MarketingStudio

CONTRATTO DI NOMINA A RESPONSABILE ESTERNO DEL TRATTAMENTO

TRA

La società **Cliente,** in persona del suo legale rappresentante *pro tempore* (di seguito "**Titolare**"), ai sensi dell'art. 24 del Regolamento (UE) 2016/679 (di seguito "**GDPR**")

E

MARKETING STUDIO S.R.L. con sede in Torino (TO) – Corso Re Umberto, 8 - P.I. 1217710011, (di seguito "**contraente** o "**Responsabile**"), ai sensi dell'art. 28 GDPR

Congiuntamente indicate come le "**Parti**".

PREMESSO CHE

- **il Titolare** con riferimento al trattamento dei dati personali dallo stesso trattati, svolge il ruolo di Titolare del trattamento, stabilendo autonomamente le finalità, le modalità ed i mezzi del trattamento;
- Il contraente è in possesso di adeguate competenze tecniche, organizzative e *know-how* circa gli scopi e le modalità di trattamento dei Dati Personali, delle misure di sicurezza da adottare al fine di garantire la riservatezza, la completezza e l'integrità dei Dati Personali trattati, nonché circa le norme che disciplinano la protezione dei Dati Personali;
- **Il Titolare**, intende nominare **MARKETING STUDIO S.R.L.** con quale Responsabile del trattamento che intende accettare tale nomina;
- **Il Titolare**, intende rilasciare a **MARKETING STUDIO S.R.L.** con autorizzazione generale per la nomina di ulteriori responsabili del trattamento (sub- responsabili);
- **Il contraente svolge le attività indicate nel contratto stipulato tra le parti relativo allo sviluppo e fornitura del software in cloud Framework360 compreso servizio di hosting.**

I soggetti interessati cui si riferiscono i dati sono i soggetti gestiti a cura del Titolare tramite i servizi forniti.
- Oggetto del trattamento di dati ai fini della presente nomina, in base alle attività indicate nel contratto, sono:

☒ a) dati personali comuni (es. nome, cognome, residenza, data e luogo di nascita, codice fiscale, informazioni di contatto quali numero di telefono, indirizzo email);

☒ b) dati particolari (origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona).

- Con riferimento alla summenzionata nomina, con la sottoscrizione del presente documento le Parti intendono regolare i reciproci rapporti in relazione al trattamento dei Dati Personali effettuato dal Responsabile per conto del Titolare.

Tutto ciò premesso, alla luce di quanto precede, le Parti stipulano quanto segue:

1. NOMINA DEL RESPONSABILE DEL TRATTAMENTO

Con la sottoscrizione del presente atto che forma parte integrante del Contratto, **Il Titolare** nomina **MARKETING STUDIO S.R.L.** con quale Responsabile del Trattamento ai sensi dell'art. 28 del Regolamento (UE) 2016/679, con l'incarico di effettuare le operazioni di trattamento sui Dati Personali necessarie all'adempimento degli obblighi derivanti dal presente Contratto. Il Responsabile, con la sottoscrizione del presente accordo, accetta tutti i termini sotto indicati, conferma la diretta e approfondita conoscenza degli obblighi che si assume in relazione al dettato normativo vigente e si impegna a procedere al trattamento dei Dati Personali attenendosi alle istruzioni ricevute dal Titolare attraverso la presente nomina o a quelle ulteriori che saranno conferite nel corso delle attività prestate in suo favore.

2. NATURA E DURATA DEL TRATTAMENTO

Il trattamento deve essere svolto da parte del Responsabile in esecuzione del vigente rapporto contrattuale con **il Titolare** e per le finalità ad esso relative; la presente nomina produce i suoi effetti a partire dalla data della sua sottoscrizione e rimarrà in vigore fino alla data di cessazione del Contratto.

