Palasil è un servizio di Terahold S.r.l. ("Terahold"). Questa pagina descrive le misure di sicurezza che Terahold applica al servizio Palasil alla data di questa versione. Gli impegni contrattuali di Terahold sulla sicurezza sono quelli dell'Appendice B del Data Processing Agreement (il "DPA"), che elenca le misure tecniche e organizzative e prevale su questa pagina in caso di differenze. I termini con l'iniziale maiuscola non definiti in questa pagina hanno il significato indicato nei Termini di servizio, disponibili su palasil.com/legal.

Questa pagina è pubblicata in inglese e in italiano. In caso di contrasto prevale la versione inglese (Palasil Security Overview).

1. Dove sono conservati e trattati i dati

1.1 La base di dati, l'autenticazione e l'archiviazione dei file del Servizio si trovano nell'Unione europea, a Francoforte. Le funzioni server dell'applicazione sono eseguite nell'Unione europea, a Francoforte. Il server applicativo dell'agente AI e l'archivio dei log tecnici si trovano nell'Unione europea.

1.2 Le richieste ai modelli linguistici usati dall'agente AI possono essere trattate fuori dall'Unione europea. I fornitori che eseguono i modelli devono avere sede negli Stati Uniti o in un paese che beneficia di una decisione di adeguatezza della Commissione europea, in base alle informazioni pubblicate da OpenRouter, Inc.; i server che usano possono trovarsi in altri paesi. Le richieste sono soggette a conservazione zero e non sono usate per l'addestramento, come descritto nella pagina AI e trasparenza.

1.3 Alcuni fornitori di Terahold sono stabiliti fuori dall'Unione europea, come indicato nella pagina Sub-responsabili. I trasferimenti di dati personali verso di essi sono coperti dalle garanzie del Capo V del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (il "GDPR"), come indicato in quella pagina.

1.4 L'infrastruttura che conserva i dati del Servizio si trova nell'Unione europea ed è soggetta alla legge dello Stato membro in cui si trova. Alcuni fornitori di quell'infrastruttura sono stabiliti fuori dall'Unione europea, per esempio negli Stati Uniti o a Singapore, e possono essere soggetti alla legge di quei paesi, compresa la legge sull'accesso ai dati da parte delle autorità pubbliche. Il paese di stabilimento di ciascun fornitore è indicato nella pagina Sub-responsabili.

1.5 Per impedire accessi da parte di autorità di paesi extra UE, o trasferimenti verso di esse, che sarebbero in conflitto con il diritto dell'Unione europea o di uno Stato membro, Terahold applica a tutti i dati del Servizio, personali e non personali, le seguenti misure:

a) misure tecniche: i dati del Servizio sono conservati nell'Unione europea; i dati sono cifrati in transito; le chiavi degli Strumenti Collegati sono cifrate come descritto nella Sezione 4.1; l'accesso è limitato come descritto nelle Sezioni 2 e 3;

b) misure contrattuali: se Terahold riceve da un'autorità pubblica una richiesta di accesso ai dati di un Cliente, ne informa il Cliente, salvo divieto di legge, e comunica solo i dati minimi richiesti, come previsto dal DPA; i fornitori di Terahold gestiscono tali richieste in base ai propri accordi sul trattamento dei dati;

c) misure organizzative: ogni richiesta di un'autorità pubblica è esaminata da Terahold prima di qualsiasi comunicazione.

2. Accesso al Servizio

2.1 L'accesso avviene solo su invito. Un invito è un link monouso inviato all'indirizzo email della persona invitata e valido 7 giorni.

2.2 La verifica in due passaggi è obbligatoria per il personale di Terahold e facoltativa per gli Utenti dei Clienti, che possono attivarla dalle Impostazioni; gli Utenti che non l'hanno attivata ricevono un promemoria nel Servizio. Dove la verifica in due passaggi è attivata, la applica anche la base di dati: una sessione che non l'ha completata non può leggere i dati dei Clienti.

2.3 Ogni Brand Workspace ha i propri ruoli: Owner, Manager, Editor e Analyst. Gli Analyst hanno accesso in sola lettura, anche a livello di base di dati. In forza di un Contratto Palasil Custom, il personale di Terahold entra nel Brand Workspace con il ruolo "Admin di Palasil". I dati dei diversi Clienti sono separati nella base di dati da regole di accesso, che Terahold verifica con test prima di modificarle. La base di dati accetta un record solo se gli oggetti a cui si riferisce appartengono allo stesso Brand Workspace.

