

Salviminda

Sabisu Consulting BV · S-Link

Data Processing Agreement

Pursuant to Article 28 of Regulation (EU) 2016/679 (GDPR)

v1.1 (Draft) · 20 September 2026

DRAFT — PENDING LEGAL REVIEW

1. Parties

Data Controller: [Client company name], [registered address], [company registration number / VAT number] ("Controller").

Data Processor: Sabisu Consulting BV (trading as Salviminda), Leuvensesteenweg 280, 3200 Aarschot, Belgium, company number 1003.537.848, VAT BE 1003.537.848 ("Processor").

The Controller and the Processor are hereinafter individually referred to as a "Party" and jointly as the "Parties". This Data Processing Agreement ("DPA") is entered into pursuant to Article 28 of the GDPR and forms part of the agreement(s) governing the provision of the S-Link e-invoicing service by the Processor to the Controller ("Principal Agreement").

2. Definitions

"GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

"Personal Data", "Processing", "Controller", "Processor", "Data Subject", "Supervisory Authority", "Personal Data Breach" and "Sub-processor" have the meanings given to them in the GDPR.

"Services" means the Peppol e-invoicing, ERP integration and related services provided by the Processor under the Principal Agreement, including the S-Link connector and the S-Link Hub platform.

"Security Measures" means the technical and organisational measures set out in Schedule 2, as elaborated in the Processor's Information Security Policy, as each may be updated from time to time provided that the level of protection is not reduced. A copy of the Information Security Policy is available to the Controller on request.

"Sub-processor List" means the list of authorised Sub-processors in Schedule 3, as updated in accordance with clause 4(d).

3. Subject Matter, Nature, Duration and Purpose

3.1 The Processor shall process Personal Data on behalf of the Controller solely for the purpose of providing the Services, which comprises the automated transmission, routing, conversion, storage and deletion of electronic invoices and other business documents via the Peppol network and applicable national platforms, and the integration of such documents with the Controller's ERP system. Business documents processed through the Services, including their full content, are stored in the S-Link Hub platform operated by the Processor on Microsoft Azure in the West Europe region.

3.2 The Processor shall process Personal Data for the term of the Principal Agreement, unless applicable law requires further retention.

3.3 Schedule 1 to this DPA sets out a description of the processing activities, including the categories of Personal Data and Data Subjects.

3.4 In the event of any conflict between this DPA and the Principal Agreement in relation to the Processing of Personal Data, this DPA shall prevail.

4. Processor Obligations

The Processor agrees that, in relation to Personal Data processed on behalf of the Controller, it shall:

- (a) Process the Personal Data only on the documented instructions of the Controller, including with regard to transfers to a third country, unless required to do so by applicable EU or Member State law, in which case the Processor shall inform the Controller of that legal requirement before processing, unless prohibited from doing so by law. The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes the GDPR or other applicable data protection law;
- (b) Ensure that all persons authorised to process the Personal Data — employees, contractors and freelance professionals, in every location — are subject to binding obligations of confidentiality that survive the end of their engagement, or are under an appropriate statutory obligation of confidentiality, and receive data protection and security training at onboarding and at least annually;
- (c) Implement and maintain the Security Measures, ensuring a level of security appropriate to the risk in accordance with Article 32 GDPR;
- (d) Not engage a Sub-processor without the prior specific or general written authorisation of the Controller. Schedule 3 sets out the Sub-processors authorised by the Controller on signature of this DPA, and by signing the Controller grants general written authorisation for those Sub-processors. The Processor shall inform the Controller of any intended addition or replacement of a Sub-processor at least 30 days in advance, giving the Controller the opportunity to object on reasonable data-protection grounds within that period. Where the Controller objects and the Parties cannot agree an alternative, either Party may terminate the affected part of the Services in accordance with the Principal Agreement;
- (e) Ensure that any agreement with a Sub-processor imposes data protection obligations equivalent to those in this DPA, and remain fully liable to the Controller for the performance of that Sub-processor's obligations in accordance with Article 28(4) GDPR;
- (f) Taking into account the nature of the Processing, assist the Controller by appropriate technical and organisational measures in fulfilling its obligation to respond to requests from Data Subjects exercising their rights under Chapter III of the GDPR. Where the Processor receives such a request directly, it shall not respond to it on its own initiative but shall forward it to the Controller without undue delay;
- (g) Assist the Controller in ensuring compliance with obligations pursuant to Articles 32 to 36 of the GDPR (security, breach notification, data protection impact assessments and prior consultation), taking into account the nature of the Processing and the information available to the Processor;
- (h) At the choice and written direction of the Controller, upon termination or expiry of the Principal Agreement, return all Personal Data to the Controller in a commonly used, machine-readable format and delete existing copies, or delete all Personal Data, in each case within 90 days of that direction and unless Union or Member State law requires storage of such Personal Data. Deletion extends to backups in accordance with the Processor's backup cycle. The Processor shall confirm deletion in writing;
- (i) Make available to the Controller, on written request, all information necessary to demonstrate compliance with this Article and allow for and contribute to audits in accordance with clause 8;
- (j) Maintain a record of all categories of Processing carried out on behalf of the Controller in accordance with Article 30(2) GDPR, and make it available to the Controller or a Supervisory Authority on request;
- (k) Maintain a data protection contact point, currently privacy@salviminda.com, to which the Controller may address all notices and requests under this DPA.

