LetsBe Biz — Data Processing Agreement

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

Confidential — For authorized recipients only

Contents

1. LetsBe Biz — Data Processing Agreement (DPA)

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, Privacy Policy v1.0, Security & GDPR Framework v1.1

> **Important:** This Data Processing Agreement is a comprehensive draft based on GDPR Article 28 requirements and LetsBe's platform architecture. It must be reviewed by qualified legal counsel before being made available to customers. It is not legal advice.

1.1 1. Parties and Background

1.1.1 1.1 Parties

This Data Processing Agreement ("DPA") is entered into between:

- **The Customer** ("Controller," "you," "your") — the individual or entity that subscribes to the LetsBe Biz service; and
- **LetsBe Solutions LLC** ("Processor," "LetsBe," "we," "us," "our") — the provider of the LetsBe Biz platform.

1.1.2 1.2 Background

This DPA forms part of the Terms of Service ("Agreement") between the Controller and the Processor and supplements the Agreement with respect to the processing of personal data.

The Controller uses the LetsBe Biz platform, which includes a dedicated virtual private server (VPS), open-source business tools, and AI agents. In providing the Service, the Processor processes personal data on behalf of the Controller. This DPA sets out the parties' obligations and rights regarding that processing.

1.1.3 1.3 Precedence

In the event of any conflict between this DPA and the Agreement, this DPA shall prevail with respect to data protection matters. In the event of any conflict between this DPA and the Standard Contractual Clauses (Annex IV), the Standard Contractual Clauses shall prevail.

1.2 2. Definitions

In this DPA:

- **“Data Protection Laws”** means all applicable legislation relating to data protection and privacy, including GDPR (Regulation (EU) 2016/679), the UK GDPR, the Swiss Federal Act on Data Protection (FADP), CCPA/CPRA, PIPEDA, and any applicable US state privacy laws, in each case as amended from time to time.
- **“GDPR”** means Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation).
- **“Personal Data”** means any information relating to an identified or identifiable natural person that the Processor processes on behalf of the Controller in connection with the Service, as further described in Annex I.
- **“Processing”** has the meaning given in GDPR Article 4(2) — any operation performed on personal data, including collection, recording, organization, storage, adaptation, retrieval, consultation, use, disclosure, restriction, erasure, or destruction.
- **“Subprocessor”** means any third party engaged by the Processor to process Personal Data on behalf of the Controller.
- **“Data Subject”** means an identified or identifiable natural person to whom the Personal Data relates.
- **“Personal Data Breach”** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data.
- **“SCCs”** means the Standard Contractual Clauses approved by European Commission Implementing Decision (EU) 2021/914, as may be amended or replaced.
- **“Hub”** means LetsBe’s centralized platform for account management, billing, and monitoring, hosted in the EU (Germany).
- **“VPS”** means the dedicated virtual private server provisioned for the Controller, running containerized business tools and AI agents.
- **“Safety Wrapper”** means the LetsBe security extension that redacts credentials and (optionally) PII from data before transmission to LLM providers.

1.3 3. Scope and Duration of Processing

1.3.1 3.1 Scope

This DPA applies to all Personal Data that the Processor processes on behalf of the Controller in the course of providing the LetsBe Biz service. The subject matter, nature, purpose, duration, types of Personal Data, and categories of Data Subjects are described in **Annex I**.

1.3.2 3.2 Duration

The Processor shall process Personal Data for the duration of the Agreement (the Controller's active subscription), plus the post-termination data retention periods described in Section 11 of this DPA.

1.4 4. Controller Obligations

The Controller:

4.1. Is responsible for ensuring that its use of the Service complies with Data Protection Laws, including having a valid legal basis for processing Personal Data.

4.2. Determines what Personal Data enters the platform, which tools are activated, what data is imported, and how AI agents are configured (including autonomy levels, data access scope, and PII scrubbing settings).