2.4 Nel pannello interno di amministrazione, gli amministratori di Terahold vedono informazioni di servizio, come stato, piano e pagamenti di ciascun Brand Workspace e l'elenco dei suoi Utenti, e non i contenuti del Brand Workspace. Il personale di Terahold con il ruolo di sviluppatore vede in quel pannello solo il registro delle attività e l'elenco degli Utenti dei Brand Workspace (nome, email, Brand Workspace, ruolo, stato della verifica in due passaggi, ultimo accesso); entra in un Brand Workspace solo tramite l'accesso di supporto descritto nella Sezione 3.2.

2.5 Le seguenti azioni richiedono all'Utente di confermare di nuovo la propria identità con il secondo fattore, o con la password se la verifica in due passaggi non è attivata, e la conferma vale 10 minuti: eliminare o archiviare un Brand Workspace, cambiare le chiavi degli Strumenti Collegati, cambiare l'Owner, togliere membri, concedere l'accesso di supporto e cambiare gli Admin di Palasil di un Brand Workspace, insieme alle corrispondenti azioni degli amministratori di Terahold, come togliere la verifica in due passaggi a un Utente, invitare o togliere amministratori, registrare pagamenti e cambiare contratti o prezzi.

2.6 Una password si può cambiare solo con la password attuale o tramite il link di recupero ricevuto via email. Dopo 10 tentativi errati di inserire la password o il codice di verifica per lo stesso indirizzo email o Utente entro 15 minuti, gli ulteriori tentativi sono bloccati per 15 minuti.

3. Accesso da parte di Terahold

3.1 Terahold non accede ai contenuti di un Brand Workspace, salvo:

a) per svolgere i servizi concordati in un Contratto Palasil Custom;

b) per gestire una richiesta di supporto, quando un Owner, un Manager o un Editor del Brand Workspace ha concesso l'accesso di supporto come descritto nella Sezione 3.2;

c) per l'accesso tecnico all'infrastruttura da parte di personale autorizzato, solo per manutenzione, sicurezza, gestione degli incidenti e risoluzione dei malfunzionamenti;

d) quando lo impone la legge.

3.2 L'accesso di supporto si concede dalle Impostazioni del Brand Workspace, nella sezione "Accessi Palasil", da parte di un Owner, un Manager o un Editor, per 3 o 7 giorni, e si può disattivare in qualsiasi momento. Il personale di Terahold non concede mai l'accesso di supporto, anche quando è membro del Brand Workspace. Finché l'accesso di supporto è attivo, il personale autorizzato di Terahold può entrare nel Brand Workspace; ogni ingresso richiede un motivo, senza il quale i dati del Brand Workspace non sono mostrati. Il registro "Accessi Palasil" del Brand Workspace registra:

a) quando l'accesso di supporto è attivato e disattivato;

b) ogni ingresso del personale di Terahold, con la persona, la data e l'ora e il motivo;

c) ogni modifica fatta dal personale di Terahold durante l'accesso di supporto, comprese quelle fatte dall'agente AI su sua richiesta, con le sole esclusioni della Sezione 6.2 del DPA;

d) ogni scaricamento dei dati con la funzione "Export all data";

e) le bozze salvate in Klaviyo, i segmenti creati in Klaviyo, le programmazioni e gli invii di campagne fatti dal personale di Terahold durante l'accesso di supporto, con la persona, la data e l'ora.

Le letture non sono registrate. Al primo ingresso del personale di Terahold, gli Owner, i Manager e gli Editor del Brand Workspace ricevono una notifica nel Servizio.

3.3 Owner, Manager ed Editor possono leggere il registro "Accessi Palasil" nelle Impostazioni. Ogni voce è conservata per 12 mesi dalla sua data, anche dopo la cancellazione del Brand Workspace; dopo la cancellazione, solo Terahold può accedervi.

3.4 In forza di un Contratto Palasil Custom, il personale di Terahold lavora nel Brand Workspace come membro riconoscibile con il ruolo "Admin di Palasil" e i suoi singoli ingressi non sono registrati nel registro "Accessi Palasil". Il registro annota, e gli Owner ricevono una notifica nel Servizio, ogni volta che un Admin di Palasil entra nel team del Brand Workspace o ne esce e ogni volta che il Brand Workspace passa dal self-service a un Contratto Palasil Custom o viceversa.

3.5 Il personale e i collaboratori di Terahold sono vincolati da obblighi scritti di riservatezza, trattano i dati solo secondo le istruzioni di Terahold e lavorano solo con account e strumenti di Terahold o dei Clienti. Il loro accesso è personale, limitato a ciò che richiedono i loro compiti e revocato al termine dell'incarico. Su richiesta, Terahold comunica al Cliente i nomi delle persone che accedono ai suoi dati.

