Accordo sul Trattamento dei Dati

Accordo sul trattamento dei dati personali per conto di un titolare del trattamento ai sensi dell'Art. 28 GDPR

tra il cliente (di seguito denominato "**Cliente**") e CA Customer Alliance GmbH, Hausvogteipl. 12, 10117 Berlino, Germania (di seguito denominata "**Fornitore**").

Si prega di inviare eventuali domande o commenti relativi a questo accordo sul trattamento dei dati o alla protezione dei dati in generale al seguente indirizzo e-mail: dataprotextion@customer-alliance.com

1. **Oggetto dell'Accordo**

Nel corso della fornitura dei servizi come da accordo di servizio (di seguito denominato "**Accordo Principale**"), è necessario che il Fornitore gestisca dati personali rispetto ai quali il Cliente agisce in qualità di titolare del trattamento in termini di legge sulla protezione dei dati (di seguito denominati "**Dati del Cliente**"). Questo accordo specifica gli obblighi e i diritti di protezione dei dati delle parti in relazione all'utilizzo dei Dati del Cliente da parte del Fornitore per fornire i servizi previsti dall'Accordo Principale.

2. **Ambito dell'incarico**

    1. Il Fornitore tratterà i Dati del Cliente per conto e in conformità con le istruzioni del Cliente ai sensi dell'Art. 28 GDPR (Trattamento per Conto). Il Cliente rimane il titolare del trattamento in termini di legge sulla protezione dei dati.

    2. Il trattamento dei Dati del Cliente da parte del Fornitore avviene nelle modalità e nell'ambito e per le finalità determinate nell'Allegato 1 del presente accordo; il trattamento si riferisce ai tipi di dati personali e alle categorie di interessati ivi specificati. La durata del trattamento corrisponde alla durata dell'Accordo Principale.

    3. Il trattamento dei Dati del Cliente da parte del Fornitore avviene in linea di principio all'interno dell'Unione Europea o di un altro stato contraente dello Spazio Economico Europeo (SEE). Al Fornitore è tuttavia consentito trattare i Dati del Cliente in conformità con le disposizioni del presente accordo al di fuori del SEE se informa preventivamente il Cliente sul luogo del trattamento dei dati e se sono soddisfatti i requisiti degli Artt. 44-48 GDPR o se si applica un'eccezione ai sensi dell'Art. 49 GDPR.

3. **Diritto del Cliente di impartire istruzioni**

    1. Il Fornitore tratta i Dati del Cliente in conformità con le istruzioni del Cliente, a meno che il Fornitore non sia legalmente obbligato a fare diversamente. In quest'ultimo caso, il Fornitore informerà il Cliente di tale requisito legale prima del trattamento, a meno che tale legge non vieti tali informazioni per importanti motivi di interesse pubblico.

    2. Le istruzioni del Cliente sono in linea di principio definitivamente stabilite e documentate nelle disposizioni del presente accordo. Istruzioni individuali che si discostano dalle disposizioni del presente accordo o che impongono requisiti aggiuntivi richiedono un accordo reciproco e devono essere fatte per iscritto.

    3. Il Fornitore garantirà che i Dati del Cliente siano trattati in conformità con le istruzioni impartite dal Cliente. Se il Fornitore è del parere che un'istruzione impartita dal Cliente violi questo accordo o la legge applicabile sulla protezione dei dati, è autorizzato, dopo aver informato di conseguenza il Cliente, a sospendere l'esecuzione dell'istruzione fino a quando il Cliente non confermi l'istruzione.

4. **Responsabilità Legale del Cliente**

1. Il Cliente è l'unico responsabile della liceità del trattamento dei Dati del Cliente e della salvaguardia dei diritti degli interessati nel rapporto tra le parti.

2. Il Cliente è responsabile di fornire al Fornitore i Dati del Cliente in tempo utile per la prestazione dei servizi secondo l'Accordo Principale ed è responsabile della qualità dei Dati del Cliente. Il Cliente informerà il Fornitore immediatamente e completamente se durante l'esame dei risultati del Fornitore riscontra errori o irregolarità in merito alle disposizioni sulla protezione dei dati o alle sue istruzioni.

