LetsBe Biz — Privacy Policy

Draft — Requires Legal Review Before Publication

Version: v1.0
Date: February 26, 2026
Company: LetsBe Solutions LLC
Contact: matt@letsbe.solutions

221 North Broad Street, Suite 3A, Middletown, DE 19709

Contents

1. LetsBe Biz — Privacy Policy

Version: 1.0 **Date:** February 26, 2026 **Authors:** Matt (Founder), Claude (Drafting) **Status:** Draft — Requires Legal Review Before Publication **Companion docs:** Terms of Service v1.0, Security & GDPR Framework v1.1, Data Processing Agreement (forthcoming)

> **Important:** This document is a comprehensive draft intended to serve as the public-facing privacy policy for the LetsBe Biz platform. It must be reviewed by qualified legal counsel (EU and US) before publication. It is not legal advice.

1.1 1. Who We Are

LetsBe Solutions LLC ("LetsBe," "we," "us," "our") operates the LetsBe Biz platform — a managed service that provides small and medium-sized businesses with a dedicated virtual private server (VPS) running open-source business tools, powered by AI agents.

Contact for privacy inquiries: - Email: privacy@letsbe.solutions - Postal address: 221 North Broad Street, Suite 3A, Middletown, DE 19709, USA

Data Protection Officer: Matt Ciaccio (Founder), serving as interim DPO. Contact: privacy@letsbe.solutions. Formal DPO appointment will be assessed at approximately 100 customers per GDPR Art. 37 requirements.

EU Representative (Art. 27): To be appointed before serving EU customers, as required for non-EU established entities offering services to EU residents. Contact details will be published here once appointed. In the interim, privacy inquiries from EU residents may be directed to privacy@letsbe.solutions.

1.2 2. Scope of This Policy

This Privacy Policy applies to:

- The **LetsBe Biz website** (letsbe.solutions and related domains)
- The **Hub** (our centralized platform for account management, billing, and monitoring)
- The **LetsBe Biz service** (your dedicated VPS, the AI agents that operate on it, and all associated tools)
- **Marketing and sales communications** (emails, newsletters, contact forms)

This policy does **not** cover the personal data you or your end users store inside the business tools on your VPS (e.g., CRM contacts, client emails, invoices). For that data, you are the data controller, and LetsBe acts as your data processor under the terms of

the Data Processing Agreement (DPA). The DPA governs how we handle your business data and is available in your account dashboard.

1.3 3. Our Role Under Data Protection Law

LetsBe plays two distinct roles depending on the type of data:

Data Controller — for data we collect directly from you in connection with running the LetsBe platform:

- Account registration data (name, email, business name)
- Billing and payment data (processed via Stripe)
- Website usage data (cookies, analytics)
- Support and communication records
- Aggregated telemetry (token usage, error rates — no PII)

Data Processor — for business data stored on your VPS:

- CRM records, emails, files, calendar events, invoices, AI conversation transcripts, and all other data in your tools
- For this data, you (the customer) are the controller, and our processing is governed by the DPA

This Privacy Policy primarily describes our activities as a data controller. For our processing activities as a data processor, please refer to the DPA.

1.4 4. What Data We Collect

1.4.1 4.1 Data You Provide Directly

Data	When Collected	Purpose
Name and email address	Account registration	Account creation, authentication, communications
Business name, industry, team size	Onboarding wizard	Service customization, tool recommendations
Billing address	Subscription checkout	Tax calculation, invoicing, legal compliance

Data	When Collected	Purpose
Payment method	Subscription checkout	Recurring billing (processed by Stripe — we do not store card numbers)
Data center region preference	Onboarding	VPS provisioning in your chosen region (EU or NA)
Support messages	When you contact us	Providing assistance, improving the service
Feedback and survey responses	When you participate	Product improvement

1.4.2 4.2 Data We Collect Automatically

Data	How Collected	Purpose
IP address	Web server logs	Security, abuse prevention, approximate geolocation for compliance
Browser type and operating system	HTTP headers	Website compatibility, analytics
Pages visited and time spent	Website analytics (cookie-based, consent required)	Understanding usage patterns, improving the website
Referral source	HTTP referrer header	Understanding how visitors find us
Token usage metrics	Hub telemetry	Billing accuracy, service optimization
Error rates and uptime data	Hub monitoring	Service reliability, incident detection
Agent activity counts	Hub telemetry (aggregated, no PII)	Capacity planning, product improvement

1.4.3 4.3 Data from Third Parties

Source	Data	Purpose
Stripe	Payment confirmation, subscription status	Billing management

Source	Data	Purpose
Poste Pro (self-hosted)	Delivery receipts, bounce notifications	Ensuring communications reach you. Self-hosted on LetsBe infrastructure; no third-party data sharing for email delivery.

