SALVIMINDA

Data Processing Agreement

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

Sabisu Consulting BV, trading as Salviminda · Leuvensesteenweg 280, 3200 Aarschot, Belgium · BE 1003.537.848

Version 2.4 — approved 5 November 2026

1. Parties

Data Controller: the Client, as identified in the signed copy of this Agreement ('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').

This Data Processing Agreement ('DPA') is entered into pursuant to Article 28 GDPR and forms part of the agreement governing the provision of the S-Link e-invoicing service by the Processor to the Controller (the 'Principal Agreement').

2. Subject matter, nature, duration and purpose

2.1 The Processor processes personal data on behalf of the Controller solely to provide the Services, comprising the automated transmission, routing, conversion, storage and deletion of electronic invoices and other business documents via the Peppol network and applicable national platforms, and their integration 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.

2.2 Processing continues for the term of the Principal Agreement, unless applicable law requires further retention.

2.3 In the event of conflict between this DPA and the Principal Agreement in relation to the processing of personal data, this DPA prevails.

3. Processor obligations

In relation to personal data processed on behalf of the Controller, the Processor shall:

— process personal data only on the documented instructions of the Controller, including as regards transfers to a third country, unless required by EU or Member State law, and immediately inform the Controller if, in its opinion, an instruction infringes the GDPR or other applicable data protection law;

— ensure that all persons authorised to process the data — employees, contractors and freelance professionals, in every location — are bound by confidentiality obligations surviving the engagement, and receive data protection and security training at onboarding and at least annually;

— implement and maintain the technical and organisational measures described in the Technical and Organisational Measures document, ensuring a level of security appropriate to the risk in accordance with Article 32 GDPR;

— not engage a sub-processor without prior specific or general written authorisation. The authorised sub-processors are those published in the Sub-processor List; the Processor notifies the Controller of any intended addition or replacement at least 30 days in advance, with the opportunity to object on reasonable data-protection grounds;

— impose on each sub-processor data protection obligations equivalent to those in this DPA, and remain fully liable to the Controller for that sub-processor's performance in accordance with Article 28(4) GDPR;

— assist the Controller in responding to requests from data subjects under Chapter III GDPR, and forward to the Controller without undue delay any such request it receives directly, rather than responding to it on its own initiative;

— assist the Controller in complying with Articles 32 to 36 GDPR;

— at the Controller's choice and written direction, on termination or expiry, return all personal data 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, with deletion extending to backups in accordance with the backup cycle, and confirm deletion in writing;

— make available all information necessary to demonstrate compliance and contribute to audits in accordance with section 6;

— maintain a record of all categories of processing carried out on behalf of the Controller under Article 30(2) GDPR;

— maintain a data protection contact point, currently privacy@salviminda.com.

4. Controller obligations

4.1 The Controller warrants that it has a lawful basis for the processing and that it has provided all required notices to, and obtained all required consents from, data subjects.

4.2 The Controller provides documented instructions regarding the processing and promptly notifies the Processor of changes to them.

4.3 The Controller is responsible for ensuring that the personal data provided is accurate, complete and relevant.

4.4 The Controller acknowledges the sub-processors and processing locations set out in the Sub-processor List, including access to personal data from the Philippines as described in section 7, and reflects them in its own record of processing activities and transfer documentation.

5. Security and personal data breaches

5.1 The Processor notifies 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.

5.2 The notification includes, so far as available: the nature of the breach, including the categories and approximate number of data subjects and records concerned; the name and contact details of the Processor's

data protection contact point; the likely consequences; and the measures taken or proposed. Where the information cannot be provided at once, it is provided in phases without further undue delay.

5.3 The Processor maintains a record of all personal data breaches, including those not notified to the Controller, and does not notify a supervisory authority or data subjects on the Controller's behalf unless required by law or instructed by the Controller.

