La versione originale di questo Accordo di Elaborazione Dati informativa sulla privacy è stata redatta in inglese e successivamente tradotta in altre lingue. Queste traduzioni interne sono fornite unicamente per cortesia e non hanno valore legale.

Accordo di Elaborazione Dati

Accordo sul trattamento dei dati personali per conto di un responsabile del trattamento ai sensi dell'Art. 28 del GDPR tra il cliente (di seguito denominato "**Cliente**") e CA Customer Alliance GmbH, Ullsteinstr. 130, 12109 Berlino, Germania (di seguito denominato "**Fornitore**").

1. Oggetto dell'Accordo

Nell'ambito della prestazione di servizi ai sensi dell'accordo di servizio (di seguito denominato "**Accordo Principale**"), è necessario che il Fornitore tratti dati personali per conto del Cliente, per i quali il Cliente agisce come responsabile del trattamento ai sensi del diritto in materia di protezione dei dati (di seguito denominati "**Dati del Cliente**"). Questo accordo specifica gli obblighi di protezione dei dati e i diritti delle parti in relazione all'uso dei Dati del Cliente da parte del Fornitore per la prestazione dei servizi previsti nell'Accordo Principale.

2. Ambito dell'incarico

2.1. Il Fornitore tratterà i Dati del Cliente per conto e conformemente alle istruzioni del Cliente ai sensi dell'Art. 28 del GDPR (Trattamento per conto terzi). Il Cliente rimane il responsabile del trattamento ai sensi del diritto in materia di protezione dei dati.

2.2. Il trattamento dei Dati del Cliente da parte del Fornitore avviene secondo le modalità, la portata e lo scopo stabiliti nell'**Allegato 1** a questo accordo; il trattamento riguarda i tipi di dati personali e le categorie di soggetti interessati specificati nell'Allegato. La durata del trattamento corrisponde al termine dell'Accordo Principale.

2.3. Il trattamento dei Dati del Cliente da parte del Fornitore avverrà in linea di principio all'interno dell'Unione Europea o in un altro Stato contraente dello Spazio Economico Europeo (SEE). Tuttavia, il Fornitore è autorizzato a trattare i Dati del Cliente in conformità alle disposizioni di questo accordo al di fuori del SEE se informa preventivamente il Cliente sul luogo di trattamento dei dati e se sono soddisfatti i requisiti dell'Art. 44-48 del GDPR o se si applica un'eccezione di cui all'Art. 49 del GDPR.

3. Diritto del Cliente di impartire istruzioni

3.1. Il Fornitore tratta i Dati del Cliente conformemente alle istruzioni del Cliente, a meno che il Fornitore sia legalmente tenuto a procedere diversamente. In tal caso, il Fornitore informerà il Cliente di tale obbligo legale prima del trattamento, a meno che la legge vieti tale informazione per importanti ragioni di interesse pubblico.

3.2. Le istruzioni del Cliente sono in linea di principio definitivamente stabilite e documentate nelle disposizioni di questo accordo. Le istruzioni individuali che deviano dalle disposizioni di

questo accordo o che impongono requisiti aggiuntivi richiedono un accordo reciproco e devono essere scritte.

3.3. Il Fornitore garantisce che i Dati del Cliente siano trattati conformemente alle istruzioni fornite dal Cliente. Se il Fornitore ritiene che un'istruzione fornita dal Cliente violi questo accordo o il diritto applicabile in materia di protezione dei dati, è autorizzato, previa comunicazione al Cliente, a sospendere l'esecuzione dell'istruzione fino a quando il Cliente conferma l'istruzione.

4. Responsabilità legale del Cliente

4.1. Il Cliente è il solo responsabile della liceità del trattamento dei Dati del Cliente e della tutela dei diritti degli interessati nel rapporto tra le parti.

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

4.3. Se il Fornitore è tenuto a fornire informazioni a un organo governativo o a una persona in merito al trattamento dei Dati del Cliente o a collaborare con tali enti in qualsiasi altro modo, il Cliente è obbligato, su prima richiesta, ad assistere il Fornitore nella fornitura di tali informazioni e nell'adempimento di altre obbligazioni di collaborazione.

5. Requisiti per il personale

Il Fornitore impegna tutte le persone coinvolte nel trattamento dei Dati del Cliente a rispettare la riservatezza riguardo al trattamento dei Dati del Cliente.