5. Controller Obligations

5.1 The Controller warrants that it has a lawful basis for processing the Personal Data and that it has provided all required notices to, and obtained all required consents from, Data Subjects.

5.2 The Controller shall provide the Processor with documented instructions regarding the Processing and shall promptly notify the Processor of any changes to such instructions.

5.3 The Controller is responsible for ensuring that the Personal Data provided to the Processor is accurate, complete and relevant.

5.4 The Controller acknowledges the Sub-processors and processing locations set out in Schedule 3, including access to Personal Data from the Philippines as described in clause 7, and shall reflect them in its own record of processing activities and transfer documentation.

6. Security and Personal Data Breaches

6.1 The Processor shall notify the Controller without undue delay, and in any event within 48 hours of becoming aware, of any Personal Data Breach affecting Personal Data processed under this DPA.

6.2 The notification referred to in clause 6.1 shall include, to the extent then available: (i) a description of the nature of the breach, including the categories and approximate number of Data Subjects and Personal Data records concerned; (ii) the name and contact details of the Processor's data protection contact point; (iii) the likely consequences of the breach; and (iv) the measures taken or proposed to address the breach and mitigate its possible adverse effects. Where the information cannot be provided at the same time, it shall be provided in phases without further undue delay.

6.3 The Processor shall maintain a record of all Personal Data Breaches, including those not required to be notified to the Controller, and shall not notify a Supervisory Authority or Data Subjects on the Controller's behalf unless required by law or instructed to do so by the Controller.

7. International Data Transfers and Processing Locations

7.1 Personal Data at rest is stored within the European Union, in the Microsoft Azure West Europe region. The Processor does not replicate Personal Data at rest outside the European Union.

7.2 The Controller acknowledges and authorises that Personal Data is accessed remotely from the Philippines by freelance professionals engaged directly by the Processor as part of its delivery team, for development and support purposes, as set out in Schedule 3. The Philippines is not the subject of an adequacy decision of the European Commission. The Processor has therefore concluded Standard Contractual Clauses pursuant to Commission Implementing Decision (EU) 2021/914 with each such person, maintains a documented transfer impact assessment which it reviews at least annually, and applies the supplementary measures described in Schedule 2.

7.3 Save as set out in Schedule 3, the Processor shall not transfer Personal Data to, or make Personal Data accessible from, a country outside the European Economic Area without the prior written consent of the Controller and without an appropriate safeguard under Chapter V of the GDPR being in place.

7.4 The Processor shall make available to the Controller, on request, a copy of the transfer mechanisms relied upon under this clause and of its transfer impact assessment, with commercially confidential terms redacted.

