ACCORDO PER IL TRATTAMENTO DI DATI PERSONALI – DATA PROCESSING AGREEMENT

(ai sensi dell'art. 28 del Regolamento UE 2016/679)

1. PREMESSE

1.1 Il presente DPA (Data Processing Agreement) disciplina il trattamento di Dati personali, svolto da **Adamo Lab di Riccardo Barbotti** (il "Responsabile del Trattamento" o "Responsabile" o "Fornitore"), necessario all'erogazione dei servizi offerti (i "Servizi") al Cliente (il "Titolare del Trattamento" o "Titolare" o "Cliente") ed è allegato ai "**Termini di Servizio**" della piattaforma Adamo Gestionale (https://www.adamogestionale.it).

1.2 Qualora il Cliente svolga operazioni di trattamento per conto di altro Titolare, il Cliente potrà agire come Responsabile del Trattamento. In tal caso, il Cliente garantisce che le istruzioni impartite e le attività intraprese in relazione al trattamento dei Dati Personali, inclusa la nomina, da parte del Cliente, del Fornitore quale ulteriore Responsabile del Trattamento derivante dalla stipulazione del presente DPA, sono state autorizzate dal relativo Titolare del trattamento e si impegna ad esibire al Fornitore, dietro sua semplice richiesta scritta, la documentazione attestante quanto sopra.

2. RIFERIMENTI NORMATIVI

2.1 Il presente DPA garantisce che il trattamento dei Dati svolto dal Fornitore sia conforme al Regolamento UE 679/2016 ("GDPR") e più in generale alla normativa italiana ed europea in materia di privacy e protezione dei dati personali (la "Legge Applicabile").

3. TRATTAMENTO DI DATI PERSONALI

3.1 Finalità del trattamento: la finalità del trattamento dei Dati è la fornitura dei Servizi da parte del Fornitore, come specificato nei Termini di Servizio.

3.2 Per fornire i Servizi al Cliente, il Responsabile del Trattamento tratterà, per conto del Titolare, determinate categorie di Dati personali raccolti dal Titolare e inseriti da quest'ultimo nei database della piattaforma Adamo Gestionale.

3.3 Per "Dati personali" si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato») come definito dall'art. 4 del GDPR. Le categorie di Dati personali trattati dal Responsabile del Trattamento per conto del Titolare sono elencate nel Sub-Allegato A. Il Responsabile svolge esclusivamente le attività di trattamento necessarie e rilevanti ad assicurare l'esecuzione dei Servizi al Titolare.

3.4 Il Responsabile del Trattamento adotta un registro delle attività di trattamento in conformità con l'art. 30, par. 2 del GDPR.

4. ISTRUZIONI

4.1 Il Responsabile del Trattamento può trattare i dati personali esclusivamente in conformità con le istruzioni documentate del Titolare del trattamento (le "Istruzioni"), a meno che la Legge Applicabile non disponga diversamente. Con il presente DPA, il Titolare fornisce l'istruzione che il Responsabile del Trattamento possa trattare i Dati personali solamente allo scopo di fornire i Servizi attenendosi alle disposizioni contenute nei Termini di Servizio. Subordinatamente ai termini del presente DPA e con il reciproco accordo delle parti, il Titolare del Trattamento può fornire al Responsabile ulteriori istruzioni scritte coerenti con i termini del presente Accordo.

4.2 Il Titolare del Trattamento garantisce di trattare i Dati personali in conformità alla normativa vigente in materia di privacy e protezione dei dati personali. Le istruzioni fornite dal Titolare devono essere conformi alla Legge Applicabile. Il Titolare sarà l'unico responsabile dell'esattezza, la qualità e la limitazione della conservazione dei Dati Personali raccolti e trattati. Il Titolare dovrà inoltre garantire che i Dati siano raccolti e trattati in maniera lecita, corretta e trasparente.

4.3 Il Responsabile del Trattamento informa il Titolare nel caso in cui ritenga che le Istruzioni violino la Legge Applicabile e non eseguirà tali Istruzioni finché non saranno riconosciute come legittime.