6. Sicurezza del trattamento

6.1. Il Fornitore adotta, conformemente all'Art. 32 del GDPR, le misure tecniche e organizzative necessarie ed appropriate, tenendo conto dello stato dell'arte, dei costi di implementazione e della natura, portata, circostanze e finalità dei Dati del Cliente, nonché delle diverse probabilità e gravità del rischio per i diritti e le libertà degli interessati, al fine di garantire un livello di protezione adeguato dei Dati del Cliente in relazione al rischio. Le misure attuali sono riportate nell'**Allegato 2**.

6.2. Il Fornitore ha 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

7.1. Il Cliente concede al Fornitore l'autorizzazione generale a coinvolgere ulteriori responsabili del trattamento per quanto riguarda il trattamento dei Dati del Cliente. I responsabili del trattamento aggiuntivi consultati al momento della conclusione dell'accordo sono indicati nell'**Allegato 3**. In generale, non è richiesta un'autorizzazione per le relazioni contrattuali con

fornitori di servizi che si occupano dell'esame o della manutenzione di procedure o sistemi di trattamento dei dati da parte di terzi o che prevedono altri servizi aggiuntivi, anche se l'accesso ai Dati del Cliente non può essere escluso, purché il Fornitore adotti misure ragionevoli per proteggere la riservatezza dei Dati del Cliente.

7.2. Il Fornitore informerà il Cliente di eventuali modifiche previste riguardo alla consultazione o alla sostituzione dei responsabili del trattamento aggiuntivi. In casi specifici, il Cliente ha il diritto di opporsi al coinvolgimento di un potenziale responsabile del trattamento aggiuntivo. L'opposizione può essere sollevata solo per importanti motivi che devono essere dimostrati al Fornitore. Nel caso in cui il Cliente non si opponga entro 14 giorni dalla ricezione della notifica, scade il suo diritto di opporsi al coinvolgimento corrispondente. Se il Cliente si oppone, il Fornitore ha il diritto di risolvere l'Accordo Principale e questo accordo con un preavviso di tre (3) mesi.

7.3. L'accordo tra il Fornitore e il responsabile del trattamento aggiuntivo deve imporre a quest'ultimo gli stessi obblighi che incombono al Fornitore in base a questo accordo. Le parti concordano che tale requisito è soddisfatto se il contratto prevede un livello di protezione corrispondente a questo accordo, ovvero se sono imposti al responsabile del trattamento aggiuntivo gli obblighi previsti dall'Art. 28, paragrafo 3, del GDPR.

8. Diritti degli interessati

8.1. Il Fornitore supporterà il Cliente in modo ragionevole attraverso misure tecniche e organizzative nell'adempimento dell'obbligo del Cliente di rispondere alle richieste per l'esercizio dei diritti degli interessati.

8.2. Qualora un interessato presenti una richiesta per l'esercizio dei suoi diritti direttamente al Fornitore, il Fornitore trasmetterà tempestivamente questa richiesta al Cliente.

8.3. Il Fornitore informerà il Cliente di qualsiasi informazione relativa ai Dati del Cliente memorizzati, sui destinatari dei Dati del Cliente ai quali il Fornitore li comunicherà in conformità alle istruzioni e sullo scopo della memorizzazione, fino a quando il Cliente non dispone di queste informazioni e non è in grado di raccoglierle da solo.

8.4. Il Fornitore, entro i limiti del ragionevole e del necessario, consentirà al Cliente di correggere, cancellare o limitare ulteriormente il trattamento dei Dati del Cliente, o su istruzione del Cliente correggerà, bloccherà o limiterà ulteriormente il trattamento stesso, se ciò è impossibile per il Cliente.

9. Obblighi di notifica e di assistenza del Fornitore

9.1. Nella misura in cui il Cliente è soggetto a un obbligo di notifica previsto dalla legge a causa di una violazione della sicurezza dei Dati del Cliente (in particolare ai sensi dell'Art. 33 e 34 del GDPR), il Fornitore informerà tempestivamente il Cliente di tutti gli eventi notificabili nella sua area di responsabilità. Il Fornitore assisterà il Cliente nell'adempimento degli obblighi di notifica su richiesta del Cliente, nella misura ragionevole e necessaria.