3. Se il Fornitore è tenuto a fornire informazioni a un ente governativo o a una persona sul trattamento dei Dati del Cliente o a collaborare con questi organismi in qualsiasi altro modo, il Cliente è obbligato, su prima richiesta, ad assistere il Fornitore nel fornire tali informazioni e nell'adempiere ad altri obblighi di cooperazione.

5. **Requisiti per il personale**

Il Fornitore impegnerà tutte le persone coinvolte nel trattamento dei Dati del Cliente alla riservatezza rispetto al trattamento dei Dati del Cliente.

6. **Sicurezza del trattamento**

1. Il Fornitore adotta, ai sensi dell'Art. 32 GDPR, le necessarie, appropriate misure tecniche e organizzative, tenendo conto dello stato della tecnica, dei costi di implementazione e della natura, dell'ambito, delle circostanze e delle finalità dei Dati del Cliente, nonché della diversa probabilità e gravità del rischio per i diritti e le libertà degli interessati, al fine di garantire un livello di protezione dei Dati del Cliente adeguato al rischio. Le misure attuali sono riportate nell'**Allegato 2**.

2. Il Fornitore avrà il diritto di modificare le misure tecniche e organizzative durante il periodo dell'accordo, purché continuino a rispettare i requisiti di legge.

7. **Coinvolgimento di ulteriori responsabili del trattamento**

1. Il Cliente concede al Fornitore l'autorizzazione generale per coinvolgere ulteriori responsabili del trattamento relativamente al trattamento dei Dati del Cliente. Ulteriori responsabili del trattamento consultati al momento della conclusione dell'accordo risultano dall'**Allegato 3**. In generale, non è richiesta alcuna autorizzazione per i rapporti contrattuali con fornitori di servizi che si occupano dell'esame o della manutenzione di procedure o sistemi di trattamento dati da parte di terzi o che implicano altri servizi aggiuntivi, anche se non può essere escluso l'accesso ai Dati del Cliente, purché il Fornitore adotti misure ragionevoli per proteggere la riservatezza dei Dati del Cliente.

2. Il Fornitore notificherà al Cliente eventuali modifiche previste in relazione alla consultazione o alla sostituzione di ulteriori responsabili del trattamento. Nei singoli casi, il Cliente ha il diritto di opporsi al coinvolgimento di un potenziale ulteriore responsabile del trattamento. Un'obiezione può essere sollevata dal Cliente solo per importanti motivi che devono essere dimostrati al Fornitore. Nella misura in cui il Cliente non si oppone entro 14 giorni dal ricevimento della notifica, il suo diritto di opporsi al corrispondente coinvolgimento decade. Se il Cliente si oppone, il Fornitore ha il diritto di risolvere l'Accordo Principale e questo accordo con un periodo di preavviso di tre (3) mesi.

3. L'accordo tra il Fornitore e l'ulteriore responsabile del trattamento deve imporre a quest'ultimo gli stessi obblighi che incombono al Fornitore ai sensi del presente accordo. Le parti concordano che questo requisito è soddisfatto se il contratto ha un livello di protezione

corrispondente a questo accordo, rispettivamente se gli obblighi stabiliti nell'Art. 28 par. 3 GDPR sono imposti all'ulteriore responsabile del trattamento.

8. **Diritti degli interessati**

    1. Il Fornitore supporterà il Cliente, entro limiti ragionevoli, in virtù di misure tecniche e organizzative nell'adempimento dell' obbligo di quest'ultimo di rispondere alle richieste di esercizio dei diritti degli interessati.

    2. Nella misura in cui un interessato presenta una richiesta per l'esercizio dei suoi diritti direttamente al Fornitore, il Fornitore inoltrerà questa richiesta al Cliente in modo tempestivo.

    3. Il Fornitore informerà il Cliente di qualsiasi informazione relativa ai Dati del Cliente archiviati, ai destinatari dei Dati del Cliente ai quali il Fornitore dovrà divulgarli in conformità con l'istruzione e sullo scopo della conservazione, nella misura in cui il Cliente non dispone di queste informazioni e nella misura in cui non è in grado di raccoglierle da solo.

