

Privacy Policy

Kerovento

Effective date	August 1, 2026
Version	4.0
Applies to	Kerovento, an internal web application
Data controller	Supastrip Inc., Virginia, USA · Processor: Zintra LLC, Miami, Florida, USA

This Privacy Policy explains how Supastrip Inc. (“Supastrip,” “we,” “us,” or “our”) collects, uses, stores, protects, and deletes information in connection with Kerovento (the “Application”), a financial, operational, and workforce management, analytics, and reporting application used by Supastrip Inc. and its affiliated entities. The Application is licensed to Supastrip by Zintra LLC (“Zintra”), a Florida limited liability company, which provides it under the Kerovento name. Supastrip is the controller of the data described in this Policy. Zintra acts as a processor on Supastrip’s instructions and does not determine the purposes for which that data is processed. Section 5.5 sets out Zintra’s role.

The Application is used solely for our own internal business purposes. It is **not** offered to, marketed to, or used by members of the general public; it does **not** have public user registration; and we do **not** sell, rent, license, or share for value any information it processes.

1. About the Application

Kerovento is a private, internally hosted web application that consolidates financial, accounting, operational, and workforce data from systems that Supastrip owns or is authorized to access, and presents that data to authorized Supastrip personnel as management dashboards and reports. The instance described in this Policy is configured specifically for Supastrip and deployed in infrastructure under Supastrip’s control.

Two characteristics of the Application are central to this Policy:

- **Read-only.** Kerovento reads data from connected systems and displays it. It does not create, post, modify, or delete records in any connected accounting, ERP, or payroll system.
- **Internal-only.** There is no public-facing interface, no customer portal, no self-service sign-up, and no consumer user base. Access is limited to named Supastrip employees and authorized contractors.

1.1 Functional modules

The Application currently comprises the following reporting modules:

- Sales — revenue trend, open orders, customer concentration
- Production — output volumes, work-order status, machine and line performance
- Cash & Banking — bank balances and cash-position summaries
- Accounts Receivable / Accounts Payable Aging
- Inventory — stock levels, valuation, aging and reserve analysis
- General Ledger / Budget vs. Actual — by entity and cost center
- Labor & Workforce — headcount, hours, labor cost and absorption by cost center

2. Information We Access

To produce internal financial, operational, and workforce reporting, the Application connects to business systems that we own or are authorized to access and reads data from them. Depending on the connected system, this may include:

2.1 Connected systems and data categories

Connected system	Categories of data accessed
QuickBooks Online (Intuit Inc. — authorized API)	Chart of accounts, trial balance, general-ledger balances and transactions, accounts receivable and payable balances, customer and vendor lists, invoices and bills, and related company financial records, for the company files we connect.
SAP Business One (ERP, operated by our hosting provider)	Sales orders and invoices, purchase documents, production and work-order data, inventory items, quantities and valuations, business-partner master records, and general-ledger and cost-center data.
isolved (payroll and human capital management)	Employee-level workforce and payroll records. See Section 3, which governs this category specifically.
Business intelligence datasets (Power BI / Microsoft Fabric)	Aggregated and modelled metrics from reporting datasets we already maintain, derived from the systems above.
Production and machine systems (machine telemetry)	Machine run-time, output, downtime, changeover, and scheduling telemetry. This data is equipment-level. Where telemetry is associated with a shift or operator, it is treated as workforce data under Section 3.
Internal planning and budget workbooks	Budget, forecast, and capacity-planning figures prepared by Supastrip finance and operations staff.

The Application accesses this data **only for accounts and instances that we own or are authorized to access**, and only after an authorized administrator of Supastrip has explicitly established that connection.

2.2 Business-contact and transactional personal data

Personal data appears within business records processed by the Application, including:

- the name of an employee who entered, approved, or is referenced on a transaction;
- the name, business address, business email, or business telephone number of a customer or vendor contact;
- the name of a sales representative associated with an order; and
- operator or shift identifiers associated with production records.

This data is processed as an integral part of the underlying business record, solely for internal reporting.

2.3 Application usage data

To operate and secure the Application, we log limited technical information about its use, such as the authenticated user identifier, the date and time of access, the pages or reports requested, and error diagnostics. These logs are used for security, troubleshooting, and access control, and for no other purpose.

3. Employee and Payroll Data

The Application connects to isolated and processes employee-level workforce and payroll records. This is personal data processed as primary content, not incidentally, and it is subject to the additional protections in this Section.