9.2. Il Fornitore assisterà il Cliente, nella misura ragionevole e necessaria, nelle valutazioni d'impatto sulla protezione dei dati da effettuare dal Cliente e, se necessario, nelle consultazioni successive con l'autorità di controllo ai sensi dell'Art. 35 e 36 del GDPR.

10. Cancellazione dei Dati del Cliente

10.1. Il Fornitore cancellerà i Dati del Cliente al termine di questo accordo, a meno che il Fornitore sia obbligato per legge a conservare ulteriormente i Dati del Cliente.

10.2. Il Fornitore potrà conservare la documentazione che serve come prova dell'elaborazione ordinata e precisa dei Dati del Cliente anche dopo la conclusione dell'accordo.

11. Prove e ispezioni

11.1. Il Fornitore fornirà al Cliente, su richiesta del Cliente, tutte le informazioni richieste e disponibili al Fornitore per dimostrare la conformità alle sue obbligazioni in base a questo accordo.

11.2. Il Cliente avrà il diritto di effettuare ispezioni presso il Fornitore per verificare il rispetto delle disposizioni di questo accordo, in particolare l'attuazione delle misure tecniche e organizzative, comprese le ispezioni.

11.3. Per effettuare ispezioni conformemente all'Art. 11.2, il Cliente avrà il diritto di accedere ai locali aziendali del Fornitore in cui vengono trattati i Dati del Cliente nei normali orari di lavoro (dal lunedì al venerdì dalle 10:00 alle 18:00) previa notifica anticipata in conformità all'Art. 11.5, a proprie spese, senza interruzioni dell'attività aziendale e nel rispetto rigoroso dei segreti aziendali e commerciali del Fornitore.

11.4. Il Fornitore avrà il diritto, a sua discrezione e tenendo conto degli obblighi legali del Cliente, di non divulgare informazioni sensibili per quanto riguarda l'attività del Fornitore o se il Fornitore violerebbe disposizioni di legge o contrattuali diverse in caso di divulgazione. Il Cliente non avrà diritto di accedere a dati o informazioni sui clienti del Fornitore, informazioni sui costi, rapporti di controllo di qualità e gestione contrattuale o altre informazioni confidenziali del Fornitore che non siano direttamente rilevanti per gli scopi di audit concordati.

11.5. Il Cliente informerà il Fornitore in anticipo (di solito almeno due settimane prima) di tutte le circostanze relative all'esecuzione dell'audit. Il Cliente può effettuare un audit all'anno solare. Ulteriori audit saranno effettuati a pagamento e previa consultazione con il Fornitore.

11.6. Se il Cliente incarica un terzo di effettuare l'audit, il Cliente dovrà obbligare per iscritto il terzo nello stesso modo in cui il Cliente è obbligato nei confronti del Fornitore in base a questa Sezione 11 di questo accordo. Inoltre, il Cliente dovrà obbligare il terzo a mantenere la segretezza e la riservatezza, a meno che il terzo sia soggetto a un obbligo professionale di segretezza.

11.7. A discrezione del Fornitore, la prova della conformità alle obbligazioni in base a questo accordo potrà essere fornita, anziché attraverso un'ispezione, mediante la presentazione di una idonea e attuale opinione o relazione da parte di un'autorità indipendente (ad esempio,

revisore, reparto di audit, responsabile della protezione dei dati, reparto di sicurezza informatica, revisori della protezione dei dati o revisori della qualità) o una certificazione adeguata da parte di una autorità indipendente della sicurezza informatica o della protezione dei dati, ad esempio secondo il "BSI-Grundschutz", ("relazione di audit"), se la relazione di audit consente al Cliente di convincersi in modo adeguato della conformità alle obbligazioni contrattuali.

12. Durata del contratto e risoluzione

La durata e la risoluzione di questo accordo saranno disciplinate dalle disposizioni di durata e risoluzione dell'Accordo Principale. La risoluzione dell'Accordo Principale comporta automaticamente la cancellazione di questo accordo. La risoluzione isolata di questo contratto è esclusa.

13. Responsabilità

13.1. La responsabilità del Fornitore in base a questo accordo sarà disciplinata dalle limitazioni di responsabilità previste nell'Accordo Principale. Nella misura in cui terzi avanzino pretese contro il Fornitore che siano causate dalla violazione colpevole del Cliente di questo accordo o di una delle sue obbligazioni come responsabile del trattamento ai sensi del diritto in materia di protezione dei dati, il Cliente, su prima richiesta, indennizzerà e manterrà il Fornitore indenne da tali pretese.

