

ZYNTRALYNK INC.

PRIVACY STATEMENT

Effective Date: August 21, 2026

Important: This document is a general privacy-policy baseline for Zyntralynk's enterprise software and AI-enabled SAP solutions. It should be reviewed and adapted by qualified privacy/legal counsel to match Zyntralynk's actual data flows, subprocessors, hosting arrangements, cookies, and regulatory obligations before publication.

1. Scope of This Privacy Statement

This Privacy Statement explains how Zyntralynk Inc. ("Zyntralynk," "we," "us," or "our") may collect, use, disclose, retain, and protect personal information in connection with our websites, enterprise software, AI-enabled agents, integrations, support activities, demonstrations, and related services (collectively, the "Services"). It applies to information for which Zyntralynk determines the purposes and means of processing. Where Zyntralynk processes personal information solely on behalf of an enterprise customer, the customer's agreement and applicable data-processing terms govern that processing.

2. Information We May Collect

Depending on how the Services are used, we may collect business contact information such as name, business email address, company, title, and telephone number; account and authentication information; communications and support requests; transaction, subscription, and billing-related information; device, browser, log, diagnostic, and usage information; and information submitted by customers or authorized users through the Services. Enterprise integrations may also process data from SAP or other connected systems as configured and authorized by the customer.

3. Enterprise and SAP-Related Data

Zyntralynk solutions may connect to SAP environments, SAP BTP, SAP Joule or Joule Studio, APIs, workflow services, and other enterprise applications. The categories of information processed depend on the customer's configuration, permissions, and business process. Customers are responsible for determining which data the Services may access and for configuring appropriate authorizations, data minimization, retention, and governance controls. Zyntralynk does not require customers to provide personal information that is unnecessary for the applicable use case.

4. How We Use Information

We may use information to provide, operate, configure, secure, maintain, and support the Services; authenticate users and administer accounts; process transactions and customer requests; troubleshoot and improve performance; detect security threats, misuse, or technical issues; provide customer support; communicate about the Services; comply with legal obligations; and develop or improve products and features consistent with applicable agreements and law.

5. AI and Agentic Processing

Certain Services may use artificial intelligence, machine learning, large language models, rules, or autonomous-agent workflows. Information processed by these capabilities may be used to analyze enterprise events, generate recommendations, classify conditions, support root-cause analysis, orchestrate workflows, or perform customer-authorized actions. The exact processing depends on customer configuration. Where applicable, Zyntralynk may maintain operational or audit records relating to agent decisions, recommendations, approvals, system interactions, and actions for security, governance, troubleshooting, and accountability purposes.

6. Legal Bases for Processing

Where applicable law requires a legal basis, Zyntralynk may process personal information as necessary to perform a contract, take requested pre-contractual steps, pursue legitimate business interests such as providing and securing the Services, comply with legal obligations, or based on consent where consent is appropriate. The applicable basis depends on the context and jurisdiction.

7. How We Share Information

We may disclose information to service providers and subprocessors that support hosting, infrastructure, security, analytics, communications, customer support, or other business operations; to professional advisers; to government or regulatory authorities where legally required; in connection with a merger, acquisition, financing, reorganization, or sale of assets; or as otherwise authorized by the customer or user. We do not sell personal information for monetary consideration. Any disclosures are subject to applicable contractual, confidentiality, and legal requirements.

8. Service Providers and Subprocessors

Zyntralynk may use third-party cloud, infrastructure, software, security, communications, or AI service providers in delivering the Services. The providers used may vary by product, deployment model, and customer agreement. Where required, Zyntralynk will use contractual and organizational measures designed to require appropriate protection of personal information processed on our behalf.

9. Data Security

Zyntralynk uses commercially reasonable administrative, technical, and organizational safeguards designed to protect information against unauthorized access, disclosure, alteration, loss, or misuse. No method of transmission or storage is completely secure, and we cannot guarantee absolute security. Customers remain responsible for security controls within customer-managed environments, including credentials, roles, permissions, endpoints, network configurations, and SAP or other connected-system authorizations.

10. Data Retention

We retain personal information for as long as reasonably necessary to provide the Services, satisfy contractual requirements, maintain legitimate business and security records, resolve disputes, enforce agreements, and comply with applicable legal obligations. Retention periods may vary according to the type of information, customer configuration, applicable agreement, and legal requirements. Where Zyntralynk acts as a processor, retention and deletion may be governed by customer instructions and contractual terms.

11. International Data Transfers

Zyntralynk and its service providers may process information in countries other than the country in which it was originally collected. Where required by applicable law, we will use appropriate safeguards for cross-border transfers of personal information, which may include contractual protections or other recognized transfer mechanisms.

12. Privacy Rights and Choices

Depending on applicable law and where an individual resides, the individual may have rights to request access to, correction of, deletion of, or a copy of personal information, to object to or restrict certain processing, or to withdraw consent where processing is based on consent. Some rights are subject to legal exceptions. If Zyntralynk processes information solely on behalf of an enterprise customer, individuals may need to direct requests to that customer, and Zyntralynk will assist as required by applicable contractual or legal obligations.

13. Cookies and Website Technologies

Our websites may use cookies or similar technologies that are necessary for site functionality, security, preferences, analytics, or performance. Where required by law, users will be provided appropriate notice or choices regarding non-essential technologies. Browser settings may also allow users to control certain cookies.

14. Children's Privacy

The Services are intended for business and enterprise use and are not directed to children. Zyntralynk does not knowingly collect personal information from children through the Services in circumstances where parental consent would be required. If we learn that such information was collected improperly, we will take reasonable steps to address it.

15. Third-Party Services and Links

The Services or Zyntralynk websites may contain integrations or links to SAP or other third-party products, services, or websites. Those third parties have their own privacy practices and policies. Zyntralynk is not responsible for the privacy practices of third parties acting independently of Zyntralynk.

16. Customer Responsibilities

Enterprise customers are responsible for providing required notices to their users, employees, customers, or other data subjects; establishing an appropriate legal basis for data supplied to the Services; configuring access controls and retention; and complying with privacy, employment, sector-specific, and other laws applicable to their use of the Services. Customers should avoid submitting sensitive personal information unless it is necessary, authorized, and appropriately protected for the intended use case.

17. Changes to This Privacy Statement

We may update this Privacy Statement periodically to reflect changes in our Services, legal requirements, or privacy practices. The updated statement will identify a revised effective date. Material changes will apply prospectively, subject to applicable law and contractual requirements.

18. Contact Us

Questions, requests, or concerns regarding this Privacy Statement or Zyntralynk's privacy practices may be submitted through the contact information published on Zyntralynk's official website at www.zyntralynk.com.

Copyright © 2026 Zyntralynk Inc. All rights reserved.