8. Audit Rights

8.1 Upon at least 10 business days' prior written notice, the Controller (or a qualified third-party auditor appointed by the Controller, who shall be subject to confidentiality obligations and shall not be a competitor of the Processor) may audit the Processor's compliance with this DPA, no more than once per calendar year unless a Personal Data Breach affecting the Controller has occurred or a Supervisory Authority requires otherwise.

8.2 In the first instance, the Processor may satisfy a request under clause 8.1 by providing its Information Security Policy, its Sub-processor List, relevant supplier certifications and a completed security questionnaire. Where these do not reasonably satisfy the Controller, an on-site or remote audit shall proceed.

8.3 Audits shall be conducted during normal business hours, with minimum disruption to the Processor's operations, and shall not extend to the data or systems of other clients. The Controller shall bear its own costs of the audit and shall reimburse the Processor's reasonable costs in accordance with clause 9.

9. Assistance and Costs

9.1 Reasonable assistance under clauses 4(f), 4(g) and 8 is included in the fees payable under the Principal Agreement.

9.2 Where assistance is extensive, repeated, or requires effort materially beyond the ordinary course — including audits beyond the annual audit referred to in clause 8.1, and the handling of a significant volume of Data Subject requests — the Processor may charge its standard professional rates. The Processor shall notify the Controller of the expected cost and obtain written agreement before incurring it.

10. Liability

10.1 Each Party shall be liable for damage caused to a Data Subject by Processing which infringes the GDPR, to the extent and on the basis provided for in Article 82 GDPR.

10.2 Any administrative fine imposed under Article 83 GDPR shall be borne by the Party on which it is imposed, save to the extent that it results from the other Party's breach of this DPA.

10.3 The liability of each Party under this DPA is subject to any limitations of liability set out in the Principal Agreement, save where such limitation is not permitted by applicable law.

11. Duration and Termination

This DPA shall remain in force for the duration of the Principal Agreement and shall automatically terminate on the termination or expiry of the Principal Agreement, subject to any provisions that by their nature should survive termination, including clauses 4(b), 4(h), 9 and 10.

12. General

12.1 Any amendment to this DPA must be in writing and signed by both Parties, save that the Processor may update Schedule 2 and Schedule 3 in accordance with clauses 2 and 4(d).

12.2 If any provision of this DPA is held invalid or unenforceable, the remainder shall continue in full force and the Parties shall replace the affected provision with a valid one reflecting its purpose as closely as possible.

12.3 This DPA may be executed in counterparts and by electronic signature, each of which shall be an original and together shall constitute one agreement.

13. Governing Law and Jurisdiction

This DPA is governed by and construed in accordance with Belgian law. The Parties irrevocably submit to the exclusive jurisdiction of the courts of Leuven for any dispute arising out of or in connection with this DPA, without prejudice to any mandatory right of a Data Subject or Supervisory Authority to bring proceedings elsewhere.

14. Signatures

Signed for and on behalf of Sabisu Consulting BV (Data Processor):

Authorised signatory: _____

Name (print): _____

Title: _____

Date: _____

Signed for and on behalf of [Client Name] (Data Controller):

Authorised signatory: _____

Name (print): _____

Title: _____

Date: _____

Schedule 1 — Description of Processing

Element	Details
Subject matter	Provision of the S-Link Peppol e-invoicing and ERP integration service, including the S-Link Hub platform.
Duration	For the term of the Principal Agreement.
Nature	Automated collection, structuring, conversion, storage, transmission via the Peppol network and applicable national platforms, adaptation, retrieval and deletion of electronic business-document data; ERP system integration; support and troubleshooting.
Purpose	Enabling the Controller to send and receive electronic invoices compliant with the Peppol standard and applicable e-invoicing legislation.
Types of Personal Data	(i) Business contact details: name, business email, telephone number; (ii) Business-document content, which may include personal data of sole traders and individuals named on invoices: name, address, VAT or registration number, bank account details; (iii) User credentials: username, email, password hash, role; (iv) System and access logs: IP address, timestamp, user ID, actions performed.
Categories of Data Subjects	(i) The Controller's employees and authorised users; (ii) contact persons of the Controller's clients, customers and suppliers appearing on business documents; (iii) sole traders and freelancers whose invoices are processed through the Services.
Special categories	None. The Services are not intended to process data falling within Article 9 or Article 10 GDPR, and the Controller shall not submit such data through the Services.
Processing locations	Storage and processing at rest: European Union (Microsoft Azure, West Europe). Access: Belgium and the Philippines, as set out in Schedule 3.
Processing instructions	This DPA and the Principal Agreement constitute the Controller's documented instructions.

