XVI. Legge Applicabile e foro competente

Il presente Addendum è soggetto alla legge italiana.

Qualsiasi controversia relativa all'applicazione, interpretazione o esecuzione del presente Addendum è di competenza esclusiva ed inderogabile del foro di Treviso.

XVII. Varie

Le Parti riconoscono che il presente Addendum non limita né riduce gli impegni che il Sub-Responsabile del Trattamento ha assunto nei confronti del Responsabile del Trattamento nell'Accordo, fermo restando che in caso di conflitto tra le previsioni dell'Accordo e quelle dell'Addendum in materia di trattamento di dati personali e/o di protezione dei dati personali, le previsioni dell'Addendum prevarranno.