Salviminda

Sabisu Consulting BV · S-Link

Technical and Organisational Measures

Sabisu Consulting BV (Salviminda) — S-Link Service

v2.3 · in force since 5 November 2026

Approved and in force. This document describes measures actually in place and forms the annex referred to in Schedule 2 of the Salviminda Data Processing Agreement.

This document describes the technical and organisational security measures implemented by Sabisu Consulting BV (trading as Salviminda) ("Salviminda") to protect Personal Data processed in the context of the S-Link Peppol e-invoicing service, in accordance with Article 32 of Regulation (EU) 2016/679 (GDPR).

It describes measures that are in place at the date of this version. Measures that Salviminda plans but has not yet implemented are identified as such in section 6, so that a Controller can assess the current position accurately. Salviminda is not itself certified to ISO/IEC 27001; it operates the measures described here and relies in addition on the certifications of its hosting and access-point providers, as set out in section 3.

Document metadata	
Document owner	Sabisu Consulting BV (trading as Salviminda)
Product / service	S-Link connector and S-Link Hub
Version	v2.3 — in force since 5 November 2026, superseding v2.2 (4 November 2026), v2.1 (3 November 2026), v2.0 (30 September 2026) and the v1.0 and v1.1 drafts
Status	Approved and in force
Classification	External — may be shared with clients, prospects and auditors
Next review due	By 30 September 2027, or earlier following a significant security incident or change in processing
Data protection contact	privacy@salviminda.com
Security contact	security@salviminda.com

1. Organisational Measures

1.1 Information Security Policy

Salviminda maintains a written Information Security Policy, reviewed and approved by management at least annually and after any significant security incident or major change to the platform. It establishes the framework for managing information security risks and is issued to all personnel, in every location. A copy is available to Controllers on request.

1.2 Data Protection Responsibility

Salviminda is not required to appoint a statutory Data Protection Officer under Art. 37 GDPR and has not done so. The Managing Director holds overall responsibility for data protection and the Technical Lead for the technical measures described in section 2. Data protection queries may be directed to privacy@salviminda.com and security matters, including responsible disclosure, to security@salviminda.com.

1.3 Staff Training and Awareness

— All personnel — employees, contractors and freelance professionals, in every location — receive data protection and information security briefing at onboarding, in English.

— Refresher guidance is provided at least annually and whenever material changes occur; personnel involved in procurement, recruitment or partner management receive additional guidance.

— Records of training and policy issue are maintained.

1.4 Confidentiality Obligations

All employees, contractors and freelance professionals with access to Personal Data are contractually bound by confidentiality obligations that survive the end of their employment or engagement, and are subject to documented processing instructions.

1.5 Access Control

— Access to Personal Data is granted on a need-to-know basis under role-based access control, on documented approval. Administrative and privileged access is granted individually and only for the period required. Support and development roles currently carry standing read access to client tenants in S-Link Hub and to the ticket system; per-tenant scoping of that access is a planned measure identified in section 6.

— User access rights are reviewed at least quarterly.

— Access rights are revoked on change of role and on the last working day of any staff member or contractor; client-side accounts are reported to the client for removal.

— Privileged access is strictly limited, held in accounts separate from day-to-day accounts, and logged.

— Every person accessing a client environment or production does so under an account identifying them individually. Shared or generic accounts are not used.

1.6 Sub-processor and Vendor Management

Before engaging a new sub-processor or vendor that will have access to Personal Data, Salviminda conducts a due diligence assessment covering the vendor's security posture, certifications and data protection compliance. Data processing agreements are concluded with all sub-processors, and their assurance is reviewed annually. The current sub-processors are listed in the Salviminda Sub-processor List and in Schedule 3 of the Data Processing Agreement; Controllers are notified of intended changes at least 30 days in advance.

1.7 Incident Response

— A documented Personal Data Breach response procedure is maintained. All suspected or confirmed breaches are assessed, logged and escalated, and are reported internally to the Technical Lead and Managing Director immediately.

— Containment steps — isolating affected accounts or systems, revoking or rotating credentials and API keys, preserving evidence — are taken within 24 hours.

— Where Salviminda acts as processor, it notifies the affected Controller without undue delay and at the latest within 48 hours of becoming aware, with the information the Controller needs to meet its own 72-hour notification duty. Salviminda does not notify a Supervisory Authority or Data Subjects on a Controller's behalf unless required by law or instructed by the Controller.

— Where Salviminda acts as controller, it notifies the Belgian Data Protection Authority within 72 hours where Art. 33 GDPR requires it.

— A post-incident review is held within 10 working days and a written incident report is provided to affected Controllers on request. A register of all breaches is maintained, including those not notified.

1.8 Records of Processing Activities

Salviminda maintains a register of processing activities in accordance with Article 30 GDPR, covering its activities both as controller and as processor, and makes it available to Controllers and to a Supervisory Authority on request.