1.4.4 4.4 Data We Do Not Collect

We want to be clear about what we do **not** collect or have access to in our role as controller:

- **Your business tool data** — CRM contacts, client emails, files, invoices, and other data inside your VPS tools. This data stays on your VPS and is controlled by you. We access it only as a processor under the DPA.
- **Raw AI conversation content** — AI session transcripts are stored on your VPS, not on the Hub. We do not read or analyze your AI conversations.
- **Credentials and secrets** — Passwords, API keys, and OAuth tokens generated for your tools are stored encrypted on your VPS. They are never transmitted to the Hub or to AI providers.

1.5 5. How We Use Your Data

1.5.1 5.1 Legal Bases for Processing (GDPR Art. 6)

Processing Activity	Legal Basis	Explanation
Account creation and management	**Contract performance** (Art. 6(1)(b))	Necessary to deliver the LetsBe Biz service you subscribed to
Payment processing via Stripe	**Contract performance** (Art. 6(1)(b))	Necessary for billing your subscription
Server provisioning and maintenance	**Contract performance** (Art. 6(1)(b))	Core service delivery
Sending transactional emails (invoices, password resets, service notifications)	**Contract performance** (Art. 6(1)(b))	Necessary for operating your account
Token usage metering and billing	**Contract performance** (Art. 6(1)(b)) + **Legitimate interest** (Art. 6(1)(f))	Billing accuracy and abuse prevention

Processing Activity	Legal Basis	Explanation
Error and performance monitoring	**Legitimate interest** (Art. 6(1)(f))	Service reliability and incident response. Our interest: maintaining platform stability. Balanced against: data is aggregated and contains no PII.
Website analytics (cookie-based)	**Consent** (Art. 6(1)(a))	Understanding how visitors use our website. Collected only with your explicit consent via cookie banner.
Marketing emails and newsletters	**Consent** (Art. 6(1)(a))	Keeping you informed about product updates, tips, and offers. Opt-in only. You can unsubscribe at any time.
Fraud prevention and security	**Legitimate interest** (Art. 6(1)(f))	Protecting our platform and customers from abuse. Our interest: security. Balanced against: limited data used (IP address, access patterns).
Compliance with legal obligations	**Legal obligation** (Art. 6(1)(c))	Tax records (HGB §257), responding to lawful authority requests

1.5.2 5.2 What We Do NOT Do With Your Data

- **We do not sell your personal data.** Ever. To anyone. For any reason.
- **We do not share your data with advertisers** or data brokers.
- **We do not use your data for profiling** or targeted advertising.
- **We do not train AI models on your data.** We use API-tier access to LLM providers with contractual prohibitions on training. Your business data never enters any AI training pipeline.
- **We do not monetize your data** in any way beyond providing the service you pay for.

1.6 6. AI and Your Privacy

LetsBe Biz uses AI agents powered by third-party large language models (LLMs) to operate business tools on your behalf. This section explains the data flows involved

and the protections we implement.

1.6.1 6.1 How AI Data Flows Work

When an AI agent performs a task on your VPS (e.g., drafting an email, updating a CRM record, generating a report), the following occurs:

1. **On your VPS (local):** The agent reads data from your tools and writes results back. This data stays on your server.
2. **Outbound to LLM provider (external):** The agent sends a prompt — containing task context and relevant tool outputs — to a third-party LLM provider for inference. **Before transmission**, the prompt passes through the Safety Wrapper (see §6.2).
3. **Response from LLM provider:** The model's response is returned to your VPS and applied to the relevant tool.

1.6.2 6.2 The Safety Wrapper — How We Protect Your Data

Before any data leaves your VPS for AI inference, the Safety Wrapper applies a four-layer redaction process:

1. **Registry match** — All 50+ provisioned credentials on your VPS are registered. Any credential value found in the prompt is replaced with a deterministic placeholder (e.g., `[REDACTED:postgres_password]`).
2. **Placeholder substitution** — Ensures all known secrets are consistently replaced.
3. **Regex safety net** — Pattern matching catches credential-like strings the registry might miss (API keys, tokens, connection strings).
4. **Heuristic detection** — Additional checks for common credential formats.