4.3. Is responsible for the lawfulness of the instructions it gives to the Processor. If the Processor reasonably believes an instruction infringes Data Protection Laws, it will notify the Controller without undue delay.

4.4. Shall ensure that Data Subjects have been informed about the processing of their Personal Data by the Processor, to the extent required by Data Protection Laws (e.g., GDPR Articles 13 and 14).

4.5. Is responsible for responding to Data Subject requests. The Processor will assist the Controller in fulfilling these requests as described in Section 8.

1.5 5. Processor Obligations

The Processor shall:

1.5.1 5.1 Processing on Instructions

Process Personal Data only on the documented instructions of the Controller, unless required to do so by EU or Member State law to which the Processor is subject — in which case, the Processor shall inform the Controller of that legal requirement before processing (unless prohibited by law from doing so).

The Controller's documented instructions include: (a) processing in accordance with the Agreement and this DPA; (b) processing initiated by the Controller through use of the Service (including AI agent configuration and tool operation); and (c) processing to comply with other reasonable instructions provided by the Controller where consistent with the terms of this DPA.

1.5.2 5.2 Confidentiality

Ensure that persons authorized to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. The Processor shall limit access to Personal Data to those employees, contractors, and agents who need access to perform their duties.

1.5.3 5.3 Security (GDPR Art. 32)

Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, as described in **Annex II**. These measures include:

- Encryption of Personal Data at rest and in transit
- The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems
- The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident
- A process for regularly testing, assessing, and evaluating the effectiveness of security measures

1.5.4 5.4 Subprocessing

Not engage any Subprocessor without the prior written authorization of the Controller, subject to the general authorization procedure described in Section 7.

1.5.5 5.5 Assistance with Data Subject Rights

Assist the Controller, by appropriate technical and organizational measures, in fulfilling the Controller’s obligation to respond to Data Subject requests, as described in Section 8.

1.5.6 5.6 Assistance with Controller Obligations

Assist the Controller in ensuring compliance with the obligations under GDPR Articles 32–36 (security, breach notification, data protection impact assessments, and prior consultation), taking into account the nature of processing and the information available to the Processor.

1.5.7 5.7 Data Return and Deletion

At the choice of the Controller, return or delete all Personal Data after the end of the provision of the Service, as described in Section 11.

1.5.8 5.8 Audit Rights

Make available to the Controller all information necessary to demonstrate compliance with this DPA and allow for and contribute to audits and inspections, as described in Section 10.

1.6 6. Details of Processing

The details of the processing activities are set out in **Annex I**, which includes:

- Subject matter and duration of the processing
- Nature and purpose of the processing
- Types of Personal Data processed
- Categories of Data Subjects
- The Controller's obligations and rights

1.7 7. Subprocessors

1.7.1 7.1 General Authorization

The Controller provides **general written authorization** for the Processor to engage Subprocessors for the purposes described in this DPA. The current list of authorized Subprocessors is set out in **Annex III**.

1.7.2 7.2 Notification of Changes

The Processor shall notify the Controller of any intended addition or replacement of a Subprocessor at least **30 days** before the new Subprocessor begins processing Personal Data. Notification will be provided via email and published on the LetsBe subprocessor changelog page.

1.7.3 7.3 Objection Right

The Controller may object to a new Subprocessor on reasonable data protection grounds within the 30-day notice period. If the Controller objects:

1. The Processor will make reasonable efforts to address the Controller's objection, including offering an alternative Subprocessor or configuration that avoids data processing by the objected-to Subprocessor.
2. If the Processor cannot reasonably accommodate the objection, the Controller may terminate the affected subscription without penalty by providing written notice within the objection period.