2. Technical Measures

2.1 Encryption in Transit

— All data exchanged between the S-Link service and external systems (client ERP environments, S-Link Hub, the access point) is encrypted using TLS 1.2 or higher, with TLS 1.3 preferred and weak ciphers disabled.

— HTTPS is enforced for all web-based access; HTTP requests are redirected to HTTPS.

— Peppol message exchange uses the AS4 messaging protocol, which provides message integrity and confidentiality between access points.

2.2 Encryption at Rest

— Data stores containing Personal Data, including the business documents held in S-Link Hub, are encrypted at rest with platform-managed AES-256 encryption provided by Microsoft Azure.

— Backups are encrypted with the same standard.

— Encryption keys are managed by the platform, separately from the encrypted data; Salviminda personnel do not handle raw key material.

— Full-disk encryption is enabled on all devices used to deliver the Services.

2.3 Authentication and Access Control

— Multi-factor authentication is mandatory on all Salviminda accounts, in every location — Microsoft Entra ID and Microsoft 365, the Azure portal, code hosting and partner portals — including all administrative and privileged access to production.

— The S-Link portal offers multi-factor authentication to client user accounts. It is optional for those accounts and Salviminda recommends that clients enable it.

— Passwords are a minimum of 14 characters, unique per system, generated and stored in an approved secrets manager. Credentials are not reused across clients. Salviminda does not impose arbitrary periodic password rotation, in line with current guidance, but rotates credentials immediately on suspected compromise or on the departure of anyone who held them, and at least annually for API keys and service credentials.

— Role-based access control is implemented: users may access only the data and functions relevant to their role.

— Credentials and API keys are held exclusively in the secrets manager and never in e-mail, chat, tickets or source code.

2.4 Logging and Monitoring

— Access to systems containing Personal Data, access to client environments, and material processing events are logged with a timestamp, user identifier and action performed.

— Logs are retained for 12 months and are protected against tampering; they are not modifiable by operational staff.

— Alerting is enabled on the Microsoft Entra ID and Azure environments for unusual sign-ins, failed authentication, privilege changes and service degradation.

— Logs are reviewed after incidents and on a periodic basis.

2.5 Patching and Vulnerability Management

— Operating systems, applications and cloud components are kept on supported versions, with security updates applied automatically or within 14 days of release.

— Vulnerabilities are prioritised by CVSS score and exposure, with remediation within 72 hours for critical, 14 days for high, 30 days for medium and the next planned release for low severity.

— Software dependencies are monitored automatically for known vulnerabilities through the code-hosting platform's dependency alerts, and flagged vulnerabilities are assessed and patched within the timescales above.

— Salviminda reviews security advisories from Microsoft, its access-point partner and key dependency maintainers, and accepts responsible disclosure at security@salviminda.com.

2.6 Backup and Recovery

— Automated backups of all data stores containing Personal Data are performed daily.

— Backups are encrypted and held in a geographically separate location within the European Union.

— Restore tests are performed at least annually.

— The recovery time objective is 24 hours and the recovery point objective is 24 hours. S-Link is designed so that a client's ERP and invoicing continue to operate independently of Salviminda's own availability, with documents queued and retried automatically during a temporary outage.

2.7 Network and Environment Security

— S-Link Hub is reachable only over HTTPS on published endpoints. Management interfaces and data stores are not exposed to the public internet.

— Production, test and development resources are separated into distinct Azure resource groups or subscriptions.

— The platform benefits from the network-layer protections provided by Microsoft Azure, including platform-level distributed denial-of-service protection and TLS termination.

— No inbound services are exposed from staff devices. Connections to client systems and cloud services use encrypted channels only; untrusted public Wi-Fi is used only with a VPN active.

2.8 Secure Development

— Secure coding practices are followed in the development of the S-Link application and platform.

— All source code is held in a private, access-controlled repository with version history and mandatory multi-factor authentication. Changes are made on branches and reviewed by a second developer before merging where a second developer is available.

— Client production data is never copied into development or test environments; anonymised or synthetic data is used for testing.

— Secrets, connection strings and API keys are injected at deployment time from the secrets manager and are never committed to source control.

— Each release is documented in release notes, and Controllers are informed of changes affecting security, data flows or permissions before deployment.

3. Hosting and Physical Security

S-Link Hub is hosted on Microsoft Azure in the West Europe region (the Netherlands), under Salviminda's own Azure subscription. Microsoft Ireland Operations Ltd acts as hosting sub-processor under the Microsoft Products and Services Data Protection Addendum, and holds ISO/IEC 27001, ISO/IEC 27017 and ISO/IEC 27018 certification and SOC 1, 2 and 3 reports, together with the EU Data Boundary commitments. Physical and environmental security of the data centres is provided and certified by Microsoft.

— Salviminda personnel have no physical access to data centre hardware.

— Salviminda operates a clear-desk and clear-screen practice; confidential information is not left visible and screens are locked when unattended.