    4. Il Fornitore, nei limiti di ciò che è ragionevole e necessario, consentirà al Cliente di correggere, cancellare o limitare l'ulteriore trattamento dei Dati del Cliente, o su istruzione del Cliente correggerà, bloccherà o limiterà ulteriormente il trattamento stesso, se e nella misura in cui ciò sia impossibile per il Cliente.

9. **Obblighi di notifica e supporto del Fornitore**

    1. Nella misura in cui il Cliente è soggetto a un obbligo di notifica legale a causa di una violazione della sicurezza dei Dati del Cliente (in particolare ai sensi degli Artt. 33, 34 GDPR), il Fornitore informerà il Cliente in modo tempestivo di eventuali eventi segnalabili nel suo ambito di responsabilità. Il Fornitore assisterà il Cliente nell'adempimento degli obblighi di notifica su richiesta di quest'ultimo nella misura ragionevole e necessaria.

    2. Il Fornitore assisterà il Cliente nella misura ragionevole e necessaria con le valutazioni d'impatto sulla protezione dei dati da effettuarsi da parte del Cliente e, se necessario, successive consultazioni con l'autorità di controllo ai sensi degli Artt. 35, 36 GDPR.

10. **Cancellazione dei Dati del Cliente**

    1. Il Fornitore cancellerà i Dati del Cliente alla scadenza del presente accordo, a meno che il Fornitore non sia obbligato per legge a conservare ulteriormente i Dati del Cliente.

    2. Il Fornitore può conservare la documentazione, che serve come prova del trattamento ordinato e accurato dei Dati del Cliente, anche dopo la cessazione dell'accordo.

11. **Prove e audit**

    1. Il Fornitore fornirà al Cliente, su richiesta di quest'ultimo, tutte le informazioni richieste e disponibili al Fornitore per dimostrare la conformità ai suoi obblighi ai sensi del presente accordo.

    2. Il Cliente avrà il diritto di sottoporre ad audit il Fornitore in merito alla conformità alle disposizioni del presente accordo, in particolare all'attuazione delle misure tecniche e organizzative; incluse le ispezioni.

    3. Per effettuare ispezioni in conformità con la Sezione 11.2, il Cliente ha il diritto di accedere ai locali commerciali del Fornitore in cui i Dati del Cliente vengono trattati entro il normale orario di lavoro (dal lunedì al venerdì dalle 10 alle 18) dopo tempestiva notifica preventiva in

conformità con la Sezione 11.5. a proprie spese, senza disturbare lo svolgimento delle attività e nel rigoroso rispetto della segretezza degli affari del Fornitore e dei segreti commerciali.

4. Il Fornitore ha il diritto, a sua discrezione e tenendo conto degli obblighi legali del Cliente, di non divulgare informazioni sensibili riguardanti l'attività del Fornitore o se il Fornitore violerebbe disposizioni di legge o altre disposizioni contrattuali a seguito della sua divulgazione. Il Cliente non ha il diritto di accedere a dati o informazioni sui clienti del Fornitore, informazioni sui costi, rapporti sul controllo di qualità e sulla gestione dei contratti, o qualsiasi altro dato confidenziale del Fornitore che non sia direttamente rilevante per le finalità di audit concordate.

5. Il Cliente informerà il Fornitore in tempo utile (di solito almeno due settimane in anticipo) di tutte le circostanze relative allo svolgimento dell'audit. Il Cliente può effettuare un audit per anno civile. Ulteriori audit sono effettuati contro rimborso dei costi e previa consultazione con il Fornitore.

6. Se il Cliente incarica un terzo per l'esecuzione dell'audit, il Cliente obbligherà il terzo per iscritto nello stesso modo in cui il Cliente è obbligato nei confronti del Fornitore secondo questa Sezione 11 del presente accordo. Inoltre, il Cliente obbligherà il terzo a mantenere segretezza e riservatezza, a meno che il terzo non sia soggetto a un obbligo professionale di segretezza.

7. A discrezione del Fornitore, la prova della conformità con gli obblighi ai sensi del presente accordo può essere fornita, invece di un' ispezione, presentando un'appropriata, attuale opinione o relazione di un'autorità indipendente (ad es. revisore dei conti, dipartimento di audit, responsabile della protezione dei dati, dipartimento di sicurezza IT, revisori della protezione dei dati o revisori della qualità) o una certificazione idonea da parte di audit sulla sicurezza IT o sulla protezione dei dati -- ad es. secondo "BSI-Grundschutz" -- ("rapporto di audit"), se il rapporto di audit consente al Cliente in modo appropriato di convincersi della conformità agli obblighi contrattuali.