5. OBBLIGHI DEL RESPONSABILE DEL TRATTAMENTO

5.1 Riservatezza

5.1.1 Il Responsabile del Trattamento tratta tutti i Dati personali come informazioni strettamente riservate. I Dati Personali non possono essere copiati, trasferiti o trattati in conflitto con le Istruzioni, a meno che non venga autorizzato a seguito di ulteriori accordi con il Titolare del Trattamento.

5.1.2 I dipendenti del Responsabile sono soggetti a un obbligo di riservatezza e hanno firmato un'apposita nomina che li autorizza a trattare i Dati in maniera conforme alla Legge Applicabile e alle disposizioni contenute nel presente DPA.

5.1.3 I Dati personali sono trattati solamente dal personale necessario ai fini dell'erogazione dei Servizi.

5.1.4. Il Responsabile del Trattamento assicura, inoltre, che i dipendenti che svolgono operazioni di trattamento sui Dati personali trattano solo le categorie di Dati personali previste dal presente DPA e in conformità con le Istruzioni.

5.2 Sicurezza

5.2.1 Il Responsabile del Trattamento deve attuare le misure tecniche e organizzative appropriate come stabilito nel presente DPA e ai sensi dell'articolo 32 del GDPR. Il Responsabile del Trattamento può aggiornare o modificare le misure di sicurezza di volta in volta a condizione che tali aggiornamenti e modifiche non comportino il peggioramento dei livelli di sicurezza complessiva. Le misure di sicurezza sono elencate nel Sub-Allegato B.

5.3 Valutazioni d'impatto sulla protezione dei dati e consultazione preventiva

5.3.1 Se l'assistenza del Responsabile del Trattamento è necessaria e pertinente, il Responsabile assisterà il Titolare nel predisporre le valutazioni d'impatto sulla protezione dei dati in conformità all'art. 35 del GDPR, insieme a qualsiasi consultazione preventiva ai sensi dell'art. 36 del GDPR.

5.4 Diritti degli interessati

5.4.1 Se il Titolare riceve una richiesta da un interessato per l'esercizio dei propri diritti ai sensi della Legge Applicabile e la risposta corretta e legittima a tale richiesta richiede l'assistenza del Responsabile del Trattamento, il Responsabile assisterà il Titolare fornendo, entro un tempo ragionevole, le informazioni necessarie e la documentazione richiesta dal Titolare. Il Responsabile dovrà assistere il Titolare nel gestire tali richieste in conformità con la Legge Applicabile.

5.4.2 Se il Responsabile del Trattamento riceve una richiesta da un interessato per l'esercizio dei propri diritti ai sensi della Legge Applicabile e tale richiesta è connessa ai Dati Personali raccolti dal Titolare, il Responsabile dei dati deve immediatamente inoltrare la richiesta al Titolare e deve astenersi dal rispondere direttamente all'interessato.

5.5 Violazione di Dati personali

5.5.1 In caso di violazione di Dati personali (“Data Breach”) che possa comportare la distruzione, la perdita, l'alterazione, la divulgazione o l'accesso non autorizzato o accidentale ai Dati personali trattati per conto del Titolare del Trattamento, il Responsabile dovrà dare comunicazione al Titolare entro quarantotto (48) ore dal momento in cui il Data Breach viene rilevato dal Responsabile.

5.5.2 Il Responsabile del Trattamento dovrà compiere ogni ragionevole sforzo per identificare la causa di tale violazione e adottare le misure che riterrà necessarie per determinarne la causa e per impedire che tale violazione si ripresenti.

5.6 Documentazione di conformità e diritti di audit

5.6.1 Su richiesta del Titolare, il Responsabile del Trattamento dovrà mettere a disposizione del Titolare tutte le informazioni rilevanti necessarie a dimostrare la conformità al presente DPA.

5.6.2 Il Responsabile riconosce il diritto del Titolare, con le modalità e nei limiti di seguito indicati, ad effettuare audit per verificare la conformità del Responsabile agli obblighi previsti dal presente DPA e dalla normativa. Il Titolare potrà avvalersi, per tali attività, di proprio personale specializzato o di revisori esterni, purché tali soggetti siano previamente vincolati da idonei impegni alla riservatezza.

