

Data Processing Agreement

GDPR Article 28 Data Processing Agreement for customers of PrepBusiness, operated by Jasara Technology Inc.

Version 1.0 · Last updated July 20, 2026

This Data Processing Agreement ("DPA") governs how Jasara Technology Inc. processes personal data on behalf of customers of the PrepBusiness platform, and reflects our commitments as a data processor under Regulation (EU) 2016/679 ("GDPR"). It supplements the service agreement between the Customer and Jasara Technology Inc. for use of PrepBusiness (the "Service Agreement").

Parties

- **Processor:** Jasara Technology Inc. (operating as PrepBusiness / TradeLink), incorporated in Canada. Data protection contact: keith@jasaratech.com. Data subject request contact: support@jasaratech.com.
- **Controller:** the Customer identified in the signature block below, acting as controller (or as processor on behalf of its own customers).

1. Definitions

Terms not defined here carry the meaning given in the GDPR, including "personal data", "processing", "controller", "processor", "data subject", and "personal data breach". "Subprocessor" means any third party engaged by the Processor to process personal data on behalf of the Controller.

2. Roles and Scope

In respect of personal data processed under the Service Agreement, the Customer acts as controller and Jasara Technology Inc. acts as processor. The Processor processes personal data only for the purpose of providing the Service and only in accordance with this DPA and the Service Agreement. The details of the processing are set out in Annex I.

3. Processor Obligations (Article 28(3))

The Processor shall:

- **(a) Documented instructions.** Process personal data only on the Customer's documented instructions, including as to international transfers, unless required otherwise by law. The Service Agreement and this DPA are the Customer's complete documented instructions.
- **(b) Confidentiality.** Ensure that persons authorized to process the personal data are bound by an appropriate obligation of confidentiality and access it on a need-to-know basis.
- **(c) Security.** Implement the technical and organizational measures set out in Annex II, in accordance with Article 32 GDPR.
- **(d) Subprocessors.** Engage subprocessors only in accordance with Section 4 and Annex III.
- **(e) Data subject rights.** Assist the Customer by appropriate measures, insofar as possible, in responding to data subject requests under Chapter III GDPR, and forward any request received directly from a data subject without undue delay.
- **(f) Assistance with compliance.** Assist the Customer in ensuring compliance with Articles 32 to 36 GDPR, taking into account the nature of processing and the information available to the Processor.
- **(g) Deletion or return.** At the Customer's choice, delete or return all personal data after the end of the provision of services, and delete existing copies unless storage is required by law. Certification of destruction is available on request.
- **(h) Audits and information.** Make available the information necessary to demonstrate compliance with Article 28 GDPR, and allow for and contribute to audits, subject to reasonable notice and confidentiality. Existing third-party audit reports may be provided where they reasonably address the request.

4. Subprocessors

The Customer grants the Processor general authorization to engage the subprocessors listed in Annex III. The Processor will inform the Customer of any intended addition or replacement of a subprocessor, giving the Customer 30 days to object on reasonable data-protection grounds. The Processor imposes on each subprocessor data protection obligations no less protective than those in this DPA, and remains fully liable for each subprocessor's performance.

5. International Transfers

Personal data processed and stored at rest under this DPA is located within the EU/EEA (Germany and France), as set out in Annex III. The Processor is established in Canada, which benefits from a European Commission adequacy decision.

Where a subprocessor processes personal data outside the EU/EEA, such transfers are made under an appropriate Chapter V GDPR safeguard: the EU Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914), together with any necessary supplementary measures, and, where the recipient is actively self-certified, the EU-US Data Privacy Framework. Where the processing is subject to the UK GDPR, the UK International Data Transfer Addendum applies to any restricted transfer.

6. Personal Data Breach

The Processor will notify the Customer without undue delay after becoming aware of a personal data breach affecting the Customer's personal data, and will provide the information reasonably required for the Customer to meet its obligations under Articles 33 and 34 GDPR. Security incidents are handled in accordance with the Processor's Security Incident Response Plan.

7. Government and Law Enforcement Requests

If the Processor receives a legally binding request from a public authority to disclose personal data processed under this DPA, it will, unless legally prohibited, notify the Customer without undue delay and provide reasonable cooperation to enable the Customer to seek a protective order or other remedy. The Processor assesses the legality of each request, challenges requests that appear unlawful or overbroad, and discloses only the minimum personal data necessary.

8. Duration, Liability, and Governing Law

This DPA remains in force for as long as the Processor processes personal data on behalf of the Customer under the Service Agreement. Each party's liability is subject to the limitations set out in the Service Agreement, which also specifies the governing law. In the event of a conflict regarding the processing of personal data, this DPA prevails.

9. Execution

This DPA is pre-signed by the Processor below. To enter into it, the Customer completes and signs the Customer signature block and emails the signed DPA to the Processor at support@jasaratech.com. The DPA becomes valid once the Processor receives it. The Processor does not countersign or return a separate copy.

Processor — Jasara Technology Inc.

Keith Brink

Signature

Keith Brink - Founder & CEO

Name and title

-

Date

Customer

Signature

Company / name and title

Date

Annex I — Description of the Processing

Categories of data subjects

The Customer's end customers (buyers of orders fulfilled through the platform, including Amazon, eBay, and direct/FBM orders) and the Customer's own personnel who hold user accounts on the platform.

Categories of personal data

Recipient / buyer name, shipping address, email address, phone number, order identifiers and order contents, and platform account holder name and email address.

Special categories of personal data

None. The Service is not intended to process special-category data under Article 9 GDPR.

Nature and purpose

Provision of warehouse management, prep, and fulfillment software, including order fulfillment, inventory management, product listing management, and generation of shipping labels.

Duration and retention

For the term of the Service Agreement. Personal data is retained for up to 30 days after order delivery, then deleted; non-personal operational data is retained for up to 18 months. Backups are retained for approximately 21 days.

Annex II — Technical and Organizational Measures

Area	Measure
Encryption in transit	TLS 1.3 enforced for all communications
Encryption at rest	AES-256 on production database volumes and backups
Access control	Role-based access, least privilege, quarterly access reviews
Authentication	Single sign-on with 2-step verification enforced for staff accounts
Administrative access	Restricted to a private VPN
Perimeter security	Web application firewall and managed ingress
Monitoring and logging	Centralized metrics and logs, retained 12 months
Vulnerability management	Weekly automated scans and an annual external penetration test
Backups	Daily and weekly encrypted backups, ~21-day retention
Deletion standard	NIST SP 800-88; certification of destruction on request

Annex III — List of Subprocessors

Subprocessor	Service provided	Location
Lithus	Managed infrastructure and platform operations	Germany (EU)
Hetzner Online GmbH	Production server hosting	Germany (EU)
OVH	Encrypted off-site backup storage	Gravelines, France (EU)
Shippo	Shipping label generation (name, address, phone)	United States
Cloudflare	Web application firewall and TLS termination	United States

All personal data at rest is stored in the EU/EEA (Germany for production, France for backups). Transfers to the United States subprocessors rely on the EU Standard Contractual Clauses, and, where the recipient is certified, the EU-US Data Privacy Framework, as set out in Section 5.