12. **Durata del contratto e cessazione**

La durata e la cessazione del presente accordo sono disciplinate dalle disposizioni relative alla durata e alla cessazione dell'Accordo Principale. Una cessazione dell'Accordo Principale comporta automaticamente l'annullamento del presente accordo. È esclusa una cessazione isolata del presente contratto.

13. **Responsabilità**

1. La responsabilità del Fornitore ai sensi del presente accordo sarà disciplinata dalle limitazioni di responsabilità previste dall'Accordo Principale. Nella misura in cui terzi fanno valere pretese contro il Fornitore che sono causate dalla violazione colposa del presente accordo o di uno dei suoi obblighi come titolare del trattamento in termini di legge sulla protezione dei dati che lo riguarda, il Cliente dovrà su prima richiesta indennizzare e manlevare il Fornitore da tali pretese.

2. Il Cliente si impegna a indennizzare il Fornitore su prima richiesta contro tutte le possibili multe imposte al Fornitore corrispondenti alla parte di responsabilità del Cliente per la violazione sanzionata dalla multa.

14. **Disposizioni finali**

1. Le controversie derivanti dal presente contratto saranno disciplinate dalla legge tedesca. Il luogo di esecuzione e la giurisdizione sarà la sede legale dell'Appaltatore. In caso di contraddizioni nelle due versioni linguistiche, prevarrà la versione tedesca.

2. Nel caso in cui singole disposizioni del presente accordo siano inefficaci o diventino inefficaci o contengano una lacuna, le restanti disposizioni rimarranno inalterate. Le parti si impegnano a sostituire la disposizione inefficace con una disposizione legalmente ammissibile che si avvicini maggiormente allo scopo della disposizione inefficace e che soddisfi in tal modo i requisiti dell'Art. 28 GDPR.

3. In caso di conflitti tra il presente accordo e altri accordi tra le parti, in particolare l'Accordo Principale, prevalgono le disposizioni del presente accordo.

Allegato:

Allegato 1: Scopo, tipo ed estensione del trattamento dei Dati del Cliente, tipi di dati personali e categorie di interessati

Allegato 2: Misure tecniche e organizzative

Allegato 3: Ulteriori Responsabili del Trattamento

Allegato 1 - Scopo, tipo ed estensione del trattamento dei Dati del Cliente, tipi di dati personali e categorie di interessati

1. **Scopo del trattamento dei dati**

Il Fornitore invia messaggi ai clienti finali del e per conto del Cliente prima e durante la fornitura del suo servizio per ottenere feedback, migliorare, standardizzare e automatizzare la comunicazione tra il Cliente e i suoi clienti finali. I risultati vengono elaborati e valutati per conto del Cliente. Inoltre, le valutazioni provenienti da feedback indiretto e derivato, come informazioni da fonti interne e/o pubbliche, vengono utilizzate per rappresentare pienamente la voce del cliente finale. Il Fornitore aggrega e quindi anonimizza i dati del Cliente raccolti attraverso la piattaforma al fine di offrire al Cliente servizi aggiuntivi come reportistica, benchmarking e funzionalità di monitoraggio KPI relative al feedback fornito dai clienti finali del Cliente.

2. **Tipi di dati personali**

a. Dati anagrafici (es. nome, genere, lingua);

b. Dati di contatto (es. indirizzo e-mail, indirizzo, n. di telefono);

c. Dati di comunicazione (es. corrispondenza e-mail);

d. Dati contrattuali (es. durata del contratto, informazioni sulla fornitura del servizio come fatturato o costi);

e. Se applicabile, dati di segmentazione individuali esistenti del Cliente per i suoi clienti finali come modalità di conclusione del contratto (internet, telefono, ecc.), paese di origine, categoria di servizio o fascia d'età;

f. Valutazione del Cliente da parte del cliente finale (recensione del cliente);

g. Analisi di soddisfazione (es. valutazioni di testo, argomento ed espressione).