Additionally, **configurable PII scrubbing** is available. You can enable scrubbing for email addresses, phone numbers, physical addresses, financial data, and names before they are sent to AI providers. Credential scrubbing (layer 1-4) is always on and cannot be disabled.

1.6.3 6.3 LLM Providers and Training

We route AI requests through OpenRouter to the following LLM providers:

- **Anthropic** (Claude models) — US-based
- **Google** (Gemini models) — EU and US infrastructure
- **DeepSeek** (DeepSeek models) — China-based (opt-in only, maximum redaction applied)

All providers are contractually prohibited from using your data for model training. We use paid API-tier access, which uniformly comes with no-training guarantees. See our Subprocessor List (§9) for details.

1.6.4 6.4 DeepSeek — Enhanced Protections

Given the sensitivity of data transfers to China, DeepSeek models require explicit opt-in and automatically apply the maximum redaction level (mandatory PII scrubbing). The model selection UI transparently discloses the hosting jurisdiction. You can block specific providers entirely via your account settings.

1.7 7. Data Sharing and Recipients

We share your personal data only with the following categories of recipients, and only to the extent necessary for the stated purposes:

Recipient	Data Shared	Purpose	Location
Netcup GmbH	Server infrastructure data	VPS hosting	Germany/Austria (EU) or Manassas, Virginia (US) — per your region choice
Stripe	Name, email, billing address, payment method	Payment processing	EU entity for EU customers, US entity for NA customers
OpenRouter	Redacted AI prompts (transit only)	LLM API aggregation	US
Anthropic	Redacted AI prompts (transit only)	LLM inference	US
Google	Redacted AI prompts (transit only)	LLM inference	EU + US
DeepSeek	Redacted AI prompts (transit only, maximum redaction, opt-in)	LLM inference	China
Poste Pro (self-hosted)	Email address, email content	Transactional emails (system notifications, invoices, password resets) and marketing emails (with your consent)	Self-hosted on LetsBe infrastructure (no third-party transfer)

We do not share your data with any other third parties. We do not use ad networks, social media pixels, or data brokers.

Legal disclosures: We may disclose personal data if required by law, regulation, legal process, or governmental request — for example, in response to a valid court order. We will notify you of such requests to the extent legally permitted.

1.8 8. International Data Transfers

1.8.1 8.1 Your VPS Data

Your VPS is provisioned in the data center region you choose at signup:

- **EU region** (Netcup — Nuremberg, Germany / Vienna, Austria): Your business data does not leave the EU. GDPR applies natively.
- **NA region** (Netcup — Manassas, Virginia, USA): Your business data stays in the US. CCPA and applicable US state privacy laws apply.

1.8.2 8.2 Hub Data

The Hub (account management, billing, monitoring) always operates in the EU (Germany), regardless of your VPS region. Your account data is always GDPR-protected.

1.8.3 8.3 AI Inference — Cross-Border Transfers

The only data that regularly crosses borders is **redacted AI prompts** sent to LLM providers. These prompts have all credentials stripped and may have PII scrubbed (configurable). Transfer mechanisms:

Provider	Location	Transfer Mechanism
Anthropic	US	EU-US Data Privacy Framework (DPF) + Standard Contractual Clauses (SCCs)
Google	EU + US	EU-US Data Privacy Framework (DPF) + SCCs
DeepSeek	China	SCCs + supplementary measures + mandatory enhanced redaction
OpenRouter	US	EU-US Data Privacy Framework (DPF) + SCCs
Stripe	EU / US	EU-US Data Privacy Framework (DPF) + SCCs

All subprocessor DPAs include the 2021 Standard Contractual Clauses as a fallback mechanism. We verify DPF certification for US-based subprocessors.