1.7.4 7.4 Subprocessor Obligations

The Processor shall:

- Impose data protection obligations on each Subprocessor by way of a written contract that provides at least the same level of protection as this DPA (GDPR Art. 28(4))

- Verify that each Subprocessor has appropriate technical and organizational measures in place
- Remain fully liable to the Controller for the performance of its Subprocessors' obligations

1.7.5 7.5 LLM Provider Vetting

Before authorizing a new LLM provider as a Subprocessor, the Processor verifies:

- Contractual prohibition on training models using Controller data
- Data retention limited to the inference request (or a short, documented window for abuse monitoring only)
- Valid international transfer mechanism (adequacy decision, DPF certification, or SCCs)
- Security certifications (SOC 2, ISO 27001, or equivalent)
- Commitment to notify the Processor of breaches without undue delay

---

1.8 8. Data Subject Rights

1.8.1 8.1 Assistance

The Processor shall assist the Controller in responding to requests from Data Subjects exercising their rights under Data Protection Laws, including:

- Right of access (GDPR Art. 15)
- Right to rectification (Art. 16)
- Right to erasure (Art. 17)
- Right to restriction of processing (Art. 18)
- Right to data portability (Art. 20)
- Right to object (Art. 21)
- Rights related to automated decision-making (Art. 22)

1.8.2 8.2 Implementation

The LetsBe Biz platform supports Data Subject rights as follows:

- **Access and Portability:** The Controller has full access to all data on their VPS, including SSH access. All tools support standard export formats (CSV, JSON, MBOX, CalDAV, WebDAV). AI conversation history is exportable as JSON/Markdown. Hub account data is accessible via the customer portal.
- **Rectification:** The Controller has full administrative access to edit any data in their tools and Hub account.
- **Erasure:** The Controller can delete specific data within tools. Full account deletion follows the procedure in Section 11.

- **Restriction:** The Controller can disable individual AI agents, restrict tool access, or freeze their account (stopping all AI processing).
- **Objection to AI processing:** The Controller can configure the Safety Wrapper to exclude specific data categories from AI context. Individual agents can be disabled.

1.8.3 8.3 Direct Requests

If a Data Subject contacts the Processor directly with a request, the Processor shall promptly redirect the request to the Controller (unless the request relates to the Processor's own controller activities, such as Hub account data).

1.8.4 8.4 Costs

Assistance with Data Subject requests is included in the subscription at no additional charge for a reasonable volume of requests. For requests that are manifestly unfounded, excessive, or require significant manual effort beyond what the platform provides self-service, the Processor may charge a reasonable fee based on administrative costs, with prior notice to the Controller.

1.9 9. Personal Data Breach

1.9.1 9.1 Notification to Controller

The Processor shall notify the Controller of a Personal Data Breach **without undue delay** after becoming aware of it, and in any event within **48 hours** of confirmation. The notification shall include:

- A description of the nature of the breach, including (where possible) the categories and approximate number of Data Subjects and records concerned
- The name and contact details of the Processor's data protection contact
- A description of the likely consequences of the breach
- A description of the measures taken or proposed to address the breach, including measures to mitigate its possible adverse effects

1.9.2 9.2 Notification to Supervisory Authority

The Processor shall assist the Controller in notifying the relevant supervisory authority within **72 hours** of the Controller becoming aware of the breach (GDPR Art. 33), by providing all necessary information and cooperation.

1.9.3 9.3 Notification to Data Subjects

Where the breach is likely to result in a high risk to the rights and freedoms of Data Subjects, the Processor shall assist the Controller in communicating the breach to affected Data Subjects (GDPR Art. 34).

1.9.4 9.4 Breach Response

The Processor maintains a documented breach response plan (see Security & GDPR Framework §3.7) that includes:

1. **Contain** — Isolate affected VPS, revoke compromised credentials
2. **Assess** — Determine scope, data categories affected, number of Data Subjects
3. **Notify** — Supervisory authority (72 hours), Controller (without undue delay), Data Subjects (if high risk, as directed by Controller)
4. **Remediate** — Patch vulnerability, rotate affected credentials, update security measures
5. **Document** — Full incident report with timeline, impact assessment, remediation steps
6. **Review** — Post-incident review within 14 days, update security procedures