3. DIRITTI DEL TITOLARE

Il Titolare del trattamento ha diritto di ottenere dal Responsabile tutte le informazioni relative alle misure organizzative e di sicurezza da questo adottate necessarie per dimostrare il rispetto delle istruzioni e degli obblighi affidati.
Il Titolare inoltre, ha il diritto di disporre - a propria cura e spese - verifiche a campione o specifiche attività di audit in ambito protezione dei dati personali e sicurezza, avvalendosi di personale espressamente incaricato a tale scopo, presso le sedi del Responsabile.

4. OBBLIGHI DEL RESPONSABILE

Nell'adempimento delle proprie obbligazioni, il Responsabile si obbliga a rispettare il Regolamento (UE) 2016/679, il Codice Privacy novellato dal decreto legislativo 10 agosto 2018 n. 101, ed ogni altra istruzione impartita dal Titolare, tenendo conto dei provvedimenti tempo per tempo emanati dall'Autorità di Controllo italiana, ovvero dal Gruppo di Lavoro Articolo 29 e dal Comitato Europeo per la protezione dei dati, inerenti al trattamento svolto.
Il Responsabile si impegna:

- ad effettuare il Trattamento soltanto dei Dati Personali che siano necessari e/o strumentali all'esecuzione del presente Contratto.
- sin dalla data di sottoscrizione del presente atto, a rendere disponibili ed a comunicare ai propri Subfornitori soltanto quei Dati Personali che siano strettamente necessari per l'adempimento delle obbligazioni di cui al presente Contratto, o che siano necessari per l'adempimento di obblighi di legge o imposti dalle normative europee.
- a cooperare con il Titolare in qualsiasi momento al fine di assicurare il corretto trattamento dei Dati Personali;

- a fornire al Titolare tutte le informazioni o i documenti che potranno essere ragionevolmente richiesti da quest'ultimo per l'adempimento degli obblighi di legge e per comprovare l'adozione delle misure tecniche e organizzative adeguate da parte di essa.
- a conservare i dati personali per un tempo strettamente necessario e specificatamente indicato al titolare al termine del quale i dati verranno cancellati;

In particolare, il Responsabile si impegna a rispettare gli obblighi ed istruzioni di seguito elencati.

4.1. Misure tecniche ed organizzative adeguate e violazioni dei dati personali

Il Responsabile dovrà adottare le misure tecniche ed organizzative adeguate previste dalla normativa italiana ed europea in materia di protezione dei Dati Personali, cosi come ogni altra previsione derivante dall'Autorità di Controllo, ovvero dal Gruppo di Lavoro Articolo 29 e dal Comitato Europeo per la protezione dei dati.
Il Responsabile, in considerazione della conoscenza maturata quale conseguenza dei progressi tecnici e tecnologici, della natura dei Dati Personali e delle caratteristiche delle operazioni di Trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche, mette in atto misure tecniche ed organizzative adeguate e dovrà assicurare che le misure di sicurezza progettate ed implementate siano in grado di ridurre il rischio di danni volontari o accidentali, perdita di dati, accessi non autorizzati ai dati, trattamenti non autorizzati o trattamenti non conformi agli scopi di cui al presente Contratto.
In particolare, il Responsabile si obbliga a:
4.1.1 adottare tutte le misure di cui all'art. 32 del Regolamento (UE) 2016/679 in modo da garantire la riservatezza, l'integrità e la disponibilità dei dati personali trattati, tenendo conto dei provvedimenti tempo per tempo emanati dall'Autorità di Controllo inerenti ai Trattamenti svolti dal Responsabile, ovvero dal Gruppo di Lavoro Articolo 29 e dall'istituendo un canale Comitato Europeo per la protezione dei dati;
4.1.2 non trasferire i Dati Personali del Titolare al di fuori dell'usuale luogo di lavoro, a meno che tale trasferimento non sia autorizzato dalle competenti pubbliche autorità, anche regolamentari e di vigilanza;
4.1.3 istituire e mantenere il registro delle attività di trattamento ai sensi dell'art. 30 del GDPR per l'attività espletata per conto del Titolare;
4.1.4 comunicare al Titolare il nominativo ed i recapiti di contatto del proprio eventuale responsabile della protezione dei dati designato ai sensi degli artt. 37 e ss. del GDPR;
4.1.5 assistere il Titolare relativamente ai Dati Personali oggetto di trattamento, nel garantire – ove applicabili - il rispetto degli obblighi relativi:
- alla sicurezza del trattamento;
- alla notifica di una violazione dei Dati Personali all'Autorità di controllo ai sensi dell'art. 33 del GDPR;
- alla comunicazione di una violazione dei Dati Personali all'interessato ai sensi dell'art. 34 del GDPR;
- alla valutazione d'impatto sulla protezione dei Dati Personali ai sensi dell'art. 35 del GDPR;
- alla consultazione preventiva ai sensi dell'art. 36 del GDPR.

