DATA PROCESSING AGREEMENT

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

InvoicePeppol

Operated by New Start Enterprises

https://invoicepeppol.com

Version 1.0 — April 2026

1. Preamble

This Data Processing Agreement (**"DPA"**) forms part of the Terms of Service between InvoicePeppol, operated by New Start Enterprises (**"Processor"** or **"we"**), and the entity or individual using the InvoicePeppol service (**"Controller"** or **"you"**).

This DPA governs the processing of personal data by the Processor on behalf of the Controller in connection with the InvoicePeppol service, in accordance with Article 28 of the General Data Protection Regulation (EU) 2016/679 ("GDPR").

By using InvoicePeppol, you accept this DPA. If you are entering into this DPA on behalf of an organization, you represent that you have authority to bind that organization.

2. Definitions

"Personal Data" means any information relating to an identified or identifiable natural person contained within the invoice files you upload or the account information you provide.

"Processing" means any operation performed on Personal Data, including collection, storage, retrieval, use, transmission, erasure, or destruction.

"Sub-processor" means any third party engaged by the Processor to process Personal Data on behalf of the Controller.

"Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data.

3. Scope and Purpose of Processing

The Processor processes Personal Data solely for the purpose of providing the InvoicePeppol service, which includes:

- Extracting structured data from uploaded PDF invoices using AI-assisted document processing
- Generating EN 16931 compliant XML output files (Peppol BIS 3.0, XRechnung, ZUGFeRD, Factur-X)
- Maintaining user accounts and authenticating access
- Processing payments for the service

The categories of Personal Data processed and data subjects concerned are detailed in Annex 1.

4. Processor Obligations

The Processor shall:

- Process Personal Data only on documented instructions from the Controller, including with respect to transfers of Personal Data to a third country, unless required to do so by EU or Member State law
- Ensure that persons authorised to process the Personal Data have committed themselves to confidentiality
- Implement appropriate technical and organisational measures as described in Annex 2
- Respect the conditions for engaging Sub-processors as set out in Section 6
- Assist the Controller, taking into account the nature of processing, in responding to requests for exercising data subject rights under Chapter III of the GDPR
- Assist the Controller in ensuring compliance with obligations under Articles 32 to 36 of the GDPR, taking into account the nature of processing and the information available to the Processor
- At the choice of the Controller, delete or return all Personal Data after the end of the provision of services, and delete existing copies unless EU or Member State law requires storage
- Make available to the Controller all information necessary to demonstrate compliance with Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller

5. Controller Obligations

The Controller shall:

- Ensure it has a lawful basis for providing Personal Data to the Processor
- Ensure that data subjects have been informed of the processing in accordance with Articles 13 and 14 of the GDPR
- Be responsible for the accuracy, quality, and legality of Personal Data provided to the Processor
- Review and verify all extracted data and generated XML output before submission to any tax authority, Peppol network, or business partner

6. Sub-processors

6.1 Authorised Sub-processors

The Controller provides general authorisation for the Processor to engage the Sub-processors listed in Annex 3. The Processor shall inform the Controller of any intended changes concerning the addition or replacement of Sub-processors, giving the Controller the opportunity to object to such changes within 30 days.

6.2 Sub-processor Obligations

Where the Processor engages a Sub-processor, the Processor shall impose on that Sub-processor, by way of contract, the same data protection obligations as set out in this DPA. The Processor shall remain fully liable to the Controller for the performance of that Sub-processor’s obligations.

7. International Data Transfers

Certain Sub-processors process Personal Data outside the European Economic Area (EEA). Where such transfers occur, the Processor ensures that appropriate safeguards are in place in accordance with Chapter V of the GDPR, including:

- Standard Contractual Clauses (SCCs) as adopted by the European Commission, where the recipient is established in a country without an adequacy decision
- Supplementary measures where required, such as encryption of data in transit and contractual commitments regarding government access requests

The specific transfer mechanisms applicable to each Sub-processor are detailed in Annex 3.

For clarity: invoice file content is transmitted to AI processing Sub-processors solely for the purpose of data extraction. This data is processed transiently and is not stored by the Sub-processor beyond the duration of the API request.

8. Security Measures

The Processor implements the technical and organisational measures described in Annex 2. These measures are designed to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing.

The Processor shall regularly review and update these measures as necessary to maintain appropriate protection.

9. Data Breach Notification

The Processor shall notify the Controller without undue delay, and in any event within 72 hours, after becoming aware of a Data Breach affecting the Controller’s Personal Data. The notification shall include:

- A description of the nature of the Data Breach, including the categories and approximate number of data subjects and records concerned
- The name and contact details of the Processor’s contact point
- A description of the likely consequences of the Data Breach
- A description of the measures taken or proposed to address the Data Breach, including measures to mitigate its possible adverse effects

10. Data Subject Rights

The Processor shall assist the Controller in fulfilling its obligations to respond to data subject requests under the GDPR, including rights of access, rectification, erasure, restriction of processing, data portability, and objection.

Given the transient nature of invoice processing (files are deleted immediately after conversion), the Processor’s ability to fulfil certain requests with respect to invoice content may be limited. Account data (email address, billing history) can be provided, rectified, or deleted upon verified request to security@invoicepeppol.com.

11. Audit Rights

The Controller has the right to conduct audits, including inspections, to verify the Processor’s compliance with this DPA. Audits shall be conducted with reasonable prior notice (at least 30 days), during normal business hours, and in a manner that does not unreasonably disrupt the Processor’s operations.