3. **Categorie di interessati**

a. Personale del Cliente;

b. Clienti finali del Cliente;

c. Fornitori del Cliente.

Allegato 2 -- Misure tecniche e organizzative

Sono state adottate le seguenti misure tecniche e organizzative per proteggere i dati personali:

- **1. Controllo degli accessi fisici**

Alle persone non autorizzate deve essere negato l'accesso alle apparecchiature di elaborazione dati con cui vengono elaborati e utilizzati i dati personali.

Garantito da:

a. Definizione di aree di sicurezza e persone autorizzate

b. Sicurezza delle stanze (chiave, tapparella, ecc.)

c. Registro delle presenze

d. Sicurezza esterna dell'edificio (recinzione, porte/finestre di sicurezza)

e. Cura nella selezione delle guardie di sicurezza

f. Cura nella selezione dei servizi di pulizia

g. Videosorveglianza degli ingressi

h. Gestione delle chiavi / regolamento (apertura e chiusura) / documentazione dell'assegnazione delle chiavi

i. Sistema automatico di controllo degli accessi

j. Tessere con chip / sistemi di transponder

k. Sistema di chiusura manuale

l. Serrature di sicurezza

m. Porte con pomello (esterno)

n. Diritti di accesso altamente limitati alla sala server

o. Server in armadi server chiudibili a chiave, chiave presso il dipartimento IT

2. **Controllo degli accessi (esterno)**

Deve essere impedito che i sistemi di elaborazione dati possano essere utilizzati da persone non autorizzate.

Garantito da:

a. Possibilità di chiusura della stazione dati

b. Login con nome utente e password e specifiche per la loro modifica (periodo di validità max. 1 anno)

c. Crittografia delle password

d. Software antivirus per server

e. Software antivirus per client

f. Firewall

g. Mobile Device Management

h. Utilizzo di tunnel VPN per l'accesso remoto

i. Blocco delle interfacce esterne (USB)

j. Crittografia di notebook / tablet

k. Gestione delle autorizzazioni utente

l. Creazione di profili utente

m. Assegnazione centralizzata delle password

n. Politica di password sicure

o. Politica di cancellazione / distruzione

p. Politica di protezione dei dati e sicurezza

3. **Controllo degli accessi (interno)**

Occorre assicurarsi che coloro che sono autorizzati a utilizzare un sistema di elaborazione dati possano accedere solo ai dati soggetti alla loro autorizzazione di accesso e che i dati personali non possano essere letti, copiati, modificati o rimossi senza autorizzazione durante l'elaborazione, l'uso e dopo la memorizzazione.

Garantito da:

a. Autenticazione con utenti + password

b. Gestione dei diritti graduata per utente / definizione dei ruoli

c. Gestione dei diritti utente da parte degli amministratori

d. Numero minimo di amministratori

e. Documentazione della gestione dei diritti

f. Oscuramento dello schermo durante le interruzioni del lavoro

g. Aggiornamenti di sicurezza regolari

h. Distruggidocumenti (min. livello 3, taglio incrociato)

i. Registrazione degli accessi alle applicazioni, in particolare durante l'inserimento, la modifica e la cancellazione dei dati

j. Politica di password sicure

k. Politica di cancellazione / distruzione

l. Politica di protezione dei dati e sicurezza

4. **Controllo della separazione**

Garantire che i dati raccolti per scopi diversi possano essere elaborati separatamente.

Garantito da:

a. Sistemi software separati

b. Database e archiviazione separati

c. Controllo tramite concetto di autorizzazione

d. Separazione attraverso regolamenti di accesso

e. Impostazione dei diritti del database

5. **Controllo del trasferimento**

Deve essere garantito che i dati personali non possano essere letti, copiati, alterati o rimossi senza autorizzazione durante la trasmissione elettronica o durante il loro trasporto o memorizzazione su supporti dati, e che sia possibile verificare e stabilire in quali punti è prevista una trasmissione di dati personali mediante apparecchiature di trasmissione dati.