13.2. Il Cliente si impegna a indennizzare il Fornitore su prima richiesta da tutte le possibili sanzioni pecuniarie inflitte al Fornitore corrispondenti alla parte di responsabilità del Cliente per l'infrazione sanzionata con la sanzione.

14. Disposizioni finali

14.1. Le controversie derivanti da questo contratto saranno regolate dalla legge tedesca. Il luogo di esecuzione e giurisdizione sarà la sede del Fornitore. In caso di contraddizioni tra le due versioni linguistiche, prevarrà la versione tedesca.

14.2. In caso di inadempimento o inefficacia di singole disposizioni di questo accordo o di lacune, le restanti disposizioni rimarranno inalterate. Le parti si impegnano a sostituire la disposizione inefficace con una disposizione legalmente valida che si avvicini il più possibile allo scopo della disposizione inefficace e che soddisfi i requisiti dell'Art. 28 del GDPR.

14.3. In caso di conflitti tra questo accordo e altre intese tra le parti, in particolare l'Accordo Principale, le disposizioni di questo accordo prevarranno.

Allegati:

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

Allegato 2: Misure tecniche e organizzative

Allegato 3: Responsabili del trattamento aggiuntivi

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

1. Scopo del trattamento dei dati

Il Fornitore invia messaggi ai clienti finali a nome del Cliente, prima e durante la fornitura dei suoi servizi, al fine di ottenere feedback, migliorare, standardizzare ed automatizzare la comunicazione tra il Cliente e i suoi clienti finali. I risultati vengono elaborati ed valutati per conto del Cliente. Inoltre, vengono utilizzate valutazioni basate su feedback indiretti e derivati, come informazioni provenienti da fonti interne e/o pubbliche, al fine di rappresentare appieno 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 la creazione di report, il benchmarking e il monitoraggio degli indicatori chiave di prestazione (KPI) correlati al feedback fornito dai clienti finali del Cliente.

2. Tipi di dati personali

a) Dati anagrafici (ad esempio, nome, genere, lingua);

b) Dati di contatto (ad esempio, indirizzo e-mail, indirizzo, numero di telefono);

c) Dati di comunicazione (ad esempio, corrispondenza via e-mail);

d) Dati contrattuali (ad esempio, durata del contratto, informazioni sulla fornitura dei servizi 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 gruppo di età;

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

g) Analisi della soddisfazione (ad esempio, valutazioni di testo, argomento ed espressione).

3. Categorie di soggetti interessati

a) Personale del Cliente;

b) Clienti finali del Cliente;

c) Fornitore del Cliente.

Allegato 2 - Misure tecniche e organizzative

Le seguenti misure tecniche e organizzative sono state adottate per proteggere i dati personali:

1. Controllo di accesso

L'accesso alle apparecchiature di elaborazione dati con cui vengono trattati e utilizzati i dati personali sarà negato a persone non autorizzate.

Garantito da:

a) Definizione delle aree di sicurezza e delle persone autorizzate
b) Sicurezza della stanza (chiave, tapparella, ecc.)
c) Registro delle presenze
d) Sicurezza esterna dell'edificio (recinzione, porte/finestre di sicurezza)
e) Attenzione nella selezione delle guardie di sicurezza
f) Attenzione nella selezione dei servizi di pulizia
g) Videosorveglianza degli ingressi
h) Gestione delle chiavi / documentazione dell'assegnazione delle chiavi
i) Sistema automatico di controllo degli accessi
j) Schede chip / sistemi di trasponder
k) Sistema di bloccaggio manuale
l) Serrature di sicurezza
m) Porte con pomello (all'esterno)

2. Controllo degli accessi (esterni)

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

Garantito da:

a) Bloccabilità della stazione di lavoro
b) Accesso con nome utente e password e specifiche per modificarli
c) Crittografia delle password
d) Server Software Anti-Virus
e) Client Software Anti-Virus
f) Firewall
g) Gestione dispositivi mobili
h) Utilizzo di tunnel VPN per l'accesso remoto
i) Blocco delle interfacce esterne (USB)
j) Crittografia di notebook / tablet
k) Gestione dei permessi degli utenti
l) Creazione di profili utente
m) Assegnazione centralizzata delle password
n) Politica di sicurezza delle password sicura

o) Politica di cancellazione / distruzione
p) Politica sulla protezione dei dati e sulla sicurezza