1.9 9. Subprocessors

We maintain a current list of subprocessors who process personal data on our behalf:

Subprocessor	Purpose	Data Processed	Location	DPA Status
Netcup GmbH	VPS hosting	All tenant data (encrypted at rest)	Germany, Austria (EU); Manassas, Virginia (US)	DPA via Netcup CCP
OpenRouter	LLM API aggregation	Redacted AI prompts (transit only)	US	DPA required — DPF certified
Anthropic	LLM inference (Claude models)	Redacted AI prompts (transit only)	US	No-training API terms; DPA available
Google	LLM inference (Gemini models)	Redacted AI prompts (transit only)	EU + US	No-training API terms (paid tier); DPA available
DeepSeek	LLM inference (DeepSeek models)	Redacted AI prompts (transit only, max redaction)	China	DPA + SCCs + supplementary measures
Stripe	Payment processing	Name, email, payment method	EU / US	DPA included in Stripe Terms
Poste Pro (self-hosted)	System emails	Email address, email content	Self-hosted on LetsBe infrastructure (Hub server)	N/A — no third-party subprocessor

Changes to subprocessors: We provide at least 30 days' advance notice before adding a new subprocessor, via our subprocessor changelog page and email notification. You may object to a new subprocessor on reasonable data protection grounds within the notice period. If we cannot accommodate your objection, you may terminate your subscription without penalty.

1.10 10. Data Retention

We retain personal data only as long as necessary for the purposes described in this policy or as required by law.

Data	Retention Period	Reason
Active account data (name, email, business profile)	Duration of your subscription	Service delivery

Data	Retention Period	Reason
Billing records (invoices, payment history)	7 years after creation	German tax law (HGB §257)
Hub account record after cancellation	90 days (soft-delete + backup rotation)	Operational cleanup
Website analytics data	24 months	Website improvement
Token usage telemetry (aggregated, no PII)	24 months	Service optimization
Support tickets	24 months after resolution	Operational reference
Marketing consent records	Duration of consent + 3 years	Demonstrating lawful consent
Server access logs (IP addresses)	90 days	Security and abuse prevention

Your VPS data (all business tool data, AI conversations, credentials) is retained for the duration of your subscription. Upon cancellation, a 48-hour cooling-off period applies, followed by a 30-day data export window. After the export window, your VPS is securely wiped (disk overwrite, snapshots deleted, instance removed). See the Terms of Service §10 for full details.

1.11 11. Your Rights

1.11.1 11.1 Rights Under GDPR (EU/EEA Residents)

If you are in the EU or EEA, you have the following rights regarding the personal data we process as a controller:

Right of Access (Art. 15) — You can request a copy of the personal data we hold about you. We will respond within 30 days. Account data is also visible in your Hub customer portal at any time.

Right to Rectification (Art. 16) — You can correct inaccurate personal data. You have full administrative access to edit data in your Hub customer portal (name, email, business details) and all data in your VPS tools. If you encounter data you cannot self-edit, contact us for assistance.

Right to Erasure (Art. 17) — You can request deletion of your personal data. Account deletion triggers VPS deprovisioning after the export window. Billing records are retained for 7 years per legal obligation. We will clearly explain any data we cannot delete and the legal basis for retention.

Right to Restriction of Processing (Art. 18) — You can request that we limit how we process your data (for example, while a rectification request is being assessed). During restriction, we store the data but do not process it further.

Right to Data Portability (Art. 20) — You can request your account data in a structured, machine-readable format (JSON). Your VPS tool data is already fully portable via open-source export formats (CSV, JSON, MBOX, CalDAV, WebDAV) and direct SSH access.

Right to Object (Art. 21) — You can object to processing based on legitimate interest (Art. 6(1)(f)). We will stop processing unless we demonstrate compelling legitimate grounds. You can always object to marketing communications — one-click unsubscribe in every email.

Automated Decision-Making (Art. 22) — LetsBe's AI agents propose actions but do not make binding decisions without human oversight. Autonomy levels ensure human approval for consequential actions. No fully automated decisions affect your legal rights or similarly significant interests.

1.11.2 11.2 Rights Under CCPA/CPRA (California Residents)

If you are a California resident, you have the following additional rights:

Right to Know — You can request disclosure of the categories and specific pieces of personal information we collect, the sources, the business purposes, and the third parties with whom we share it.

Right to Delete — You can request deletion of personal information we collected from you, subject to certain exceptions (legal obligations, security, completing transactions).

Right to Opt-Out of Sale/Sharing — **LetsBe does not sell or share your personal information** as defined by the CCPA. There is nothing to opt out of. We do not engage in data sales, data brokering, cross-context behavioral advertising, or any other form of data monetization.

Right to Non-Discrimination — We will not discriminate against you for exercising your privacy rights.

Right to Correct — You can request correction of inaccurate personal information.

Right to Limit Use of Sensitive Personal Information — You can limit the use of sensitive personal information to what is necessary for providing the service. LetsBe's architecture already limits data use to service delivery by design.