The Processor may satisfy audit requests by providing relevant certifications, audit reports, or documentation demonstrating compliance, where available and sufficient.

12. Data Retention and Deletion

12.1 Invoice Data

Uploaded PDF files and generated XML files are processed transiently in memory. Invoice content is not written to permanent storage and is deleted immediately upon completion of the conversion session. No invoice data is retained on our servers.

12.2 Account Data

Account information (email address, hashed password, billing records) is retained for as long as the account remains active and for the period required by applicable law thereafter. Upon account deletion or termination, all associated data is permanently removed within 30 days, except where retention is required by law (e.g. tax and accounting records).

12.3 Deletion Request

You may request deletion of your account and all associated data at any time by contacting security@invoicepeppol.com. We will process your request within 30 days.

13. Term and Termination

This DPA shall remain in effect for the duration of your use of the InvoicePeppol service. Upon termination or expiry of the service, the provisions of Section 12 (Data Retention and Deletion) shall apply.

Sections that by their nature should survive termination shall remain in effect, including obligations relating to confidentiality, data deletion, and liability.

14. Liability

The liability of each party under this DPA is subject to the limitations and exclusions of liability set out in the Terms of Service. Nothing in this DPA limits either party’s liability for breaches of the GDPR to the extent such limitation is not permitted under applicable law.

15. Governing Law and Jurisdiction

This DPA shall be governed by Belgian law. Any disputes arising under this DPA shall be submitted to the courts of Brussels, Belgium, consistent with the Terms of Service.

16. Contact

For any questions or requests relating to this DPA, contact:

InvoicePeppol — New Start Enterprises

Email: security@invoicepeppol.com

Website: https://invoicepeppol.com

Annex 1: Details of Processing

Categories of Data Subjects

- Employees, contractors, or representatives of the Controller whose names or contact details appear on invoices
- Customers, suppliers, or business partners of the Controller identified in invoices

- The Controller’s own representatives who create accounts on the service

Categories of Personal Data

- Invoice content: names, business addresses, email addresses, phone numbers, VAT identification numbers, IBAN/BIC bank details, and any other personal data present in uploaded PDF invoices
- Account data: email address, hashed password, authentication tokens
- Billing data: payment transaction references (handled by Razorpay; we do not store card details)
- Technical data: IP addresses and session identifiers (for security and rate limiting)

Purpose of Processing

- Extraction of structured data from PDF invoices for conversion to EN 16931 compliant XML
- User authentication and account management
- Payment processing and billing
- Service security and abuse prevention

Duration of Processing

Invoice content: transient only (seconds to minutes per conversion, immediately deleted). Account and billing data: duration of the account plus legal retention periods.

Annex 2: Technical and Organisational Measures

Encryption

- All data in transit is encrypted using TLS 1.3 (HTTPS enforced via HSTS)
- Payment data is handled entirely by Razorpay (PCI DSS Level 1 certified); we never see or store card details
- Passwords are stored using industry-standard one-way hashing algorithms

Access Control

- Server access is restricted to authorised personnel via SSH key authentication
- Principle of least privilege applied to all internal systems and tools
- Session cookies are Secure, HttpOnly, with automatic expiry after 24 hours

Application Security

- CSRF protection on all forms and state-changing requests
- Rate limiting on upload and authentication endpoints
- File validation: type, size, and content verification on all uploads
- Input sanitisation on all user inputs
- Content Security Policy (CSP) headers enforced

Infrastructure Security

- EU-based hosting (Frankfurt, Germany) on dedicated VPS infrastructure
- Cloudflare provides DDoS protection, WAF, and edge security
- Nginx reverse proxy with hardened configuration
- Application-level logging and monitoring for anomalous activity

Data Minimisation

- Invoice files are processed in memory and never written to permanent storage
- Generated XML files are available for immediate download and then deleted
- We collect only the minimum account data necessary to provide the service

Incident Response

- Defined breach notification procedure (within 72 hours)
- Responsible disclosure programme (security@invoicepeppol.com)

Annex 3: Authorised Sub-processors

The following Sub-processors are authorised to process Personal Data on behalf of the Controller:

Sub-processor	**Purpose**	**Data Processed**	**Location**	**Transfer Mechanism**
Vultr (The Constant Company)	VPS hosting and application infrastructure	Account data, technical data, transient invoice content	Frankfurt, Germany (EU)	N/A (EU)
Cloudflare, Inc.	CDN, DDoS protection, DNS, and edge security	IP addresses, request metadata	Global edge network (EU primary)	EU SCCs + DPF
Anthropic (Claude API)	AI-assisted data extraction from invoice PDFs	Transient invoice content (text only, not stored)	United States	EU SCCs
Razorpay Software Pvt. Ltd.	Payment processing and billing	Email, payment transaction data (no card details stored by us)	India	EU SCCs
Brevo (Sendinblue)	Transactional email delivery	Email addresses	EU (France)	N/A (EU)

The Processor will notify the Controller at least 30 days in advance of any intended changes to this list. The Controller may object to any new Sub-processor within that period. If the objection is not resolved, the Controller may terminate the service.

For Sub-processors located outside the EEA, Standard Contractual Clauses (SCCs) as adopted by the European Commission (Decision 2021/914) are in place. Invoice content sent to AI processing Sub-processors is transmitted via encrypted channels, processed transiently for the sole purpose of data extraction, and is not retained by the Sub-processor.