1.9.5 9.5 Breach Detection

Breach detection mechanisms include:

- Safety Wrapper audit logs (all tool executions, credential accesses)
- Hub monitoring (tenant health, connectivity)
- Anomaly detection (mass data export, credential access spikes, unauthorized API calls)
- Uptime Kuma monitoring on each VPS
- Netcup infrastructure-level monitoring

1.10 10. Audit Rights

1.10.1 10.1 Information and Evidence

The Processor shall make available to the Controller all information reasonably necessary to demonstrate compliance with this DPA, including:

- Security & GDPR Framework documentation
- Technical and organizational measures (Annex II)
- Current subprocessor list (Annex III)
- Records of processing activities (ROPA)
- SOC 2 report (when available)
- Penetration test results (summary, when available)

1.10.2 10.2 Audits and Inspections

The Controller may conduct an audit or appoint a qualified third-party auditor (subject to reasonable confidentiality obligations) to verify the Processor’s compliance with this DPA. Audits are subject to the following conditions:

- The Controller shall provide at least **30 days' written notice** before an audit
- Audits shall be conducted during normal business hours and shall not unreasonably disrupt the Processor's operations
- The Controller is entitled to **one audit per 12-month period** (additional audits may be requested in the event of a breach or regulatory investigation)
- The Controller bears the cost of audits, unless the audit reveals material non-compliance, in which case the Processor bears the cost
- The Processor may offer an equivalent assessment (SOC 2 report, third-party certification) in lieu of an on-site audit, provided it is reasonably sufficient to verify compliance

1.10.3 10.3 Cooperation

The Processor shall cooperate with the Controller and any supervisory authority in the performance of audits or investigations, to the extent required by Data Protection Laws.

1.11 11. Data Return and Deletion

1.11.1 11.1 During the Subscription

The Controller can export all Personal Data at any time during the subscription period, using:

- Tool-native export functions (CRM export, file download, email export, calendar export)
- Direct SSH access to the VPS
- Hub customer portal (for account data)

All tools on the VPS are open-source with standard export formats, ensuring full data portability consistent with the EU Data Act.

1.11.2 11.2 Upon Termination

Upon termination or expiration of the Agreement:

1. **48-hour cooling-off period:** After the billing period ends, the Controller's account is marked for deletion and a confirmation email is sent. The Controller has 48 hours to reverse the cancellation.
2. **30-day export window:** After the cooling-off period, the Controller has 30 days to export all data from the VPS. During this period, the VPS remains accessible (tools may be in read-only mode).
3. **Secure deletion:** After the 30-day export window, the Processor securely deprovisions the VPS: disk overwrite via hosting provider API, VPS instance deletion, all snapshots deleted.

4. **Hub data:** Account record is soft-deleted. Billing records are retained for 7 years per German tax law (HGB §257). All other data is purged. Soft-deleted records are hard-deleted after backup rotation (90 days).

1.11.3 11.3 Certification of Deletion

Upon request, the Processor shall provide written confirmation that Personal Data has been deleted in accordance with this Section, except for data retained under legal obligations (which will be specified in the confirmation).

1.12 12. International Data Transfers

1.12.1 12.1 Controller's VPS Region

The Controller selects a data center region at signup:

- **EU region:** Netcup data centers in Nuremberg, Germany / Vienna, Austria. Personal Data does not leave the EU.
- **NA region:** Netcup data center in Manassas, Virginia, USA. Personal Data is stored in the US.

1.12.2 12.2 Hub Data

The Hub always operates in the EU (Germany), regardless of the Controller's VPS region. Account and billing data is processed within the EU.