4.2. Violazioni dei dati personali

In eventuali casi di violazione dei dati personali consistenti nella violazione di sicurezza che comportino accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati e tali da mettere a rischio i diritti e le libertà degli individui i cui dati personali sono trattati dal Responsabile per conto del Titolare (c.d. data breach), il Responsabile deve:

• informare il Titolare tempestivamente ed in ogni caso al massimo entro e non oltre 24 ore dalla scoperta dell'evento, e con ogni altro mezzo utile di essere venuto a conoscenza di una violazione e fornire tutti i dettagli completi della violazione subita: in particolare, fornendo una descrizione della natura della violazione dei dati personali, le categorie e il numero approssimativo di interessati coinvolti, nonché le categorie e il numero approssimativo di registrazioni dei dati in questione, l'impatto della violazione dei dati personali sul Titolare, sugli interessati coinvolti e le misure adottate per mitigare i rischi;
• fornire assistenza al Titolare per far fronte alla violazione ed alle sue conseguenze soprattutto in capo agli interessati coinvolti.

Il Responsabile si attiverà per mitigare gli effetti delle violazioni, proponendo tempestive azioni correttive al Titolare, ed attuando tempestivamente tutte le azioni correttive approvate e/o richieste dal Titolare.
Tali misure sono richieste al fine di garantire un livello di sicurezza adeguato al rischio correlato al trattamento eseguito.

4.3 Documentazione Privacy

Il Responsabile dovrà adottare senza indugio la documentazione in materia di protezione dei Dati Personali prevista dalla normativa italiana ed europea e le relative procedure concernenti le adeguate misure tecniche e organizzative.

4.4. Istanze degli Interessati

Tenendo conto della natura del trattamento, il Responsabile si obbliga ad assistere e supportare il Titolare del Trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del Titolare, di dare riscontro alle richieste per l'esercizio dei diritti dell'interessato (negli ambiti e nel contesto del ruolo ricoperto e in cui opera il Responsabile) nel rispetto dei termini previsti dall'art. 12 del Regolamento (UE) 2016/679.
In particolare, qualora il Responsabile riceva richieste provenienti dagli Interessati, finalizzate all'esercizio dei propri diritti, esso dovrà:

- provvedere all'aggiornamento dei dati dell'Interessato (quali ad esempio: rettifica, cancellazione, ecc.)
- nel caso di segnalazioni da parte dell'interessato, o richieste che esulino dalla normale attività del Responsabile, quest'ultimo dovrà:
  - coordinarsi, ove necessario e per quanto di propria competenza, con le funzioni aziendali designate dal Titolare per gestire le relazioni con gli interessati;
  - assistere e supportare il Titolare del trattamento con misure tecniche e organizzative adeguate, al fine di soddisfare l'obbligo del Titolare di dare seguito alle richieste per l'esercizio dei diritti degli Interessati (negli ambiti e nel contesto del ruolo ricoperto e in cui opera il Responsabile).