3.1 Data we access

We access	We do not access
Employee name and internal employee identifier	Social Security numbers and other government tax identifiers
Job title, department, cost center, and work location	Bank account and direct-deposit details
Employment status, hire date, and termination date	Home address, personal telephone, and personal email
Hours worked, overtime, shift, and paid-time-off balances	Date of birth and demographic characteristics
Gross pay, employer burden, and fully loaded labor cost	Health, medical, benefit-election, and dependent information
Labor cost allocated to cost center, work order, or production line	Disciplinary records, performance ratings, and immigration status

We apply the principle of data minimisation: the Application requests only those fields required for the workforce and labor-cost reporting described in this Policy. Fields not required for that purpose are not retrieved, even where they exist in the source system.

3.2 Purposes

Employee and payroll data is used only to:

- calculate labor cost, overhead absorption, and cost of goods sold;
- report headcount, hours, overtime, and labor productivity by cost center and production line;
- support budgeting, forecasting, capacity planning, and month-end close; and
- support internal financial controls and audit.

It is **not** used for individual performance management, disciplinary purposes, ranking of individual employees, or any form of automated decision-making producing legal or similarly significant effects. The Application does not build profiles of individual employees and does not conduct behavioral monitoring of individuals.

3.3 Access restriction

Access to modules containing employee-level compensation data is restricted, by role, to a defined group comprising executive management, Finance, and Human Resources personnel with a documented business need. Authorized Users of other modules cannot view individual compensation data. This restriction is enforced technically through role-based access control and contractually through the End-User License Agreement.

3.4 Lawful basis and employment context

We process employee and payroll data as necessary to perform the employment relationship, to comply with our legal obligations in tax, wage-and-hour, accounting, and statutory reporting, and for our legitimate interest in operating accurate financial and operational controls. Where local law requires a different or additional basis, or requires notice to or consultation with employees or their representatives, we comply with that requirement.

This Section supplements, and does not replace, the employee privacy notices and human resources policies applicable to each Supastrip entity and location.

4. How We Use the Information

We use the information exclusively to:

- generate internal financial statements, dashboards, key performance indicators, and management reporting;
- consolidate results across our affiliated entities and operating locations;
- support internal financial analysis, budgeting, forecasting, and planning;
- support operational visibility — production scheduling, inventory management, and capacity planning;
- calculate labor cost and overhead absorption, as described in Section 3;
- support internal controls, month-end close, reconciliation, and audit preparation; and
- operate, secure, troubleshoot, and improve the Application itself.

We do **not** use the information for advertising or marketing of any kind. We do **not** sell, rent, or share it with any third party for that party's own purposes. We do **not** use it to train, fine-tune, or otherwise develop any generally available machine-learning or artificial-intelligence model.

5. Connected-System Provider Terms

Each connection is governed by the terms of the relevant provider, in addition to this Policy.

5.1 Intuit / QuickBooks Online

Access is granted exclusively through Intuit's OAuth 2.0 authorization process, initiated and approved by an administrator of the relevant QuickBooks company file. We do not request, store, or use QuickBooks user names or passwords at any time.

We request read-only accounting scopes only, and only the scopes necessary for the reporting functions described in this Policy. The Application does not write to, modify, or delete any record in QuickBooks Online.

We store only the OAuth access token, refresh token, realm (company) identifier, and connection metadata required to maintain the connection, together with the financial data needed for reporting. Tokens are stored encrypted, are accessible only to the Application's server process, and are never exposed to the browser, written to source control, or shared with any third party.

An administrator may revoke the connection at any time from within QuickBooks Online (Apps → Manage → Disconnect) or by contacting us at the address in Section 13. Upon revocation, the Application immediately ceases all access to that company's Intuit data, and stored tokens for that connection are deleted within 24 hours.

We access Intuit data through Intuit's authorized API and in accordance with Intuit's applicable developer terms and data-handling requirements, including their restrictions on the use, retention, and disclosure of Intuit data.

5.2 SAP Business One and our ERP hosting provider

Our SAP Business One environment is operated on our behalf by a third-party hosting provider under a written services agreement that includes confidentiality and data-protection obligations. The Application connects to that environment using dedicated, read-only service credentials issued to Supastrip, over an encrypted connection, subject to network access restrictions agreed with the provider. The Application does not post, modify, or delete any document, journal entry, or master-data record in SAP Business One.

5.3 isolved

The Application connects to isolved using dedicated, read-only credentials issued to Supastrip, and retrieves only the fields identified in Section 3.1. isolved processes data as our service provider under its own agreement with us, which includes confidentiality and data-protection obligations. The Application does not write to, modify, or delete any record in isolved; all payroll and personnel changes are made in isolved directly, by Human Resources.