1.12.3 12.3 LLM Inference Transfers

Redacted AI prompts are transferred to third-party LLM providers for inference. Before transfer, the Safety Wrapper strips all credentials and (if enabled) PII. Transfer mechanisms:

Provider	Location	Transfer Mechanism
Anthropic	US	EU-US Data Privacy Framework + SCCs
Google	EU + US	EU-US Data Privacy Framework + SCCs
DeepSeek	China	SCCs + supplementary measures + mandatory enhanced redaction
OpenRouter	US	EU-US Data Privacy Framework + SCCs

1.12.4 12.4 Standard Contractual Clauses

Where Personal Data is transferred from the EU/EEA to a country without an adequacy decision, the parties agree to the Standard Contractual Clauses (2021 version) as set out in **Annex IV**. The SCCs are incorporated into this DPA by reference.

For transfers where the Controller is established in the EU/EEA and the Processor processes data outside the EU/EEA:

- **Module Two** (Controller to Processor) of the SCCs applies
- The governing law is that of the EU Member State where the Controller is established, or Germany if the Controller is not established in the EU/EEA
- Disputes shall be resolved before the courts of the same jurisdiction

1.12.5 12.5 Supplementary Measures

For transfers to jurisdictions where the legal framework may not provide equivalent protection (e.g., China for DeepSeek), the Processor implements supplementary technical measures:

- Mandatory maximum PII scrubbing before transmission
- Credential redaction (always on, non-bypassable)
- Customer opt-in required (not enabled by default)
- Transparent disclosure of hosting jurisdiction in the UI
- Ability for the Controller to block specific providers entirely

---

1.13 13. Data Protection Impact Assessment

The Processor shall provide reasonable assistance to the Controller in conducting Data Protection Impact Assessments (DPIAs) required under GDPR Article 35, and in any subsequent consultations with supervisory authorities under Article 36, to the extent that the Controller does not otherwise have the information and the assistance is required due to the nature of the processing.

1.14 14. Liability

The liability of each party under this DPA is subject to the limitations and exclusions of liability set out in the Agreement (Terms of Service §8), except that:

- The limitations of liability do not apply to either party's obligations under this DPA with respect to Personal Data Breaches (Section 9)
- Each party is liable for damages caused by processing that infringes Data Protection Laws, to the extent required by those laws (GDPR Art. 82)

1.15 15. Term and Termination

1.15.1 15.1 Term

This DPA takes effect on the date the Controller accepts the Agreement and remains in effect for as long as the Processor processes Personal Data on behalf of the Controller.

1.15.2 15.2 Survival

Sections 9 (Breach Notification), 10 (Audit Rights), 11 (Data Return and Deletion), 12 (International Transfers), and 14 (Liability) survive termination of this DPA to the extent necessary.

1.16 16. Miscellaneous

1.16.1 16.1 Amendments

This DPA may be amended by the Processor with at least 30 days' written notice to the Controller. If the Controller does not object within the notice period, the amendments are deemed accepted. If the Controller objects, the existing DPA remains in force, and the Controller may terminate the Agreement if the amendments are material and the parties cannot reach agreement.

1.16.2 16.2 Governing Law

This DPA is governed by the law that governs the Agreement, except that the SCCs (Annex IV) are governed as specified therein.

1.16.3 16.3 Entire DPA

This DPA (including its Annexes) constitutes the complete agreement between the parties regarding data processing and supersedes all prior agreements on this subject.

1.17 Annex I — Details of Processing

1.17.1 A. List of Parties

Controller (Data Exporter): - Name: [Customer name — populated at signup] - Address: [Customer address — populated at signup] - Contact: [Customer email — populated at signup] - Role: Data controller for all personal data stored in their LetsBe Biz VPS tools

Processor (Data Importer): - Name: LetsBe Solutions LLC - Address: 221 North Broad Street, Suite 3A, Middletown, DE 19709, USA - Contact: privacy@letsbe.solutions - Role: Data processor providing managed VPS, tool deployment, and AI agent services