4.5. Incaricati al trattamento dei dati personali

Il Responsabile nell'ambito della propria organizzazione aziendale:

- istruire gli incaricati al trattamento sulle modalità di elaborazione dei dati, fornendo agli stessi precise istruzioni operative, anche sotto il profilo delle misure adeguate di sicurezza al fine di prevenire i rischi di distruzione, perdita, o conoscibilità dei dati da parte di soggetti terzi non autorizzati;
- Monitorare le attività di trattamento degli incaricati al trattamento e ad effettuare controlli periodici al fine di assicurare, l'applicazione delle istruzioni di sicurezza impartite e l'ottemperanza agli obblighi di legge;
- consentire l'accesso degli incaricati/ persone autorizzate al trattamento ai soli dati la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati;
- verificare periodicamente la sussistenza delle condizioni per la conservazione delle autorizzazioni all'accesso ai dati da parte degli incaricati;
- garantire che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza dei dati;
- garantire che i propri dipendenti e collaboratori siano affidabili, ed abbiano piena conoscenza della normativa primaria e secondaria in materia di protezione dei dati personali;

5. SUB-RESPONSABILI E TERZE PARTI

Il Responsabile potrebbe dover comunicare o rendere disponibili i Dati Personali del Titolare, ad uno o più Subfornitori, al fine di affidare ai Subfornitori specifiche attività di Trattamento in base a quanto previsto dal presente Contratto.
Al fine di dare attuazione alle previsioni del Regolamento (UE) 2016/679, del Codice Privacy e del presente Contratto, il Responsabile si obbliga a designare i Subfornitori quali Sub-Responsabili ed a far sottoscrivere agli stessi le medesime condizioni applicate nel presente atto di designazione a Responsabile, mediante sottoscrizione di appositi atti giuridici o contratti con i Subfornitori.
I Sub-Responsabili potranno trattare i Dati Personali nella misura in cui tale trattamento sia strettamente necessario per l'esecuzione del contratto che il Responsabile ha stipulato con il titolare, ed in ogni caso nel rispetto del presente Contratto, restando inteso tra le Parti che i Sub-Responsabili saranno inoltre obbligati al rispetto delle limitazioni cui il Responsabile stesso è tenuto.
Nello specifico, il Responsabile si obbliga:

- ad illustrare al Titolare del trattamento, su espressa richiesta, i requisiti, in capo al Sub Responsabile, ritenuti adeguati sotto il profilo delle competenze tecniche, organizzative e *know-how* circa gli scopi e le modalità di trattamento dei Dati Personali nonché delle misure di sicurezza già in possesso del sub Responsabile;
- a comunicare al il Titolare del trattamento, su espressa richiesta, le specifiche attività che intende delegare al Sub responsabile;
- a stipulare con i Sub-Responsabili un accordo scritto (o specifico atto di nomina) che imponga a quest'ultimi il rispetto degli stessi obblighi in materia di protezione dei Dati Personali a cui il Responsabile è vincolato nei confronti del Titolare, (in base alla presente nomina), ivi incluse l'adozione delle misure di sicurezza ai sensi dell'art 32 GDPR, prevedendo, in particolare, garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo che il trattamento soddisfi i requisiti della normativa italiana ed europea in materia di trattamento dei dati personali;

Qualora gli eventuali Collaboratori Esterni e sub-Responsabili del trattamento omettano in tutto o in parte di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile dichiara espressamente e garantisce di tenere indenne il Titolare del trattamento da ogni responsabilità derivante da tali condotte omissive e/o negligenti.
Il Responsabile si impegna a non comunicare, trasferire o condividere, i Dati Personali del Titolare, a Terze Parti, salvo qualora legislativamente richiesto ed informandone preventivamente il Titolare.