3. Controllo degli accessi (interni)

Si deve garantire 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) Gestione dei diritti specifici dell'utente
b) Gestione dei diritti dell'utente da parte degli amministratori
c) Numero minimo di amministratori
d) Documentazione della gestione dei diritti
e) Oscuramento dello schermo durante l'interruzione del lavoro
f) Aggiornamenti regolari per la sicurezza
g) Distruggi documenti (almeno livello 3, taglio trasversale)
h) Registrazione degli accessi alle applicazioni, in particolare all'ingresso, alla modifica e alla cancellazione dei dati

4. Controllo della separazione

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

Garantito da:
a) Sistemi software separati
b) Database e memorizzazione 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, modificati o rimossi senza autorizzazione durante la trasmissione elettronica o durante il loro trasporto o archiviazione su supporti dati e che sia possibile verificare e stabilire in quali punti è prevista una trasmissione dei dati personali tramite apparecchiature di trasmissione dati.

Garantito da:
a) Determinazione dei poteri per il trattamento dei dati
b) Determinazione delle parti trasmettenti autorizzate, dei destinatari della trasmissione e delle vie di trasmissione autorizzate
c) Sicurezza del trasporto dei supporti dati

d) W-LAN sicuro
e) Norme sulla distruzione dei supporti dati
f) Crittografia

6. Controllo dell'input

Deve essere garantito che sia possibile verificare e stabilire retrospettivamente se e da chi sono stati inseriti, modificati o rimossi dati personali nei sistemi di elaborazione dati.

Garantito da:
a) Gestione dell'accesso in lettura / scrittura
b) Registrazione degli accessi in lettura/scrittura e delle chiamate dei programmi
c) Marcatura dei documenti di inserimento dati con nome e data dopo l'inserimento
d) Disposizioni sulla modifica dei diritti di accesso e della responsabilità dei dati
e) Rigorose responsabilità per le cancellazioni

7. Controllo della disponibilità

Si deve garantire che i dati personali siano protetti da distruzione o 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 del trattamento dell'ordine

Deve essere garantito che i dati personali trattati per conto del cliente possano essere trattati solo in conformità alle istruzioni del cliente.

Garantito da:
a) Determinazione dei diritti e degli obblighi dell'appaltatore
b) Contratto per il trattamento dati per conto del cliente
c) Formazione di tutti i dipendenti con diritti di accesso
d) Audit regolari sulla protezione dei dati
e) Accordo su diritti di controllo e audit

Allegato 3: Responsabili del trattamento aggiuntivi			
Azienda, Indirizzo	**Servizio / Tipo di Elaborazion**	**Copertura Legale**	**Misure per un Livello di Protezione Comparabile (solo nei Paesi Terzi)**
ALL-INKL.COM - Neue Medien Münnich, Hauptstraße 68, 02742 Friedersdorf Germany	Web-Hosting	Accordo di Elaborazione Dati	/
CHARGEBEE INC., 340 S. Lemon Avenue, Suite #1537, Walnut, CA 917 89 USA	Fatturazione	Clausa contrattuale standard e valutazione individuale per un livello di protezione comparabile a quello standard all'interno dell'UE.	Certificazioni e audit di terze parti; certificato ISO 27001; standard SOC 1/SOC 2 e autenticazione a più fattori (MFA); politiche di sicurezza a livello di rete, applicazione e operativo; configurazione di sicurezza AWS - multiple certificazioni per i data center, inclusa la conformità ISO 27001, la certificazione PCI e i rapporti
Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 940 43 USA	Google Workspace Google Analytics	Clausa contrattuale standard e valutazione individuale per un livello di protezione comparabile a quello standard all'interno dell'UE.	Certificazioni ISO (ISO 27001, 27017, 27018); Linee guida sulla protezione dei dati; Centro di conformità e relazioni.
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen Germany	Hosting	Accordo di Elaborazione Dati	/
HubSpot, Inc., 25 First Street, Cambridge, MA 02141 USA	Inbound Marketing e Vendite	Clausa contrattuale standard e valutazione individuale per un livello di protezione comparabile a quello standard all'interno dell'UE.	Regole aziendali vincolanti; Centro dati (certificato ISO 27001 / audit SOC 2); crittografia HTTPs.