1.11.3 11.3 Rights Under Canadian PIPEDA

Canadian customers have rights to access, correct, and delete personal information under PIPEDA. Our GDPR-compliant practices meet or exceed PIPEDA requirements. You can exercise these rights through the same channels described below.

1.11.4 11.4 How to Exercise Your Rights

You can exercise any of your privacy rights by:

- **Self-service:** Edit your profile, export data, or delete your account via the Hub customer portal
- **Email:** Contact us at privacy@letsbe.solutions
- **In-app:** Use the privacy settings in your account dashboard

We will respond to all rights requests within 30 days (GDPR) or 45 days (CCPA). If we need more time (up to an additional 30/45 days respectively), we will explain why and keep you informed.

We do not charge a fee for exercising your rights, except where requests are manifestly unfounded or excessive (in which case we may charge a reasonable fee or refuse the request, with explanation).

1.11.5 11.5 Right to Lodge a Complaint

You have the right to lodge a complaint with a data protection supervisory authority. For EU customers, this is typically the authority in your country of residence. The German federal authority is:

- **BfDI** (Bundesbeauftragte für den Datenschutz und die Informationsfreiheit)
- Website: https://www.bfdi.bund.de

For California residents, you may contact the California Privacy Protection Agency (CPPA) at https://cppa.ca.gov.

1.12 12. Cookies and Website Tracking

1.12.1 12.1 Our Approach

We use cookies and similar technologies on the LetsBe website. We respect your choice and follow a consent-first model. For the full details of every cookie we set, see our Cookie Policy.

1.12.2 12.2 Cookie Categories

Category	Consent Required	Examples	Purpose
Strictly necessary	No	Session cookies, CSRF tokens, authentication state	Essential for the website and Hub to function
Analytics	Yes	Self-hosted analytics (Umami or equivalent)	Understanding how visitors use the website

Category	Consent Required	Examples	Purpose
Marketing	Yes	Email campaign tracking pixels	Measuring marketing effectiveness

We do **not** use:

- Third-party advertising cookies
- Social media tracking pixels (Facebook, LinkedIn, etc.)
- Cross-site tracking cookies
- Fingerprinting technologies

1.12.3 12.3 Cookie Consent

When you first visit our website, a cookie banner will ask for your consent to non-essential cookies. You can:

- **Accept all** — enables analytics and marketing cookies
- **Reject all** — only strictly necessary cookies are set
- **Customize** — choose which categories to allow

You can change your preferences at any time via the cookie settings link in the website footer.

1.12.4 12.4 Global Privacy Control (GPC)

We honor the Global Privacy Control signal. If your browser sends a GPC signal, we treat it as an opt-out of non-essential cookies and data sharing, consistent with CCPA requirements and emerging regulatory standards.

1.12.5 12.5 “Do Not Track”

We also honor the “Do Not Track” browser signal. When detected, non-essential cookies are not set.

1.13 13. Children’s Privacy

LetsBe Biz is a business platform designed for professional use. We do not knowingly collect personal data from children under the age of 16 (or the applicable age in your jurisdiction). If you believe a child has provided us with personal data, please contact us and we will promptly delete it.

1.14 14. Security

We take the security of your personal data seriously. Our technical and organizational measures include:

- **Encryption at rest:** Full-disk encryption on all VPS instances (Netcup infrastructure)
- **Encryption in transit:** TLS 1.3 for all connections (website, Hub, VPS, LLM providers)
- **Access controls:** Keycloak SSO for tool access, role-based access for the Hub, SSH key-only authentication (port 22022, fail2ban enabled)
- **Secrets management:** AES-256-CBC encrypted secrets registry, four-layer outbound redaction
- **Network security:** UFW firewall (ports 80, 443, 22022 only), localhost-bound internal services, per-tool Docker network isolation
- **Monitoring:** Append-only audit logs, Uptime Kuma monitoring, anomaly detection
- **Physical security:** Netcup ISO 27001 certified data centers with controlled access, CCTV, redundant power, and TÜV Rheinland audited facilities

For the complete security architecture, see our Security & GDPR Framework and the published security page on our website.

1.15 15. Changes to This Policy

We may update this Privacy Policy from time to time. When we make material changes, we will:

1. Update the “Version” and “Date” at the top of this document
2. Notify you via email at least 30 days before the changes take effect
3. Post the updated policy on our website with a clear summary of what changed
4. For significant changes, display an in-app notification in the Hub

Minor changes (formatting, clarifications that do not affect your rights) may be made without advance notice but will always be reflected in the version history.