6. CONTROLLI E ATTIVITÀ DI AUDIT

Il Responsabile si impegna a consentire al Titolare la verifica del rispetto del presente atto di designazione.
Qualora venga rilevato che un'istruzione impartita dal Titolare vìoli le disposizioni relative alla normativa rilevante in tema di protezione dei dati personali, il Responsabile si obbliga ad informare immediatamente lo stesso Titolare di tale circostanza.
Il Responsabile del trattamento, inoltre, riconosce al Titolare il diritto di effettuare controlli (audit) relativamente alle operazioni aventi ad oggetto il Trattamento dei Dati Personali del Titolare con un preavviso di almeno tre giorni lavorativi.
A tal fine, il Titolare potrà periodicamente sottoporre al Responsabile un questionario sul livello di sicurezza e conformità alla normativa in materia di protezione dei dati personali (che dovrà essere debitamente compilato e restituito) e ha il diritto di disporre - a propria cura e spese - verifiche a campione o specifiche attività di audit o di rendicontazione in ambito protezione dei dati personali e sicurezza, avvalendosi di personale espressamente incaricato a tale scopo, presso le sedi del Responsabile.
Il Responsabile nominato, per i motivi su esposti, è obbligato a mettere a disposizione in qualunque momento e dietro richiesta del Titolare del trattamento, tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui alla presente nomina ed a contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato.
Tali controlli potranno essere effettuati dal Titolare periodicamente ed in base a metodologie concordate tra le Parti.

7. CESSAZIONE DEL TRATTAMENTO

A seguito della cessazione del Trattamento affidato al Responsabile, nonché a seguito della cessazione del rapporto contrattuale sottostante, qualunque ne sia la causa, il Responsabile sarà tenuto a discrezione del Titolare a:

- Restituire al Titolare i Dati Personali trattati e a rendere una dichiarazione scritta che presso di sé non esiste alcuna copia dei dati, salvi gli eventuali obblighi di legge;
- Cancellare tutti i dati dai propri archivi fisici ed informatici, salvo obblighi di conservazione previsti dalla legge

8. ACCORDO RELATIVO AL TRASFERIMENTO DEI DATI ALL'ESTERO

Il Responsabile si impegna a circoscrivere gli ambiti di circolazione e trattamento dei Dati Personali (es. memorizzazione, archiviazione e conservazione dei dati sui propri server o in cloud) ai Paesi facenti parte dell'Unione Europea, con espresso divieto di trasferirli in paesi extra UE che non garantiscano (o in assenza di) un livello adeguato di tutela, ovvero, in assenza di strumenti di tutela previsti dal Regolamento (UE)

2016/679 (Paese terzo giudicato adeguato dalla Commissione europea, BCR di gruppo, clausole contrattuali modello, consenso degli interessati, etc.)
Il Responsabile, pertanto, non dovrà trasferire o effettuare il trattamento dei Dati Personali del Titolare, al di fuori dell'Unione Europea, per nessuna ragione, in assenza di autorizzazione scritta del Titolare. Qualora il Titolare rilasci l'autorizzazione di cui al presente paragrafo e venga pertanto effettuato un trasferimento dei Dati Personali del Titolare, al di fuori dell'Unione Europea, tale trasferimento dovrà rispettare le previsioni di cui al Regolamento (UE) 2016/679 sopra indicate.
Resta inteso tra le Parti che il Fornitore dovrà garantire che i metodi di trasferimento impiegati, ivi inclusa la conformità alle clausole contrattuali standard approvate dalla Commissione Europea e sulla base dei presupposti indicati nella medesima decisione consentano il mantenimento di costanti e documentabili standard di validità per tutta la durata del presente Contratto.