Garantito da:

a. Determinazione dei poteri per l'elaborazione dei dati

b. Determinazione delle parti autorizzate a trasmettere, dei destinatari della trasmissione e dei percorsi di trasmissione

c. Sicurezza del trasporto dei supporti dati

d. W-LAN protetto

e. Regolamenti sulla distruzione dei supporti dati

f. Crittografia delle e-mail (S/MIME, PGP, REDDCRYPT)

g. Politica di sicurezza IT

6. **Controllo dell'immissione**

Occorre assicurarsi che sia possibile verificare e stabilire retroattivamente se e da chi i dati personali sono stati inseriti nei sistemi di elaborazione dati, alterati o rimossi.

Garantito da:

a. Gestione degli accessi in lettura / scrittura

b. Registrazione degli accessi in lettura/scrittura e delle chiamate di programma

c. Marcatura dei documenti di immissione dati con nome e data dopo l'immissione

d. Disposizioni sulla modifica dei diritti di accesso e della responsabilità dei dati

e. Rigorose responsabilità per le cancellazioni

7. **Controllo della disponibilità**

Occorre assicurarsi che i dati personali siano protetti contro la distruzione o la perdita accidentale.

Garantito da:

a. Creazione di copie di backup periodiche

b. Protezione UPS in caso di interruzione di corrente

c. Protezione antivirus/firewall

d. Piano di emergenza

e. Piano di ripristino

f. Protezione DDoS permanentemente attiva

8. **Controllo dell'elaborazione dell'ordine**

Deve essere garantito che i dati personali elaborati per conto del cliente possano essere elaborati solo in conformità con le istruzioni del cliente.

Garantito da:

a. Determinazione dei diritti e degli obblighi del contraente

b. Contratto per l'elaborazione dati commissionata

c. Formazione di tutti i dipendenti con diritti di accesso

d. Audit regolari sulla protezione dei dati

e. Accordo sui diritti di controllo e audit

f. Il contraente nomina il responsabile della protezione dei dati o la persona responsabile

Azienda, indirizzo	**Servizio/Tipologia del trattamento**	**Copertura legale**	**Misure per un livello di protezione comparabile (solo nei paesi terzi)**
ALL-INKL.COM - Neue Medien Münnich, Hauptstraße 68, 02742 Friedersdorf Germania	Hosting Web	Accordo sul trattamento dei dati	/

Apollo 415 Mission Street, Piano 37, San Francisco, California 94105, U.S.A.	Arricchimento dei dati	Clausola contrattuale standard e valutazione individuale per un livello di protezione paragonabile allo standard all'interno dell'UE.	Certificato ISO (27001) e conformità SOC-2 certificata da A-LIGN.
char desarrollo de sistemas s.l.u. Parque Empresarial Arboretum – Avda. de la Fama, 16-20, 3ª pianta 08940 Cornellà de Llobregat – Barcellona – Spagna	Fornitore di sistemi di gestione della proprietà	Accordo sul trattamento dei dati	Crittografia dei dati inattivi e in transito: HTTPS per tutti i servizi che utilizzano TLS (SSL) ed è completamente conforme al GDPR
CHARGEBEE INC., 340 S. Lemon Avenue, Suite #1537, Noce, CA 91789 Stati Uniti	Fatturazione	Clausola contrattuale standard e valutazione individuale per un livello di protezione paragonabile allo standard all'interno dell'UE.	Certificazioni e audit di terze parti; Certificato ISO27001; standard SOC 1/SOC 2 e MFA; politiche di sicurezza a livello di rete, applicazione e operativo; Configurazione di sicurezza AWS: numerose certificazioni per data center, tra cui conformità ISO 27001, certificazione PCI e report SOC.