5.4 Business intelligence and machine telemetry

Business intelligence datasets are maintained by Supastrip within our own Microsoft tenant and are derived from the systems described above; no new categories of data are introduced by that layer. Machine telemetry is collected from production equipment on our own network and describes equipment performance.

5.5 Zintra LLC, the platform provider

Kerovento is licensed to Supastrip by Zintra LLC, a Florida limited liability company with its address at 3651 Percival Ave, Miami, FL 33133, United States. Zintra develops and maintains the Application and provides technical support for it.

Supastrip remains the controller of all data described in this Policy. Zintra acts as a processor and handles that data only on Supastrip's documented instructions, only to provide, secure, support and maintain the Application, and for no purpose of its own.

The Application is deployed in infrastructure under Supastrip's control. Connection credentials for the systems in Section 2.1 are issued by Supastrip and held within that environment. Zintra does not hold a standing copy of Supastrip's financial or payroll data.

Zintra personnel may access the environment where necessary to diagnose or resolve a technical issue. Such access is granted by Supastrip, is limited to what the issue requires, is logged, and ends when the issue is closed. Zintra personnel with any such access are bound by written confidentiality obligations.

Zintra does not sell data processed by the Application, does not use it for advertising, and does not use it to train, fine-tune or develop any generally available machine-learning or artificial-intelligence model. Zintra does not permit any third party to do so.

Zintra will not engage a sub-processor in respect of Supastrip data without Supastrip's prior written authorization. On termination of the licence, Zintra will return or delete any Supastrip data in its possession, except where retention is required by law.

Where an authorized implementation partner configures or supports the instance on Supastrip's behalf, that partner acts under written contract with Supastrip and is subject to the same restrictions.

6. How We Store and Protect Information

We apply administrative, technical, and physical safeguards designed to protect information against unauthorized access, alteration, disclosure, or destruction. These include:

- **Encryption and storage.** Data at rest is stored on access-controlled systems that we operate or that are operated on our behalf under contract. Data in transit is protected using TLS encryption. Connection credentials and API tokens are stored encrypted.
- **Access control.** Access to the Application and its underlying data is limited to authorized personnel on a need-to-know basis, governed by role-based access controls and unique named accounts. Modules containing employee-level compensation data are restricted to a defined group, as described in Section 3.3. Administrative access is restricted to a small number of designated individuals.

- **Authentication.** Access to the Application requires authentication. Accounts with administrative or credential-management rights, and accounts with access to employee-level payroll data, require multi-factor authentication.
- **Separation of secrets and code.** Secrets, API keys, and tokens are held in environment configuration and are excluded from source control. Financial and payroll data extracts are excluded from the Application’s code repository by policy and by configuration.
- **Minimisation at the connector.** The Application requests only the fields required for the reporting purposes described in this Policy, and requests read-only scopes wherever the connected system supports them.
- **Logging and monitoring.** Application access and administrative actions are logged and periodically reviewed. Access to employee-level compensation data is logged.
- **Personnel controls.** Access rights are reviewed periodically and are revoked promptly upon a change of role or termination of employment or engagement.

No method of electronic storage or transmission is completely secure, and while we work to protect the information described in this Policy, we cannot guarantee absolute security.

6.1 Security incidents

We maintain an internal process for identifying, investigating, containing, and remediating security incidents affecting the Application. Where an incident involves Intuit data, we will notify Intuit in accordance with their developer requirements. Where an incident involves employee or other personal data and applicable law requires notification, we will notify affected individuals and the relevant authorities within the time frames required by that law.

7. Data Retention and Deletion

We retain data only for as long as it is needed for the purposes described in this Policy, or for as long as required by our accounting, tax, employment, and legal recordkeeping obligations.

Data category	Retention
OAuth tokens and connection credentials	For the life of the connection; deleted within 24 hours of disconnection or revocation.
Financial and accounting data used for reporting	Retained for the period required by our internal retention policy and applicable tax, accounting, and statutory recordkeeping obligations.
Employee and payroll data	Retained no longer than necessary for labor-cost reporting and financial close, and in any event not less than the periods required by applicable wage-and-hour, tax, and employment recordkeeping law. Isolated remains the system of record.
Derived reports, dashboards, and consolidated outputs	Retained as internal business records in line with our accounting record retention practices. Reports containing individual

Data category	Retention
	compensation data are retained only where required for audit or statutory purposes.
Machine and production telemetry	Retained for operational analysis and capacity planning, then aggregated or deleted.
Application access and security logs	Retained for a limited period sufficient for security review and troubleshooting, then deleted.