ALL-INKL.COM - Neue Medien Münnich, Hauptstraße 68, 02742 Friedersdorf Germany	Chat in diretta	Clausa contrattuale standard e valutazione individuale per un livello di protezione comparabile a quello standard all'interno dell'UE.	Audits esterni, test di penetrazione e programmi di ricerca di vulnerabilità; audit SOC 2; certificato ISO 27001; audit HIPAA; configurazione di sicurezza AWS; API ed endpoint dell'applicazione sono solo TLS/SSL; politica di sicurezza; formazione sulla sicurezza e sensibilizzazione.
CHARGEBEE INC., 340 S. Lemon Avenue, Suite #1537, Walnut, CA 91789 USA	Estrazione dati PMS (API)	Accordo di Elaborazione Dati	Adeguatezza della protezione dei dati personali nel Regno Unito - Decisione di attuazione della Commissione dell'UE del 28 giugno 2021 - C(2021) 4800.
Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043 USA	Fornitore di posta elettronica (API di posta elettronica)	Clausa contrattuale standard e valutazione individuale per un livello di protezione comparabile a quello standard all'interno dell'UE.	Scansione di rete esterna e test di penetrazione; crittografia dei dati; rilevamento delle intrusioni; procedura di gestione dei fornitori - controllo e audit frequente di tutti i sottoprocessori.
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen Germany	Office 365	Clausa contrattuale standard e valutazione individuale per un livello di protezione comparabile a quello standard all'interno dell'UE.	Rapporti esterni di fiducia e audit; certificati ISO 27001, 27017, 27018, 22301, 27701; politica di prevenzione della perdita di dati; conformità SSAE 18 SOC 1 Type II e SSAE 18 SOC 2 Type II.
HubSpot, Inc., 25 First Street, Cambridge, MA 02141 USA	Hosting	Accordo di Elaborazione Dati	/
Intercom, Inc., 55 2nd Street, 4th Fl., San Francisco, CA 94105 USA	Operazioni Web	Accordo di Elaborazione Dati	/

Impala Travel Technology Ltd., 70 White Lion Street, London, N1 9PP UK	Soluzione di pagamento	Clausa contrattuale standard e valutazione individuale per un livello di protezione comparabile a quello standard all'interno dell'UE.	Crittografia dei dati in fase di riposo e durante il trasporto - HTTPS per tutti i servizi che utilizzano TLS (SSL); tutti i numeri di carta sono crittografati in fase di riposo con AES-256; registri di audit; politica di gestione dell'accesso; certificato PCI Service Provider di Livello 1.
Mailgun Technologies, Inc., 548 Market Street, Suite 43099, San Francisco, CA 94101 USA	Gestione della relazione con il cliente	Clausa contrattuale standard e valutazione individuale per un livello di protezione comparabile a quello standard all'interno dell'UE.	Certificato SOC II; crittografia per tutte le password, dati chiave e copie di sicurezza; tutti i dati di produzione e dei clienti sono crittografati in transito e a riposo; autenticazione a più fattori; strumenti per la prevenzione della perdita di dati; ospitato in Irlanda (UE); configurazione di sicurezza AWS - multiple certificazioni per i data center, inclusa la conformità ISO 27001, la certificazione PCI e i rapporti SOC.
Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399 USA	Fornitore di messaggi brevi (SMS)	Clausa contrattuale standard e valutazione individuale per un livello di protezione comparabile a quello standard all'interno dell'UE.	Regole aziendali vincolanti; framework di sicurezza basato su ISO 27001; certificati ISO/IEC 27001, ISO/IEC 27017 e 27018, SOC 2 Type II, PCI DSS Livello 1; configurazione di sicurezza AWS - multiple certificazioni per i data center, inclusa la conformità ISO 27001, la certificazione PCI e il rapporto SOC; i database (dati dei clienti) sono crittografati utilizzando lo standard di crittografia avanzato e i dati dei clienti sono crittografati durante il transito tra l'applicazione software del cliente e i servizi tramite TLS v1.2; test di penetrazione; politiche e procedure di gestione degli incidenti di sicurezza in conformità con il NIST SP 800-61.