Google LLC, 1600 Amphitheatre Parkway, vista sulle montagne, CA 94043 Stati Uniti	Google WorkspaceGoogle Analytics	Clausola contrattuale standard e valutazione individuale per un livello di protezione paragonabile allo standard all'interno dell'UE.	Certificati ISO (ISO 27001, 27017, 27018); Linee guida sulla protezione dei dati; Centro conformità e report.
HelpScout PBC 177 Huntington Ave, Boston, MA 02115, Stati Uniti	Helpdesk di supporto	Clausola contrattuale standard e valutazione individuale per un livello di protezione paragonabile allo standard all'interno dell'UE.	Help Scout è certificato SOC2 Tipo 2 per sicurezza e disponibilità. Leggi dell'UE sulla protezione dei dati, incluso il Regolamento generale sulla protezione dei dati dell'UE ("GDPR dell'UE") Configurazione della sicurezza AWS
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen Germania	Ospitare	Accordo sul trattamento dei dati	/
HubSpot, Inc., 25 First Street, Cambridge, MA 02141 USA	Marketing in entrata, vendite, successo dei clienti e gestione delle relazioni con i clienti	Clausola contrattuale standard e valutazione individuale per un livello di protezione paragonabile allo standard all'interno dell'UE.	Norme aziendali vincolanti; Data Center (certificato ISO 27001 / audit SOC 2); Crittografia HTTP.
Luzmo NV Tiensevest 102 scatola 201, B-3000 Lovanio, Belgio	Analisi conversazionale	#VALUE!	Conforme AICPA SOC 2 Tipo II

Mailgun Technologies, Inc., 548 Market Street, Suite 43099, San Francisco, CA 94101 Stati Uniti	Provider di posta elettronica (API di posta elettronica)	Clausola contrattuale standard e valutazione individuale per un livello di protezione paragonabile allo standard all'interno dell'UE.	Scansione della rete esterna e test di penetrazione; crittografia dei dati; rilevamento delle intrusioni; Procedura di gestione dei fornitori: controllo e audit frequenti di tutti i sub-responsabili del trattamento.
Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399 U.S.A.	Ufficio 365	Clausola contrattuale standard e valutazione individuale per un livello di protezione paragonabile allo standard all'interno dell'UE.	Rapporti di fiducia e audit esterni; ISO27001, 27017, 27018, 22301, 277701 certificati; politica di prevenzione della perdita di dati; Conforme a SSAE 18 SOC 1 Tipo II e SSAE 18 SOC 2 Tipo II.
Nonio Rua Eng.º Frederico Ulrich, 2650 4470-605 Moreira da Maia Portogallo	Fornitore di sistemi di gestione della proprietà	Accordo sul trattamento dei dati	Crittografia dei dati inattivi e in transito: HTTPS per tutti i servizi che utilizzano TLS (SSL) ed è completamente conforme al GDPR
OpenAI OpCo, LLC 3180 18th Street, San Francisco, CA 94110	Approfondimenti, reportistica, analisi	Accordo sul trattamento dei dati	/

OVH GmbH, Via St. Johanner. 41-43, 66111 Saarbrücken Germania	Ospitare	Accordo sul trattamento dei dati	/
Scaling Technologies GmbH, Pfarrer-Hillmann-Weg 1, 51069 Colonia Germania	Operazioni Web	Accordo sul trattamento dei dati	/
Striscia, Inc. 510 Townsend Street, San Francisco, CA 94103 Stati Uniti	Soluzione di pagamento	Clausola contrattuale standard e valutazione individuale per un livello di protezione paragonabile allo standard all'interno dell'UE.	Crittografia dei dati a riposo e in transito - HTTPS per tutti i servizi che utilizzano TLS (SSL); tutti i numeri delle carte sono crittografati a riposo con AES-256; registri di controllo; politica di gestione degli accessi; Certificato di fornitore di servizi PCI di livello 1.

Twilio, Inc., 375 Beale Street, Suite 300, San Francisco, CA 94105 Stati Uniti	Provider di messaggi brevi (SMS)	Clausola contrattuale standard e valutazione individuale per un livello di protezione paragonabile allo standard all'interno dell'UE.	Norme aziendali vincolanti; quadro di sicurezza basato sulla norma ISO 27001; ISO/IEC 27001, ISO/IEC 27017 e 27018, SOC 2 Tipo II, PCI DSS Livello 1 certificati; Configurazione di sicurezza AWS: molteplici certificazioni per data center, tra cui conformità ISO 27001, certificazione PCI e report SOC; i database (dati del cliente) vengono crittografati utilizzando lo standard di crittografia avanzato e i dati del cliente vengono crittografati durante il transito tra l'applicazione software del cliente e i servizi utilizzando TLS v1.2; test di penetrazione; politiche e procedure di gestione degli incidenti di sicurezza in conformità con NIST SP 800-61.