5.6.3 Il Responsabile può opporsi per iscritto alla nomina da parte del Titolare di eventuali revisori esterni che siano, ad insindacabile giudizio del Responsabile, non adeguatamente qualificati o indipendenti, siano concorrenti del Responsabile o che siano evidentemente inadeguati. In tali circostanze, il Titolare sarà tenuto a nominare altri revisori o a condurre le verifiche in proprio.

5.6.4 Il Responsabile risponderà alle richieste di documentazione aggiuntiva o di programmazione di audit inoltrate dal Titolare entro trenta (30) giorni dalla data di ricezione della richiesta.

5.7 Trasferimento dei Dati

5.7.1 In via ordinaria, il Responsabile del Trattamento non trasferirà i Dati in Paesi non appartenenti Spazio Economico Europeo (SEE). Sarà necessario, per svolgere alcune tipologie di trattamenti (a titolo esemplificativo: backup, hosting, ecc.), il trasferimento dei Dati al di fuori dello Spazio economico europeo (SEE). In tal, caso i Dati saranno trasferiti solamente a Sub-Responsabili che abbiano adottato le adeguate garanzie previste dagli artt. 44-50 del GDPR (a titolo esemplificativo: Privacy Shield Framework, Decisioni di adeguatezza della Commissione Europea, Clausole Contrattuali Standard).

6. Autorizzazione Generale alla nomina di Sub-responsabili

6.1 Al Responsabile del Trattamento viene conferita l'autorizzazione generale a nominare terze parti ("Sub-responsabili") per il trattamento dei Dati personali senza che siano necessarie ulteriori autorizzazioni scritte e specifiche dal Titolare del Trattamento.

6.2 Il Responsabile avvisa il Titolare prima che vengano stipulati accordi con un nuovo potenziale Sub-responsabile e prima che il Sub-responsabile tratti i Dati personali raccolti dal Titolare. Se il Titolare del Trattamento desidera opporsi alla nomina di un nuovo Sub-responsabile, il Titolare deve notificare tale opposizione al Responsabile per iscritto entro dieci (10) giorni lavorativi dal ricevimento della notifica da parte del Responsabile del Trattamento. L'assenza di eventuali obiezioni da parte del Titolare del Trattamento è da intendersi come consenso per la nomina di un nuovo Sub-responsabile.

6.3 Nel caso in cui il Titolare del Trattamento si opponga a un nuovo Sub-responsabile e il Responsabile non possa accogliere l'obiezione del Titolare, il Titolare del Trattamento può interrompere i Servizi fornendo comunicazione scritta al Responsabile.

6.4 Il Responsabile del Trattamento deve firmare un apposito DPA con ogni nuovo Sub-responsabile. Tale accordo deve prevedere come minimo gli stessi obblighi di protezione dei dati applicabili al Responsabile del Trattamento, compresi gli obblighi previsti dal presente DPA. Il Responsabile del Trattamento monitorerà e verificherà periodicamente la conformità dei suoi Sub-responsabili alla Legge Applicabile. La documentazione di tale monitoraggio deve essere fornita al Titolare del Trattamento se richiesto per iscritto.

6.5 Il Responsabile del Trattamento, al momento dell'introduzione del presente DPA, impiega i Sub-responsabili elencati nel Sub-Allegato C. Se il Responsabile sigla un contratto con un nuovo Sub-responsabile, tale nuovo Sub-responsabile deve essere aggiunto alla lista dei Sub-Responsabili del Sub-Allegato C.

7. LIMITAZIONE DI RESPONSABILITÀ

7.1 La responsabilità nei confronti del Cliente del Responsabile del Trattamento per eventuali perdite causate da o in qualche modo connesse alle disposizioni contenute in questo DPA, è soggetta alla clausola "**Responsabilità di Adamo**" stabilita nei Termini di Servizio.

8. DURATA

8.1 Il presente **DPA** rimarrà in vigore fino alla risoluzione del contratto di servizio principale, regolato dai "Termini di Servizio".

9. DATA PROTECTION OFFICER (DPO)

9.1 Il Responsabile del Trattamento nominerà un **Data Protection Officer (DPO)** laddove tale nomina sia richiesta dal GDPR.