9. RESPONSABILITÀ PER VIOLAZIONE DELLE DISPOSIZIONI

Qualora, come previsto ai sensi dell'art. 82 par. 4 del GDPR, il Titolare ed il Responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3 dell'art. 82 GDPR, responsabili dell'eventuale danno causato dal trattamento, entrambi sono responsabili in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.
Il Responsabile si impegna a comunicare prontamente al Titolare eventuali situazioni sopravvenute che, per il mutare delle conoscenze acquisite in base al progresso tecnico o per qualsiasi altra ragione, possano incidere sulla propria idoneità allo svolgimento dell'incarico.
Il Titolare ha il diritto di reclamare dal Responsabile la parte dell'eventuale risarcimento di cui dovesse essere chiamato a rispondere nei confronti di terzi per le violazioni commesse da Responsabile ai sensi dell'art. 82, paragrafo 5, del GDPR.
Nel caso di mancata o ritarda comunicazione di data breach al Titolare, da parte del Responsabile o del Sub-Responsabile da quest'ultimo individuato, il Titolare può richiedere il risarcimento dei danni equivalenti alla sanzione comminata dall'Autorità, quelli derivanti dal risarcimento danni degli interessati e dal danno reputazionale, a seguito dell'accertamento, da parte dell'Autorità competente, dell'effettivo danno patito dal Titolare medesimo.
Fatti salvi gli articoli 82, 83, 84, del Regolamento (UE) 2016/679, in caso di violazione delle disposizioni contenute nella presente nomina relative alle finalità e modalità di trattamento dei dati, di azione contraria alle istruzioni ivi contenute o in caso di mancato adempimento agli obblighi specificatamente diretti al Responsabile dal Regolamento (UE) 2016/679, il Responsabile sarà considerato quale Titolare del trattamento e ne risponderà direttamente dal punto di vista sanzionatorio.

10. CORRISPETTIVO

Non è dovuto alcun corrispettivo in relazione all'attività oggetto del presente Contratto.

11. RECESSO

Ogni violazione del presente Contratto dovrà intendersi quale grave violazione che consente al Titolare di risolvere il contratto con effetto immediato. Anche in mancanza di un'eventuale violazione del presente Contratto, il Titolare potrà recedere con effetto immediato a propria discrezione qualora ritenga che il Responsabile non fornisca garanzie adeguate di cui al presente Contratto o al GDPR.

12. SOPRAVVIVENZA DELLE CLAUSOLE

Alla cessazione, per qualsiasi causa, del Contratto continueranno ad avere efficacia quelle clausole che per loro natura sopravvivono all'estinzione del rapporto giuridico.

13. COMUNICAZIONI

Ogni comunicazione tra il Titolare ed il Responsabile di cui al presente Contratto dovrà avvenire tramite email o posta elettronica certificata ai seguenti indirizzi: info@marketingstudio.it

14. ACCETTAZIONE DELLA NOMINA

Con la sottoscrizione del presente atto, ai sensi dell'art. 28 del Regolamento (UE) 2016/679, il Responsabile accetta la propria nomina, in relazione ai dati personali la cui conoscenza risulta essere indispensabile per l'adempimento delle obbligazioni di cui al Contratto. Il Responsabile è a conoscenza degli obblighi previsti dal Regolamento (UE) 2016/679 e dal Codice privacy e dovrà attenersi, per lo svolgimento dei compiti assegnatigli, alle previsioni ed ai compiti contenuti nel presente atto di nomina.
La presente nomina avrà durata fino alla cessazione, per qualsivoglia motivo, del Contratto.

Torino (TO), lì 14/02/2025

RELAZIONE SUI SERVIZI AWS UTILIZZATI E MISURE TECNICHE DI SICUREZZA ADOTTATE

Questa relazione descrive i servizi AWS attualmente utilizzati e le misure tecniche di sicurezza adottate per garantire la protezione dei dati e delle infrastrutture digitali.

Infrastruttura EC2

Descrizione

Le istanze EC2 rappresentano i server virtuali utilizzati per eseguire il front end e altre operazioni pianificate tramite cron.

Misure di Sicurezza

- Utilizzo di Amazon Machine Image (AMI) sicure e aggiornate.
- Controllo degli accessi basato su Identity and Access Management (IAM).
- Configurazione di chiavi SSH per l'accesso sicuro alle istanze.
- Tutte le istanze EC2 eseguono l'ultima versione disponibile di PHP per garantire un ambiente stabile e sicuro.
- Tutti gli accessi SSH richiedono lo sblocco delle porte prima di potersi connettere. Viene sbloccato un solo IP alla volta.
- Le operazioni pianificate tramite cron utilizzano regole firewall separate rispetto alle istanze front end per garantire una segmentazione della sicurezza.

Load Balancer

Descrizione

Il load balancer distribuisce il traffico in ingresso tra le istanze del gruppo auto scaling per garantire alta disponibilità e resilienza.

