# Data Processing Agreement (template)

Template v1 - November 2026

**TEMPLATE: NOT LEGAL ADVICE. This document is a draft for discussion. It has not been reviewed by a lawyer and must be reviewed and adapted by qualified counsel for both parties before anyone signs it. Fill in every [*] item. It does not claim, and must not be read to claim, any security certification or audit result.**

## 1. Parties and purpose

This Data Processing Agreement (the "DPA") is made between [Customer legal name], [address] (the "Customer"), and [Silona operating entity legal name], St. Louis, MO ("Silona"), and forms part of the agreement under which Silona provides its supply chain planning service to the Customer (the "Agreement").

It applies to personal data that Silona processes on the Customer's behalf while providing the service. If this DPA and the Agreement conflict about personal data, this DPA prevails.

## 2. Definitions

"Personal data", "processing", "controller", "processor", "data subject" and "personal data breach" have the meanings in applicable data protection law, including [Regulation (EU) 2016/679 (GDPR)], [the UK GDPR], [the California Consumer Privacy Act as amended] and any other law that applies to the Customer's personal data ("Data Protection Law").

"Customer Data" means all data the Customer, its users and its suppliers put into the service, including the personal data described in Annex 1. "Sub-processor" means a third party engaged by Silona to process Customer Data.

## 3. Roles and instructions

The Customer is the controller and Silona is the processor of the personal data in Customer Data. Silona will process that personal data only on the Customer's documented instructions, which are the Agreement, this DPA, and the Customer's use of the service's features (including its settings, exports and deletion tools). Silona will tell the Customer if it believes an instruction breaks Data Protection Law.

The Customer is responsible for having a lawful basis for the data it loads, for the accuracy of that data, and for the access it gives to its own users and to the suppliers it invites to the Supplier Portal.

## 4. Confidentiality and personnel

Silona will limit access to Customer Data to personnel who need it to provide the service and who are bound by confidentiality obligations. [Describe screening and training commitments, if any.]

## 5. Security measures

Silona will maintain technical and organisational measures appropriate to the risk. The measures in place at the date of this template are listed in Annex 2. Silona may change them if the overall level of protection does not fall.

## 6. Sub-processors

The Customer gives general authorisation for the sub-processors listed in Annex 3. Silona will give the Customer at least [30] days' notice of a new or replacement sub-processor, by [email / in-app notice]. The Customer may object on reasonable data protection grounds within [14] days; if the parties cannot resolve the objection, the Customer may end the affected service and receive a pro-rata refund of prepaid fees for it.

Silona will bind each sub-processor to data protection terms no less protective than this DPA and remains responsible for their performance of those terms.

## 7. International transfers

Silona's sub-processors may process Customer Data in [regions to be confirmed by Silona]. Where Data Protection Law restricts a transfer, the parties will rely on [an adequacy decision / the Standard Contractual Clauses (Module Two, controller to processor) / the UK Addendum / another valid transfer mechanism], which are incorporated by reference and completed with the details in the Annexes. [Counsel to confirm the mechanism and complete the transfer impact assessment.]

## 8. Data subject requests

Silona will, taking into account the nature of the processing, help the Customer respond to requests from data subjects. The service lets Customer administrators export all company data and delete it without contacting Silona. If a data subject contacts Silona directly, Silona will refer them to the Customer unless the law requires otherwise.

## 9. Personal data breach

Silona will notify the Customer without undue delay and in any event within [72] hours after becoming aware of a personal data breach affecting Customer Data. The notice will describe, as far as known, the nature of the breach, the data and approximate number of people affected, likely consequences, and the measures taken or proposed. Silona will keep the Customer informed and help it meet its own notification duties. [Define the notification channel and contact.]

## 10. Return and deletion

During the term the Customer can export all Customer Data (JSON and CSV, with supplier documents) at any time. At the end of the Agreement, Silona will delete Customer Data within [30 / 90] days, as set by the retention setting in the service, unless the law requires it to keep some. The Customer may delete its company data immediately using the service. Copies in provider backups and point-in-time history age out on the provider's own schedule, currently described in Annex 2.