10. CANCELLAZIONE DEI DATI

10.1 Dopo la scadenza o la risoluzione del Contratto, il Responsabile del Trattamento cancellerà o restituirà al Titolare tutti i Dati Personali in suo possesso come previsto nel Contratto, eccetto nel caso in cui sia richiesto dalla Legge Applicabile al Responsabile del Trattamento di conservare alcuni o tutti i Dati personali (in quel caso il Responsabile archivierà i dati e attuerà misure ragionevoli per impedire che i Dati personali vengano ulteriormente trattati). I termini di questo DPA continueranno ad applicarsi a tali Dati personali.

11. DATI DI CONTATTO

11.1 I dati di contatto del Responsabile del Trattamento sono i seguenti:

Adamo Lab di Riccardo Barbotti

Corso Castelfidardo 30/A 10129 Torino, TO

Email: info@adamogestionale.it

Skype: adamo.lab

Sub-Allegato A

Dati personali

1. Dati personali

1.1 Il Responsabile del Trattamento tratta i seguenti tipi di Dati personali necessari all'erogazione dei Servizi:

Nome, Cognome, Sesso, Data di nascita, Stato di nascita, Codice Fiscale e P.IVA

Indirizzo postale

Immagine

Indirizzo e-mail, Sito web, PEC, numero di telefono, numero di fax

Dati bancari, metodi di pagamento, fatturato

Altre eventuali tipologie di Dati personali inserite nello spazio cloud di Adamo dal Titolare del trattamento

2.1 Il Responsabile del Trattamento tratta per conto del Titolare i Dati personali relativi alle seguenti categorie di soggetti interessati:

Clienti del Titolare del trattamento

Prospect del Titolare del trattamento

Fornitori del Titolare del trattamento

Referenti presso i clienti e i fornitori del Titolare del trattamento

Altre eventuali tipologie di categorie di soggetti interessati i cui Dati personali sono inseriti nello spazio cloud di Adamo dal Titolare del trattamento

Sub-Allegato B

Misure tecnico-organizzative

1. Server

Adamo è un'applicazione sviluppata in PHP 5.6 tramite framework CakePHP 2.7.

Attualmente i codici sorgenti di Adamo sono ospitati su un server virtualizzato presso il fornitore terzo DigitalOcean (https://www.digitalocean.com/security/)
La macchina è fisicamente situata ad Amsterdam, Olanda.
La macchina possiede uno stack LAMP: Linux Ubuntu 14.04, Webserver Apache2, MySQL e PHP5.6.
Il sistema implementa i più comuni firewall, e consente l'accesso alle porte 80 (HTTP), 443 (HTTPS) e la porta utilizzata per l'accesso SSH.
L'accesso al server può avvenire unicamente da parte del personale autorizzato via SSH (Secure Shell).
L'accesso via SSH è consentito solamente ai dispositivi autorizzati tramite algoritmo RSA a crittografia asimmetrica.
Attualmente un solo dispositivo è autorizzato all'accesso.
I software terzi installati sul server vengono aggiornati manualmente dal personale con una frequenza bimestrale.

2. Applicazione
L'applicazione è costruita seguendo gli accorgimenti di sicurezza allo stato dell'arte.
Questi includono, tra gli altri: protezione CSRF, accesso unicamente via HTTPS, prevenzione SQL Injection.

3. Database
Le informazioni degli utenti vengono memorizzati in un database MySQL.
Tutte le password degli utenti vengono oscurate tramite algoritmo di hashing bcrypt e non è possibile risalire alla password originaria.
Il database è installato sulla stessa macchina dell'applicazione, e la connessione avviene in locale.

L'accesso al database e ai file di sistema da parte del personale avviene solo via SSH.
Vengono memorizzate nel database tutte le informazioni che l'utente inserisce con propria volontà all'interno dell'applicazione. Queste vengono memorizzate unicamente per permettere all'utente l'utilizzo del servizio.
Per motivi diagnostici e di sicurezza viene memorizzato sul database un log delle operazioni compiute dall'utente che ha fatto login, quali: pagine visitate all'interno di Adamo, accessi, email inviate tramite la piattaforma. Queste informazioni includono IP e browser dell'utente che ha fatto accesso.