1.17.2 B. Description of Processing

Element	Description
Subject matter	Processing of personal data through AI-powered management of open-source business tools deployed on a dedicated VPS
Duration	For the duration of the Controller’s subscription, plus post-termination retention periods (Section 11)
Nature of processing	Storage, retrieval, organization, structuring, consultation, use (including AI-assisted analysis and automation), disclosure by transmission (redacted prompts to LLM providers), restriction, erasure
Purpose of processing	To provide the LetsBe Biz service: hosting and managing business tools on the Controller’s VPS, enabling AI agents to operate those tools on the Controller’s behalf, maintaining platform security, and facilitating data portability

1.17.3 C. Types of Personal Data

The specific types of personal data processed depend on the Controller’s tool selection and use. They may include:

- **Contact data:** Names, email addresses, phone numbers, postal addresses, job titles, company names
- **Communication data:** Email content (subject, body, attachments), chat messages, calendar event details
- **Financial data:** Invoice details, payment amounts, client billing records, expense data
- **Project data:** Task descriptions, project notes, team assignments, comments, time tracking entries
- **File data:** Documents, images, spreadsheets, and other files uploaded to file storage tools
- **Website analytics data:** Visitor IP addresses, page views, referral sources (if website analytics tools are used)
- **AI interaction data:** Conversation transcripts between the Controller’s users and AI agents, agent action logs
- **Authentication data:** Usernames and hashed passwords for tool access (managed via Keycloak SSO)

1.17.4 D. Categories of Data Subjects

The categories of Data Subjects depend on the Controller’s use of the platform and may include:

- The Controller’s employees and team members
- The Controller’s clients and customers
- The Controller’s business contacts, leads, and prospects
- Website visitors (if analytics tools are used)
- Email correspondents
- Any other individuals whose data the Controller imports into or creates within the platform tools

1.17.5 E. Special Categories of Data

The Service is not designed to process special categories of data (GDPR Art. 9) or criminal conviction data (Art. 10). If the Controller stores such data in their tools, the Controller is solely responsible for ensuring a valid legal basis and appropriate safeguards.

1.17.6 F. Frequency and Retention

- **Frequency:** Processing is continuous for the duration of the subscription (tools and AI agents operate on an ongoing basis)
- **Retention:** Personal data is retained on the Controller’s VPS for the duration of the subscription. Upon termination, the data retention schedule in Section 11 applies.

1.18 Annex II — Technical and Organizational Measures (TOMs)

The Processor implements the following measures pursuant to GDPR Article 32. These measures apply to all Personal Data processed under this DPA.

1.18.1 1. Encryption

Scope	Measure
Data at rest (VPS disk)	Netcup full-disk encryption (provider-managed)
Secrets registry	AES-256-CBC with scrypt key derivation; key stored on VPS filesystem, never in AI context
Data in transit (user ↔ Hub)	TLS 1.3 (HTTPS); Let’s Encrypt certificates, auto-renewed
Data in transit (user ↔ VPS)	TLS 1.3 via nginx reverse proxy; Let’s Encrypt certificates, auto-renewed
Data in transit (Safety Wrapper ↔ LLM)	TLS 1.3 (HTTPS via OpenRouter)
Backups (Netcup snapshots)	Provider-encrypted snapshots

Scope	Measure
SSH access	ED25519 keys, port 22022; key-only authentication, no password login

1.18.2 2. Access Control

Scope	Measure
Customer access to VPS tools	Keycloak SSO — single sign-on across all deployed tools
Customer access to Hub	Email + password, session-based authentication
Admin access to Hub	Role-based access control (Prisma + middleware)
SSH access to VPS	Key-only authentication, non-standard port (22022), fail2ban (5 attempts → 300s ban)
AI agent access to tools	Per-agent tool allow/deny lists (OpenClaw configuration)
AI agent operational scope	Three-tier autonomy levels with command gating (Safety Wrapper)
Inter-tenant isolation	Separate VPS per customer — no shared infrastructure beyond the Hub
Tool container isolation	Per-tool Docker networks with fixed subnets (172.20.X.0/28)