When a connected account is disconnected, we cease all further access to that account. Underlying data already used to produce financial records may be retained where necessary to preserve the integrity and auditability of financial statements already issued, in which case it is retained under the safeguards described in Section 6 and is not used for any new purpose.

8. Disclosure and Service Providers

We do not sell or share information processed by the Application. We may disclose information only:

- to service providers who host or support the Application and its connected systems, under written confidentiality and data-protection obligations, and solely to operate the Application on our behalf;
- to our affiliated entities, for internal consolidated financial, operational, and workforce reporting;
- to our external auditors, accountants, payroll advisors, and legal advisors, under professional confidentiality obligations, in connection with audit, tax, employment, and compliance work; or
- where required by law, regulation, subpoena, or other valid legal process, or to establish, exercise, or defend legal claims.

8.1 Categories of service providers

The Application relies on the following categories of third parties. Each is bound by contract to process data only on our instructions:

- cloud and application hosting providers;
- our ERP hosting provider, which operates the SAP Business One environment on our behalf;
- Intuit Inc., as the provider of QuickBooks Online and the API through which we access that data;
- isolved, as our payroll and human capital management provider;
- Microsoft, as the provider of the business intelligence platform within our own tenant; and

- code repository and development-tooling providers, which host application source code (but not financial or payroll data extracts).

9. International Data Transfers

Supastrip Inc. is established in the United States and operates affiliated entities outside the United States, including in Paraguay. Data processed by the Application, including workforce data, may be accessed by authorized personnel in more than one country for the purpose of consolidated reporting. Where such transfers involve personal data subject to non-U.S. data-protection or employment law, we implement appropriate safeguards, including intra-group confidentiality and data-protection commitments, role-based access limits, and the controls described in Section 6, and we comply with any local notification or consultation requirements applicable to workforce data.

10. Individual Rights

Where an individual whose personal data is processed by the Application has rights under applicable data-protection or employment law — such as rights of access, correction, deletion, restriction, portability, or objection — they may exercise those rights by contacting us at the address in Section 13, or, for employees, through Human Resources.

We will respond within the period required by applicable law. Certain requests may be limited where the data forms part of a financial, payroll, or employment record we are legally required to retain.

10.1 Source systems of record

Because the Application is read-only, corrections to personal data are made in the relevant source system — isolved for employee records, SAP Business One or QuickBooks Online for business-partner records — and flow through to the Application on the next data refresh. A request to correct data will be actioned in the source system.

10.2 Children

The Application is a business tool. It is not directed to children, and we do not knowingly process personal information relating to any individual under the age of 16.

11. Use of Automated and AI-Assisted Tools

Supastrip uses software development and analysis tools, which may include AI-assisted tools, in the course of building and maintaining the Application. Where such tools are used:

- they are used for engineering, documentation, and analytical support, not as an automated decision-maker over individuals;

- production financial data, payroll data, and credentials are not submitted to any third-party tool that is permitted to retain that data for its own model training; and
- any such tool is subject to the confidentiality and access-control requirements described in Section 6.

We do not permit any third party to use data processed by the Application to train, fine-tune, or develop generally available machine-learning or artificial-intelligence models.

12. Changes to This Policy

We may update this Privacy Policy from time to time to reflect changes in the Application, its connected systems, or applicable legal requirements. Material changes will be reflected by updating the “Effective date” and version number above. Where a change materially affects the processing of employee data, we will notify affected personnel.

13. Contact Us

Questions, requests, or concerns regarding this Privacy Policy or our data practices should be directed to:

Supastrip Inc.

Postal address	1625D Ashton Park Drive, South Chesterfield, Virginia 23834, United States
-----------------------	--

Email	info@supa-strip.com
--------------	---------------------

Attention	Privacy — Kerovento
------------------	---------------------

Questions concerning Zintra LLC’s handling of data as processor may be directed to Zintra LLC, 3651 Percival Ave, Miami, FL 33133, United States, or info@zintra.de.

This Privacy Policy is governed by the laws of the Commonwealth of Virginia, United States, without regard to its conflict-of-laws provisions.

Version History

Version	Date	Summary of changes
1.0	August 1, 2026	Initial policy.

Version	Date	Summary of changes
2.0	August 1, 2026	Expanded scope description, data source inventory, security controls, retention schedule, international transfers, individual rights, AI tooling, and incident response.
3.0	August 1, 2026	Added full connected-system inventory (SAP Business One, isolved, business intelligence, machine telemetry); added Section 3 governing employee and payroll data, including field-level minimisation, purpose limits, and role-based access restriction; added provider terms for each connection; updated security, retention, disclosure, transfers, and rights accordingly.