4. Files
L'utente ha la possibilità di caricare all'interno della piattaforma diversi files come loghi e allegati.
Ogni file viene caricato sul server e ospitato per 10 minuti. Al termine di questi, il file viene inviato tramite uno script automatico su una apposita bucket presso Amazon AWS S3, fornitore esterno.
Le macchine di Amazon AWS sono situate in Irlanda (https://aws.amazon.com/it/compliance/gdpr-center/).
L'accesso ai servizi di Amazon AWS avviene via API fornite da Amazon.
Gli operatori possono fare login presso i servizi AWS tramite accesso via email e password, con ulteriore autenticazione a due fattori.

5. Backup
Uno script automatico genera quotidianamente un backup incrementale del database in formato *.sql. Al termine del backup, questo viene compresso e memorizzato su Amazon AWS

S3 su un apposito bucket di proprietà di Adamo.
Con cadenza settimanale viene effettuato automaticamente un backup completo del database, compresso, e memorizzato su Amazon AWS S3.
Con cadenza settimanale viene effettuato un backup completo della macchina Server. Il backup viene gestito dal fornitore DigitalOcean.

6. Raccolta di informazioni tramite servizi esterni
Per motivi diagnostici viene raccolto un log degli errori dell'applicazione sotto forma di file, contenente i messaggi di errore restituiti dall'applicazione, oltre a indirizzo IP e Browser dell'utente. Qualora si tratti di errori frontend (quindi sul browser dell'utente), il log viene raccolto tramite il servizio esterno Bugsnag.
Ci si avvale di diverse applicazioni terze per fornire servizi di assistenza e monitoraggio. L'elenco dei servizi esterni è presente all'interno della privacy policy (www.adamogestionale.it/privacy)

7. Informazioni off line
Nessuna informazione dell'utente viene memorizzata su supporti cartacei, ad esclusione dei dati fiscali del Cliente per scopi contabili.

8. Misure organizzative
Tutto il personale autorizzato alla visione, anche parziale, delle informazioni memorizzate degli utenti per motivi di assistenza e/o monitoraggio è regolarmente autorizzato tramite lettera d'incarico che lo vincola alla riservatezza.
L'utente ha la possibilità di richiedere la cancellazione completa dalla piattaforma di tutte le informazioni da lui memorizzate facendone espressa richiesta via email a info@adamogestionale.it

Sub-Allegato C

Sub-responsabili approvati

Nome	Indirizzo	Riferimenti
Stripe Inc	510 Townsend Street San Francisco, CA 94103	https://stripe.com/us/privacy

Zendesk	1019 Market Street San Francisco, CA 94103, United States	https://www.zendesk.com/company/customers-partners/privacy-policy/
MailChimp (The Rocket Science Group)	675 Ponce de Leon Ave NE, Suite 5000 Atlanta, GA 30308	https://mailchimp.com/legal/privacy/
Hotjar Heat Maps & Recordings (Hotjar Ltd.)	Hotjar Ltd, Level 2 St Julians Business Centre, 3, Elia Zammit Street St Julians STJ 1000, Malta, Europe	https://www.hotjar.com/privacy
Amazon Web Services (AWS) (Amazon)	Amazon Web Services EMEA SARL, 5 rue Plaetis, L-2338, Luxembourg, ATTN: AWS EMEA Legal	https://aws.amazon.com/it/privacy/
DigitalOcean Inc.	101 6th Avenue, New York (NY) Usa	https://www.digitalocean.com/legal/privacy/
Bugsnag (Bugsnag Inc.)	39 Harrison St, San Francisco, CA 94107, Usa	https://bugsnag.com/docs/privacy
Uptime Robot (Buzpark Bilisim Tarim Urunleri Sanayi Tic. Ltd. Sti.)	Regent House, Office 21, Bisazza Street, Sliema SLM1640, Malta	https://uptimerobot.com/privacyPolicy
Google LLC	1600 Amphitheatre Parkway Mountain View, CA 94043 (USA)	https://policies.google.com/privacy?hl=it