Your continued use of the Service after the effective date of an updated policy constitutes acceptance. If you do not agree to the updated policy, you may cancel your subscription before the effective date.

1.16 16. California-Specific Disclosures

This section provides additional disclosures required by the CCPA/CPRA for California residents.

1.16.1 16.1 Categories of Personal Information Collected

In the preceding 12 months, we have collected the following categories of personal information:

CCPA Category	Examples	Collected	Source
Identifiers	Name, email, IP address, account ID	Yes	Directly from you, automatically
Commercial information	Subscription plan, payment history, token usage	Yes	Directly from you, Stripe
Internet activity	Pages visited, browser type, referral source	Yes (with consent)	Automatically via website cookies
Geolocation	Approximate location from IP address	Yes	Automatically
Professional information	Business name, industry, team size	Yes	Directly from you
Sensitive personal information	Account credentials (hashed)	Yes	Directly from you

1.16.2 16.2 Business Purposes

We collect and use personal information for the business purposes described in §5 of this policy: providing and maintaining the Service, processing payments, communicating with you, website analytics (with consent), and security.

1.16.3 16.3 Sale and Sharing

We do not sell personal information. We have not sold personal information in the preceding 12 months. We do not sell the personal information of consumers under 16 years of age.

We do not share personal information for cross-context behavioral advertising as defined by the CCPA.

1.16.4 16.4 Retention

We retain personal information as described in §10 of this policy.

1.16.5 16.5 Right to Opt-Out

Because we do not sell or share personal information, no opt-out is necessary. If our practices change, we will provide a “Do Not Sell or Share My Personal Information” link

on our website.

1.17 17. EU AI Act Transparency

In accordance with the EU AI Act (Regulation 2024/1689), we disclose that the LetsBe Biz platform deploys general-purpose AI models provided by third-party companies (Anthropic, Google, DeepSeek, and others). LetsBe is a **deployer** of these AI systems, not a provider of the underlying models.

AI-generated content is labeled as such within the platform. Human oversight is available through configurable autonomy levels, the External Communications Gate (which requires approval for outbound messages), and per-agent permission settings. For more detail, see the Terms of Service §12.

1.18 18. Open Questions (Internal — Remove Before Publication)

#	Question	Status	Notes
1	Privacy email address	**Resolved**	privacy@letsbe.solutions
2	Registered address / postal address	**Resolved**	221 North Broad Street, Suite 3A, Middletown, DE 19709, USA
3	DPO appointment	**Resolved (interim)**	Matt Ciaccio serves as interim DPO. Formal appointment at ~100 customers per GDPR Art. 37.
4	EU Representative (Art. 27)	**Partially resolved**	Required before serving EU customers. Placeholder language added; appointment needed (consider services like DataRep, MCF Technology Solutions, or a local EU contact).

#	Question	Status	Notes
5	Website analytics tool	Open	Likely Umami (self-hosted, already in tool stack). Confirm before publication.
6	Email service provider	**Resolved**	Poste Pro (self-hosted on LetsBe infrastructure). Not a third-party subprocessor. If a relay service is adopted in the future, update subprocessor tables and provide 30-day notice.
7	Cookie policy as separate document?	Open	Could be a standalone page or kept as §12 of this policy. Simpler to keep integrated.
8	CCPA threshold applicability	Open	Currently below $26.6M revenue threshold, but building for compliance proactively
9	Lead supervisory authority	Open	Likely BfDI (Germany) given Hub hosting and Netcup infrastructure. Depends on corporate establishment.

1.19 19. Changelog

Version	Date	Changes
1.0	2026-02-26	Initial draft. Covers: controller/processor roles, data collection and use with GDPR legal bases, AI-specific privacy protections (Safety Wrapper, four-layer redaction, PII scrubbing, LLM provider data flows), data sharing and subprocessors, international transfers (EU-US DPF, SCCs), data retention, full rights sections (GDPR, CCPA/CPRA, PIPEDA), cookies and GPC, children's privacy, security overview, California-specific CCPA disclosures, EU AI Act transparency. Aligned with Security & GDPR Framework v1.1 and Terms of Service v1.0.

This document is a draft requiring legal review. It should not be published or relied upon as legal advice. Qualified legal counsel in both the EU and the customer's jurisdiction should review this Privacy Policy before publication.