6. International transfers and processing locations

6.1 Personal data contained in business documents processed through the Services is stored within the European Union, in the Microsoft Azure West Europe region, and is not replicated at rest outside the European Union. Personal data submitted by Controller users in support tickets is at present held in the Processor's internal ticket application, which is hosted in the United States; the Processor is withdrawing such data from that application and is redeploying it to the Processor's own Microsoft Azure environment within the European Union by 31 January 2027, after which the data is reachable only through the application and administrative access to the environment is restricted to system administrators located in the European Union. The transfer safeguards applicable in the meantime are set out in the Sub-processor List. Where a Purchase Order or amendment records that Personal Data processed on behalf of the Controller is not to be processed outside the European Union, the Processor does not use the ticket application for that Controller until the redeployment is complete.

6.2 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. 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 reviewed at least annually, and applies the supplementary measures described in the Technical and Organisational Measures.

6.3 Save as set out in the Sub-processor List, the Processor shall not transfer personal data to, or make it accessible from, a country outside the European Economic Area without the Controller's prior written consent and an appropriate safeguard under Chapter V GDPR.

6.4 The Processor makes available, on request, a copy of the transfer mechanisms relied upon and of its transfer impact assessment, with commercially confidential terms redacted.

6.5 Where the Controller contracts directly with a transmission platform provider, the Controller instructs the Processor to transmit personal data to, and retrieve it from, that provider. The Controller is responsible for the lawfulness of that transmission, including any transfer outside the European Economic Area, and for the data protection terms of its own agreement with that provider. The Processor transmits only to the provider and destination identified in the Purchase Order, and such a provider is not a sub-processor of the Processor.

7. Audit rights, assistance and costs

7.1 The Controller may audit the Processor's compliance with this DPA. The Controller is not required to state or justify a reason for an audit.

7.2 An audit may be conducted by the Controller or by a qualified third-party auditor appointed by the Controller, who shall be bound by obligations of confidentiality and shall not be a competitor of the Processor.

7.3 The Controller shall give at least ten calendar days' written notice of an audit, or five calendar days' notice where the audit follows a personal data breach or is required by a supervisory authority.

7.4 Audits may be conducted once per calendar year. This limit does not apply where a personal data breach affecting the Controller has occurred, where a supervisory authority requires an audit, or where a previous audit identified material non-compliance that has not been remedied.

7.5 The Processor shall make available to the Controller, on request and without charge, its Information Security Policy, its Technical and Organisational Measures, its Sub-processor List, relevant supplier certifications and completed security questionnaires. The Controller may accept such documentation in satisfaction of an audit request; that decision rests with the Controller alone.

7.6 Audits shall be conducted during normal business hours and with reasonable regard for the continuity of the Processor's operations. An audit shall not extend to the data, systems or tenants of other clients of the Processor.

7.7 Each party bears its own costs in respect of the annual audit under clause 7.4. The Processor's reasonable costs in respect of any additional audit are for the Controller's account, save where the audit identifies material non-compliance by the Processor, in which case the Processor bears its own costs.

7.8 Reasonable assistance under sections 3 and 7 is included in the fees payable under the Principal Agreement. Where assistance is extensive, repeated or requires effort materially beyond the ordinary course — including the handling of a significant volume of data subject requests — the Processor may charge its standard professional rates, notified and agreed in writing in advance.

8. Liability, duration and governing law

8.1 Each party is 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. Any administrative fine under Article 83 GDPR is borne by the party on which it is imposed, save to the extent it results from the other party's breach of this DPA.

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

8.3 This DPA remains in force for the duration of the Principal Agreement and terminates automatically on its termination or expiry, subject to provisions that by their nature survive.

8.4 This DPA is governed by Belgian law. The parties submit to the exclusive jurisdiction of the courts of Leuven, without prejudice to any mandatory right of a data subject or supervisory authority to bring proceedings elsewhere.

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 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	Business contact details (name, business email, telephone); 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); user credentials (username, email, password hash, role); system and access logs (IP address, timestamp, user ID, actions performed).
Categories of data subjects	The Controller's employees and authorised users; contact persons of the Controller's clients, customers and suppliers appearing on business documents; sole traders and freelancers whose invoices are processed.
Special categories	None. The Services are not intended to process data falling within Article 9 or 10 GDPR, and the Controller shall not submit such data.
Processing locations	Storage and processing at rest: European Union (Microsoft Azure, West Europe). Access: Belgium and the Philippines.
Processing instructions	This DPA and the Principal Agreement constitute the Controller's documented instructions.