## 11. Audits and information

Silona will make available the information reasonably needed to show compliance with this DPA, including a written description of its security controls. Silona does not currently hold a third-party security certification or audit report. [If the Customer requires an on-site or remote audit, the parties will agree scope, timing and cost in good faith, no more than once a year except after a breach.]

## 12. Liability, term and law

Each party's liability under this DPA is subject to the limits in the Agreement, except where the law does not allow that limit. [Counsel to confirm.] This DPA lasts as long as Silona processes Customer Data. It is governed by [governing law] and the courts of [jurisdiction], except where Data Protection Law requires otherwise.

## Annex 1. Details of processing

| Item | Detail |
|---|---|
| Subject matter | Supply chain planning: forecasting, purchase order management, shipment tracking, alerts and supplier collaboration. |

| | |
|---|---|
| Duration | The term of the Agreement plus the retention period in section 10. |
| Nature and purpose | Storing, organising, analysing and displaying Customer Data to provide the service; sending alerts and notifications the Customer configures. |
| Categories of data subjects | Customer employees and contractors who use the service; supplier contacts invited to the Supplier Portal; named contacts in buyer or supplier records. |
| Categories of personal data | Name, work email address, job title, role, sign-in and activity records (audit log), messages and uploaded documents that may name individuals. Phone number if the user adds one for alerts. |
| Special categories | None intended. The Customer must not load special-category data. |
| Business data (not personal) | Items, inventory, demand history, purchase orders, prices, forecasts and similar commercial data are Customer Data and are protected as confidential information. |

## Annex 2. Technical and organisational measures

This list describes what exists in the product at the date of this template. It is not a certification. It should be re-checked against the live service before signing.

- Access control: roles (administrator, planner, viewer); every database query is scoped to the Customer's company; supplier users are separate accounts that see only their own purchase orders.
- Authentication: passwords stored as bcrypt hashes; optional authenticator-app two-factor sign-in with one-time recovery codes; administrators can require it; OIDC and SAML single sign-on; account and network-address lockout after repeated failed sign-ins; idle session timeout set by the Customer.
- Sessions: signed, HTTP-only, same-site, secure cookies; supplier and staff sessions are separate and cannot be used across each other.
- Encryption in transit: TLS between users, the application host and the database provider.
- Encryption at rest: the database provider encrypts stored data (AES-256 at the storage layer, per its published documentation). In addition, Silona seals ERP write-back payloads, webhook signing secrets, supplier documents, SSO client secrets and authenticator keys with AES-256-GCM before they are stored. Unit costs and prices on items and PO lines are stored as plain numbers because planning needs to total and compare them in the database.
- Logging: an append-only audit log of sign-ins, approvals, setting changes, exports and security events, visible to Customer administrators.
- Data portability and deletion: self-service export of all company data; self-service deletion; configurable automatic erasure after contract end.
- Backups: the database provider keeps point-in-time history (currently 6 hours on the plan Silona uses, per the provider's documentation). Silona provides a logical export script and a tested restore procedure. Longer backup history requires a paid provider plan. [Update if the plan changes.]
- Supplier documents: size-capped, extension, type and content checked, stored sealed, and served only as downloads with a restrictive content-security policy.
- Not in place today: third-party certification or audit, penetration test report, SCIM provisioning, customer-managed encryption keys, IP allow-listing, multi-region failover. [Edit as this changes.]

## Annex 3. Sub-processors

| Sub-processor | Purpose | Location |
|---|---|---|
| Vercel Inc. | Application hosting and serverless compute | [Region(s) to be confirmed] |
| Neon, Inc. | Managed PostgreSQL database hosting and point-in-time history | [Region to be confirmed] |
| [Email provider, if one is added] | [Sending alert and notification email] | [*] |

Each sub-processor publishes its own security and compliance documentation. Those documents describe the sub-processor's platform, not Silona.

## Signatures

| | Customer | Silona |
|---|---|---|
| Name | [*] | [*] |
| Title | [*] | [*] |
| Date | [*] | [*] |
| Signature | | |