Misure di Sicurezza

- Implementazione di SSL/TLS per cifrare le connessioni
- Abilitazione di WAF (Web Application Firewall) per proteggere contro attacchi comuni
- Restrizione degli accessi tramite gruppi di sicurezza.

Gruppo Autoscaling

Descrizione

Il gruppo autoscaling gestisce automaticamente il numero di istanze EC2 in base alla domanda di traffico.

Misure di Sicurezza

- Configurazione di regole di scaling basate su metriche di utilizzo
- Utilizzo di IAM roles per la gestione sicura delle risorse
- Monitoraggio continuo tramite CloudWatch

Gruppi di sicurezza

Descrizione

I gruppi di sicurezza definiscono le regole di traffico in entrata e in uscita per le risorse AWS.

Misure di Sicurezza

- Limitazione degli indirizzi IP che possono accedere alle risorse
- Definizione di porte specifiche per i servizi richiesti
- Aggiornamenti regolari delle regole di accesso

Amazon EFS (Filesystem)

Descrizione

File system condiviso utilizzato dalle istanze EC2 per archiviare dati.

Misure di Sicurezza

- Cifratura dei dati a riposto e in transito
- Controllo degli accessi tramite IAM

RDS (Database)

Descrizione

Database relazionale gestito da AWS per la gestione dei dati applicativi.

Misure di Sicurezza

- Abilitazione della cifratura dei dati a riposo
- Configurazione di backup automatici
- Accesso limitato tramite gruppi di sicurezza
- Tutte le query MySQL vengono sottoposte a escaping per evitare SQL injection
- I database RDS possono essere raggiunti esclusivamente dai servizi interni AWS tramite firewall, garantendo un accesso sicuro e controllato

ElastCache

Descrizione

Servizio di caching gestito per migliorare le prestazioni delle applicazioni.

Misure di Sicurezza

- Configurazioni di gruppi di sicurezza per limitare l'accesso
- Abilitazione della cifratura dei dati in transito

S3

Descrizione

Servizio di archiviazione di oggetti utilizzato per archiviare file statici.

Misure di Sicurezza

- Abilitazione di bucket policies per limitare gli accessi
- Versionamento degli oggetti
- Logging degli accessi
- Tutti i file caricati dai clienti vengono inviati esclusivamente su S3, evitando la possibilità di caricare file direttamente sul server eseguibile

CloudFront

Descrizione

Content Delivery Network (CDN) utilizzata per distribuire contenuti con bassa latenza.

Misure di Sicurezza

- Abilitazione di HTTPS per tutte le connessioni
- Configurazione di regole WAF

Lambda (Generazione. webp)

Descrizione

Funzioni Lambda eseguite ai bordi della rete per ottimizzare le immagini servite tramite CloudFront.

Misure di Sicurezza

- Controllo degli accessi tramite IAM roles.
- Limitazione delle risorse utilizzate dalle funzioni Lambda.

Amazon Simple Notification Service (SNS)

Descrizione

Servizio utilizzato per ricevere notifiche in tempo reale su eventi anomali nell'infrastruttura AWS.

Misure di Sicurezza

- Notifiche configurate per segnalare eventi come riavvii di macchine, utilizzo elevato di banda e altri eventi critici.

Backup

Descrizione

Implementazione di un piano di backup completo per garantire la disponibilità dei dati.

Misure di Sicurezza

- Backup giornalieri automatizzati di S3, EFS e RDS tramite AWS Backup
- I backup vengono conservati per un periodo di 30 giorni

Accesso ai Servizi AWS

Descrizione

L'accesso a qualsiasi servizio AWS è controllato tramite il portale di gestione AWS.

Misure di Sicurezza

- L'accesso ai servizi AWS richiede l'autenticazione a due fattore (MFA) per garantire un ulteriore livello di sicurezza.

Torino (TO), lì _____/_____/_____

Sottoscrizione
MARKETING STUDIO S.R.L.