1.18.3 3. Secrets Management and AI Data Protection

Scope	Measure
Credential generation	50+ unique credentials per tenant generated at provisioning
Credential storage	Encrypted SQLite registry on VPS — never transmitted to LLM providers
Outbound redaction	Four-layer redaction of all LLM-bound data: (1) registry match, (2) placeholder substitution, (3) regex safety net, (4) heuristic detection
Transcript redaction	Hooks strip secrets from stored session transcripts before persistence
Side-channel credential exchange	User-provided secrets exchanged via direct Safety Wrapper API, never entering AI conversation
Configurable PII scrubbing	Optional scrubbing of email addresses, phone numbers, addresses, financial data, and names before LLM transmission

Scope	Measure
External Communications Gate	All AI-initiated outbound external communications require human approval

1.18.4 4. Network Security

Scope	Measure
Firewall	UFW — only ports 80, 443, 22022 open
OpenClaw binding	Localhost only — not accessible from outside VPS
Safety Wrapper binding	Localhost only — only OpenClaw and Hub (via nginx) can reach it
Container networking	Per-tool isolated Docker networks (172.20.X.0/28), exposed via 127.0.0.1:30XX
SSRF protection	Browser tool has configurable domain allowlists
Rate limiting	OpenClaw: 10 attempts/60s with 300s lockout; Hub API rate-limited
DDoS protection	Netcup infrastructure-level protection + nginx rate limiting

1.18.5 5. Monitoring and Audit

Scope	Measure
Audit log	Append-only log of all AI agent actions on tenant VPS
Token metering	Per-agent, per-model token counts reported to Hub
Backup monitoring	Automated backup status monitoring with alerting
Uptime monitoring	Uptime Kuma on each VPS + Hub-level health checks
Hub telemetry	Aggregated metrics (no PII) — uptime, error rates, usage patterns

1.18.6 6. Physical Security

Delegated to hosting provider (Netcup GmbH):

- ISO 27001 certified data centers in Germany, Austria, and Manassas, Virginia (US)
- TÜV Rheinland annual security audits
- Controlled physical access, CCTV, security personnel

- Redundant power supply, climate control, fire suppression
- Multiple redundant network connections

1.18.7 7. Organizational Measures

Scope	Measure
Confidentiality	All personnel with access to Personal Data are bound by confidentiality obligations
Incident response	Documented breach response plan with detection, containment, notification, remediation, review phases
Vendor assessment	All Subprocessors vetted for data protection compliance with DPAs in place
Privacy by design	Architecture decisions (isolated VPS, secrets redaction, local storage) embedded from inception
Data minimization	Hub stores only account management data; all business data remains on tenant VPS

1.19 Annex III — Authorized Subprocessors

The following Subprocessors are authorized as of the date of this DPA:

Subprocessor	Purpose	Data Processed	Location	DPA Status
Netcup GmbH	VPS hosting	All tenant data (encrypted at rest)	Germany, Austria (EU region); Manassas, Virginia (NA region)	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

Subprocessor	Purpose	Data Processed	Location	DPA Status
DeepSeek	LLM inference (DeepSeek models)	Redacted AI prompts (transit only, max redaction, opt-in only)	China	DPA + SCCs + supplementary measures
Stripe	Payment processing	Customer name, email, payment method	EU (for EU customers), US (for NA customers)	DPA included in Stripe Terms
Poste Pro (self-hosted)	System emails from Hub	Customer email address, email content	Self-hosted on LetsBe infrastructure (Hub server)	N/A — no third-party subprocessor. If a third-party relay service is adopted in the future, it will be added here with 30 days' advance notice per §9.

Subprocessor changelog: Changes to this list are published at https://letsbe.biz/legal/subproce and notified to the Controller via email at least 30 days in advance.

1.20 Annex IV — Standard Contractual Clauses (SCCs)

The parties agree that, for international data transfers subject to GDPR where the receiving country does not have an adequacy decision, the Standard Contractual Clauses adopted by European Commission Implementing Decision (EU) 2021/914 of June 4, 2021 shall apply.