— Devices used for Salviminda work have automatic screen lock after a maximum of five minutes of inactivity, full-disk encryption, automatic updates, endpoint protection and a local firewall enabled, and are enrolled in Microsoft Intune where available to permit remote wipe.

— Printing of client data is avoided; any printed material containing Personal Data is cross-cut shredded when no longer needed.

4. Processing Locations and Measures for Access from Outside the EEA

Personal Data contained in business documents processed through the Services is stored within the European Union and is not replicated outside it. Personal Data submitted by client users in support tickets is at present held in Salviminda's internal ticket application, which is hosted in the United States; that data is being withdrawn and the application, together with Salviminda's internal CRM, redeployed to Salviminda's own Microsoft Azure environment within the European Union by 31 January 2027, as recorded in section 6. Salviminda's team works from Belgium and from the Philippines: freelance professionals engaged directly by Salviminda in the Philippines form part of the delivery team and access client environments and data held in S-Link Hub remotely, for development and support purposes. Where a Controller requires that Personal Data processed on its behalf not be accessible from outside the EEA, access is restricted at database level to personnel located in the European Union, and the ticket application is not used for that Controller until the redeployment described in section 6 is complete.

The Philippines is not covered by an adequacy decision. In addition to every measure described above, which applies identically to that team, the following measures apply to access from outside the EEA:

— Standard Contractual Clauses pursuant to Commission Implementing Decision (EU) 2021/914 are concluded with each individual, together with written confidentiality undertakings and documented processing instructions.

— A transfer impact assessment is documented and reviewed at least annually.

— Access is through named individual accounts with mandatory multi-factor authentication, under role-based access control, and is logged. Access rights are reconfirmed at the quarterly access review.

— Storing Personal Data locally, on removable media or in personal cloud accounts is prohibited; work is carried out against the EU-hosted systems.

— Devices used meet the standard in section 3 before any access is granted, and compliance is reconfirmed at the quarterly access review.

5. Data Minimisation and Pseudonymisation

Salviminda applies the principle of data minimisation: only Personal Data necessary for the provision of the Services is collected and processed, and S-Link transmits only the fields required by the applicable e-invoicing format and the receiving platform. Anonymised or synthetic data is used for development and testing. Where pseudonymisation is technically feasible for analytics, it is applied; pseudonymised data remains Personal Data and remains subject to the measures in this document.

6. Measures Not Currently in Place

The following measures are commonly asked about in vendor assessments and are not currently implemented. They are stated here so that a Controller can assess the position accurately rather than infer it:

— Independent third-party penetration testing of the platform is not currently performed.

— Automated infrastructure vulnerability scanning is not currently performed. Dependency vulnerability alerting is in place, as described in section 2.5.

— A web application firewall and dedicated intrusion detection or prevention systems are not currently deployed in front of S-Link Hub; the platform relies on the Azure protections described in section 2.7.

— Salviminda does not hold ISO/IEC 27001, SOC 2 or equivalent certification of its own.

— Access for support and development roles is not yet scoped per client company. These roles currently carry standing read access in S-Link Hub and in the ticket system. The following are being implemented: row-level restriction of access by client company in the production database; removal of standing administrative database access, replaced by named individual accounts and just-in-time elevation with approval, time limit and logging; delivery of support for clients with a contractual EU-only requirement by EU-based personnel only; and development work against a separate database containing synthetic data rather than client data.

— Independent validation of recovery point and recovery time objectives has not yet been performed. The objectives stated in the applicable service levels are design targets; they will be confirmed by a documented restore test and reported to Controllers on request.

— Salviminda's internal applications — TicketHub, the support-ticket application, and First Flow, the CRM — are currently hosted outside the European Union, in the United States. Both are being redeployed to Salviminda's own Microsoft Azure environment within the European Union by 31 January 2027. In the redeployed environment the data is reachable only through the applications, administrative access to the environment is restricted to system administrators located in the European Union, and access within the applications is scoped per client so that clients with a contractual EU-only requirement are served by EU-based support personnel only. Until that work is complete, client personal data is being withdrawn from the applications and the ticket application is not used for clients with such a requirement. The transfer safeguards applicable in the meantime are set out in the Sub-processor List.

Salviminda keeps these under review as the platform and client base grow, and will update this document when the position changes. A Controller with a specific requirement in any of these areas is invited to raise it before contracting so that it can be addressed in the client agreement.

7. Review and Updates

This document is reviewed at least annually, and following any significant change to the processing environment or in response to a security incident. Controllers are notified of material changes to the technical and organisational measures that may affect the level of security provided. Measures may be updated from time to time provided that the level of protection is not reduced.

Approved for and on behalf of Sabisu Consulting BV (trading as Salviminda):

Approval	
Approved by	Lidwien Morreel, Managing Director — Sabisu Consulting BV
Version	v2.3
Date of approval	5 November 2026
Signature	_____