Schedule 2 — Technical and Organisational Measures

The Processor's Information Security Policy is provided to the Controller on request and elaborates on the measures summarised below. Measures currently in place include:

- All data in transit encrypted via TLS 1.2 or higher, with HTTPS enforced and weak ciphers disabled;
- All data at rest encrypted using platform-managed AES-256 encryption on cloud storage, databases and backups; full-disk encryption on all endpoints used for the Services;
- Multi-factor authentication required on all Processor accounts, in every location, including administrative and privileged access;
- Role-based access control and least-privilege principles; access granted on documented approval, reviewed quarterly and revoked on the last working day of any staff member or contractor;
- Named individual accounts for all access to client environments and to production; such access is logged, and logs are retained for 12 months and protected against tampering;
- Separate development, test and production environments; Controller production data is never copied into development or test environments, where anonymised or synthetic data is used;
- Credentials and API keys held exclusively in an approved secrets manager, never in e-mail, chat, tickets or source code, and rotated at least annually and immediately on suspected compromise or on the departure of anyone who held them;
- Security updates applied automatically or within 14 days of release; vulnerabilities prioritised by CVSS score and exposure, with remediation within 72 hours (critical), 14 days (high) and 30 days (medium); dependency vulnerabilities monitored and patched on the same timescales;
- Automated daily backups, encrypted and held in a geographically separate location within the European Union, with restore tests performed at least annually;
- Documented Personal Data Breach response procedure, with containment within 24 hours and Controller notification within 48 hours of becoming aware;
- Peppol AS4 protocol for secure, authenticated message exchange on the Peppol network;
- All personnel, in every location, bound by confidentiality undertakings surviving the engagement and trained on data protection and security at onboarding and at least annually;
- For access from outside the European Economic Area: Standard Contractual Clauses with each individual, time-limited and least-privilege access, logging of access, and a prohibition on storing Personal Data locally or in personal accounts.

Schedule 3 — Authorised Sub-processors

By signing this DPA, the Controller grants general written authorisation to the following Sub-processors. The Processor shall notify the Controller of any intended change at least 30 days in advance in accordance with clause 4(d).

Sub-processor	Purpose	Location	Transfer safeguard
Microsoft Ireland Operations Ltd	Cloud infrastructure for S-Link Hub: compute, database hosting, encrypted storage, logging and backup; Microsoft 365 for internal e-mail and document storage	European Union — Azure West Europe (Netherlands)	Within the EU. Microsoft Products and Services Data Protection Addendum (Art. 28); EU Data Boundary commitments
B2BRouter Global SL (B2BRouter), NIF B63276174, Barcelona	Peppol access point and French accredited platform: primary channel for transmission, conversion and archiving of business documents	European Union — Spain	Within the EU. Art. 28 DPA; ISO/IEC 27001 certified
Freelance professionals engaged directly by the Processor	Development and support work for the Services, involving remote access to client environments and to data held in S-Link Hub	Philippines (remote access to EU-hosted systems)	Standard Contractual Clauses (Implementing Decision (EU) 2021/914) with each individual; documented transfer impact assessment reviewed annually; supplementary measures per Schedule 2
Avalara Europe Ltd	Peppol access point: secondary channel, engaged only where the Controller contracts for it. Not currently active	United Kingdom	European Commission adequacy decisions for the United Kingdom, renewed 19 December 2025 and valid until 27 December 2031; Art. 28 DPA

Chorus Pro, operated by the Agence pour l'informatique financière de l'État, is not a Sub-processor. Where the Controller issues an invoice to a French public-sector body, transmission through Chorus Pro is required by French law and Chorus Pro acts as a recipient under that legal obligation.