Module Two (Controller to Processor) applies to transfers from the Controller to the Processor (or its Subprocessors) where the Processor processes data outside the EU/EEA.

The SCCs are incorporated into this DPA by reference. The completed SCC annexes correspond to the Annexes of this DPA:

SCC Annex	DPA Annex
Annex I (Details of transfer)	This DPA, Annex I
Annex II (Technical and organizational measures)	This DPA, Annex II
Annex III (List of subprocessors)	This DPA, Annex III

SCC-specific selections:

- **Clause 7 (Docking clause):** Included — additional parties may accede to the SCCs
- **Clause 9(a) (Subprocessor authorization):** Option 2 — General written authorization (with 30-day notice)
- **Clause 11 (Redress):** The optional clause on independent dispute resolution is not included
- **Clause 13 (Supervision):** The competent supervisory authority is determined by the Controller's establishment. For Controllers established in Germany, the BfDI (Bundesbeauftragte für den Datenschutz und die Informationsfreiheit) applies. For Controllers established in other EU member states, the supervisory authority of their establishment applies. Where the Controller is not established in the EU, the German supervisory authority (BfDI) applies as the Processor's Hub infrastructure is located in Germany.
- **Clause 17 (Governing law):** Option 1 — the law of the State of Delaware, USA (consistent with the Agreement/ToS). For EU data subjects, the mandatory provisions of GDPR and applicable member state law continue to apply.
- **Clause 18 (Choice of forum):** The courts of Delaware, USA (consistent with the Agreement/ToS). EU data subjects retain their right to lodge complaints with their local supervisory authority.

  Note for legal counsel: The full text of the SCCs should be appended to this DPA as a separate document. The 2021 SCCs are available from the European Commission. This Annex documents the module selection and variable choices; the full SCC text is not reproduced here but is incorporated by reference.

1.21 17. Open Questions (Internal — Remove Before Publication)

#	Question	Status	Notes
1	LetsBe registered address	**Resolved**	221 North Broad Street, Suite 3A, Middletown, DE 19709, USA
2	Privacy/DPO contact email	**Resolved**	privacy@letsbe.solutions
3	Lead supervisory authority	**Resolved**	Determined by Controller's establishment; default BfDI (Germany) given Hub location. See SCC Clause 13 selections.

#	Question	Status	Notes
4	Governing law and forum selection	**Resolved**	Delaware, USA (matches ToS). EU data subjects retain GDPR rights.
5	Full SCC text appendix	Open	2021 SCCs should be appended as a separate document; consider providing as a downloadable PDF alongside this DPA
6	Email service provider	**Resolved**	Poste Pro (self-hosted). Not a third-party subprocessor — no Annex III entry needed. If a relay service is adopted, add to Annex III with 30-day notice per §9.
7	Subprocessor changelog URL	Open	Needs a page on the website before launch
8	Enterprise DPA negotiation process	Open	Standard DPA is self-service via dashboard; enterprise customers may request custom terms. Define process and contact.
9	UK Addendum	Open	If serving UK customers post-Brexit, an International Data Transfer Addendum (UK IDTA) may be needed alongside or instead of SCCs

---

1.22 18. Changelog

Version	Date	Changes
1.0	2026-02-26	Initial draft. Full GDPR Art. 28 DPA with four annexes: processing details (Annex I), TOMs (Annex II), subprocessor list (Annex III), SCC framework (Annex IV). Covers: processor obligations, subprocessor management with 30-day notice, data subject rights assistance, breach notification (48h to controller, 72h to authority), audit rights, data return/deletion with 48h cooling-off + 30-day export window, international transfers, DPIA assistance. Aligned with Security & GDPR Framework v1.1, Terms of Service v1.0, and Privacy Policy v1.0.

This document is a draft requiring legal review. The Standard Contractual Clauses referenced in Annex IV should be appended in full before this DPA is made available to customers. Qualified legal counsel should review this DPA before publication.