3.6 L'accesso tecnico alla base di dati di produzione usa chiavi separate per ciascun uso e per ciascuna persona. I log della piattaforma di base di dati e di autenticazione sono copiati in un archivio di Amazon Web Services nell'Unione europea, dove non possono essere modificati e sono conservati per 12 mesi. Le registrazioni delle azioni del personale di Terahold nel Servizio sono conservate per 12 mesi.

3.7 Quando il supporto di Terahold toglie la verifica in due passaggi a un Utente, l'Utente riceve una notifica nel Servizio.

4. Protezione dei dati e dei segreti

4.1 Le chiavi che collegano Palasil agli account Klaviyo e Shopify del Cliente sono cifrate con AES-256-GCM e possono essere lette solo da componenti lato server.

4.2 I dati sono cifrati in transito: il Servizio è accessibile solo tramite connessioni cifrate (HTTPS). La base di dati e l'archiviazione dei file sono cifrate a riposo da Supabase. Il server applicativo dell'agente AI è accessibile solo al personale autorizzato e conserva il log di esecuzione dell'agente per 14 giorni.

4.3 I file dei Brand Workspace sono conservati in un archivio privato, accessibile solo tramite il Servizio ai membri del Brand Workspace e al personale di Terahold nei casi della Sezione 3.1. I cookie che memorizzano il Brand Workspace selezionato e quelli usati per la conferma dell'identità e per il recupero della password sono httpOnly. Ogni componente automatico del Servizio usa un proprio segreto.

4.4 Gli strumenti dell'agente AI sono limitati a un elenco chiuso e il suo accesso ai file sul server applicativo è confinato alla sua cartella di lavoro. Il collegamento verso i modelli linguistici accetta solo richieste fatte con la chiave dell'agente. L'uso dell'agente AI è limitato per ciascun Utente e per ciascun Brand Workspace.

4.5 Il Servizio scarica le immagini delle newsletter del feed di ispirazione solo da indirizzi internet pubblici.

5. Trattamento con AI

5.1 Le richieste ai modelli linguistici sono inviate tramite OpenRouter, Inc. Palasil chiede la conservazione zero in ogni richiesta, e la stessa condizione e il divieto di addestramento sono impostati nell'account di Terahold. Sono esclusi i fornitori stabiliti nella Repubblica Popolare Cinese e le reti di calcolo decentralizzate. Le immagini non sono inviate ai modelli. I dati di lavoro dell'agente sono cancellati dopo 90 giorni.

5.2 Palasil crea bozze nell'account Klaviyo del Cliente, crea i segmenti proposti dall'agente AI e programma o invia una campagna solo su azione esplicita di un Utente il cui ruolo lo consente o del personale di Terahold durante l'accesso di supporto (Sezione 3.2) o con il ruolo di Admin di Palasil (Sezione 3.4); ogni bozza salvata in Klaviyo è registrata con la persona che l'ha salvata. Un segmento proposto dall'agente AI è creato esattamente come proposto, dopo la conferma nella chat, registrata con la persona e l'orario; Palasil non modifica né elimina segmenti nell'account Klaviyo del Cliente. Una campagna è inviata senza una data e un'ora programmate solo dopo un'ulteriore conferma di chi lo chiede, e parte 3 minuti dopo tale conferma; l'agente AI non può programmare né inviare campagne. L'agente AI chiede conferma all'Utente prima di eliminare contenuti o togliere una bozza dall'account Klaviyo del Cliente e inserisce link solo al sito del Cliente, salvo che l'Utente indichi un indirizzo diverso.

6. Disponibilità

6.1 La base di dati è sottoposta a copia di sicurezza giornaliera e le copie sono conservate per 7 giorni.

7. Incidenti e vulnerabilità

7.1 Terahold comunica ai Clienti le violazioni dei dati personali che riguardano i loro dati senza ingiustificato ritardo e comunque entro 48 ore da quando ne viene a conoscenza, come previsto dalla Sezione 13.1 del DPA.

7.2 Chi trova una vulnerabilità di sicurezza in Palasil può segnalarla a security@palasil.com. Terahold chiede a chi segnala di non accedere a dati che non gli appartengono e di non modificarli, di non interrompere il Servizio e di non divulgare la vulnerabilità prima che Terahold abbia confermato che è stata corretta. Le segnalazioni di sicurezza sono gestite prima delle altre richieste di supporto.

8. Modifiche

8.1 Terahold aggiorna questa pagina quando cambiano le sue misure di sicurezza. La versione vigente è disponibile su palasil.com/legal/security e le versioni precedenti restano disponibili nell'archivio su palasil.com/legal/archive.