CONTRACTS · DATA PROCESSING AGREEMENT (DPA)

Data Processing Agreement (DPA)

version v1.6 · effective from 2 October 2026

Data processing agreement under Art. 28 GDPR which we conclude with customers and partners. The facts (sub-processors, retention periods, transfers) match the real operation and the privacy notice at /gdpr. This is the binding wording in which we conclude the contract (in its Slovak version); fields marked [•] are completed with identification data at signature. Conclusion or individual adjustments: peppol@verteco.digital.

Informative translation. Only the Slovak wording is legally binding (General Terms, art. 21). In case of any discrepancy the Slovak text prevails. Open the Slovak version

DATA PROCESSING AGREEMENT (DPA)
under Art. 28 of Regulation (EU) 2016/679 (GDPR) and Act No. 18/2018 Coll.

Controller (Customer):
[business name / first name and surname], Company ID (IČO) [•], registered office / place of business [•],
registered in [register / not applicable] (hereinafter the "Controller")

Processor:
Verteco digital services, s. r. o., Company ID (IČO) 53 412 834, Tax ID (DIČ) 2121358349, VAT ID SK2121358349,
Daniela Dlabača 21, 010 01 Žilina, registered in the Commercial Register of the District Court Žilina, section Sro,
file no. 75936/L (hereinafter the "Provider")

Preamble: The Provider provides the Controller with the service of a certified Peppol Access Point and of a delivery service provider (PA SK ID EFSK000031), including the portal, the API and related services (hereinafter the "Service"). In providing the Service, the Provider processes personal data on behalf of the Controller; this agreement governs the terms of that processing.

Conclusion of the agreement: This agreement is concluded between the Controller and the Provider
at the moment the contractual relationship concerning the Service arises, by reference in the General
Terms and Conditions (Art. 13 of the General Terms), in the wording published at peppol.verteco.digital/zmluvy/dpa as at the day the relationship arises. The identification fields [•] serve only for identification upon individual signature; leaving them blank has no

effect on the validity of the agreement concluded by reference, the parties being identified by the
account and company data in the Service. An individually signed copy prevails in case of conflict.

Art. 1: Subject matter and duration of processing

1.1 The Provider processes personal data exclusively for the purpose of providing the Service, for the duration of the contractual relationship established by the General Terms or, as the case may be, by the Intermediary Terms and Conditions.

1.2 After the contractual relationship ends, the Provider shall, at the Controller's choice, return the personal data (original XML of the documents + CSV export to the extent the Provider holds them as at the day of the request), delete them, or both; it issues a confirmation of deletion on request. The export is free of charge and in machine-readable form. If the Controller does not make the choice within 90 days of the end of the relationship (Art. 16 of the General Terms), the Provider deletes the data. If the Controller has the Data archive switched off for received or issued documents (the maximum encryption mode under Art. 11a of the General Terms, set separately for each direction), the content of such documents is already deleted continuously and irreversibly during the relationship according to the Controller's setting; in such a case the obligation to return applies only to data that have not been deleted in this way.

The obligations under this point do not apply to the extent that Union or Slovak law or the binding Peppol framework requires the Provider to retain data further (in particular tax reports and records under Act No. 385/2025 Coll. and the Peppol framework, the Provider's own accounting documents under Act No. 431/2002 Coll. and security records under Art. 5.1); the obligations of this agreement apply to data so retained until their deletion.

Art. 2: Nature, purpose and categories of processing

2.1 Nature of processing: receiving, sending, validating, storing and making available electronic invoices and related documents in the Peppol network; notifications (e-mail, webhook);

generation of tax reports for the Financial Administration of the Slovak Republic (C5/TDD) to the extent
of legal obligations.
2.2 Categories of data subjects: statutory representatives, employees and contact persons of the
Controller, of its customers and suppliers; users of the portal.
2.3 Categories of data: identification and contact data (name, e-mail, telephone), invoicing
data including the content of documents (line items, amounts, IBAN, Tax ID/Company ID identifiers),
account login credentials, technical logs (IP address, user agent). Special categories of data
(Art. 9 GDPR) are not the subject of the Service and the Controller undertakes not to enter them into
the Service.

Art. 3: Instructions of the Controller
3.1 The Provider processes personal data only on documented instructions of the Controller; the use of the Service (portal, API, notification configuration), the Data archive
setting and the enabling of document links without login under Art. 11b of the General Terms (including
the issuing of every such link) and this agreement are also deemed documented instructions. This does
not apply where processing is required by Union or Slovak law; in such a case the Provider shall inform
the Controller of that requirement before processing, unless that law prohibits such information.
3.2 The documented instructions under Art. 3.1 also cover transfers of personal data to a
third country or an international organisation (Art. 28 para. 3 point (a) GDPR).
3.3 If the Provider considers an instruction to infringe the GDPR, it shall inform the Controller
thereof without delay.
3.4 The Controller declares and is responsible for ensuring that the personal data it enters into the
Service are obtained and provided in compliance with the GDPR (in particular that it has a legal basis
and has fulfilled its information obligations towards the data subjects) and that its instructions
comply with the law.

If, as a result of a breach of these obligations of the Controller or as a result of an unlawful
instruction, a sanction is imposed on the Provider or the Provider suffers damage, the Controller shall
compensate it; recourse claims under Art. 82 para. 5 GDPR remain unaffected.

Art. 4: Confidentiality
The Provider shall ensure that persons authorised to process the personal data have committed
themselves to confidentiality or are under a statutory obligation of confidentiality.

Art. 5: Security of processing (Art. 32 GDPR)
5.1 The Provider has adopted and maintains appropriate technical and organisational measures
corresponding to the risk of the processing (Art. 32 GDPR), as at the effective date of this wording
in particular: encryption of transfers (TLS), encryption and signing of messages in the Peppol network
(AS4, OpenPeppol PKI certificates), access management on the principle of least privilege including
regular review of administrator access, separate production and test environments, a security log of access and events (365-day retention), monitoring of errors and availability with a public status at /status, regular backups of the managed database and application hardening (fail-closed authorisation gates). The Provider develops the
measures continuously (the implementation of an information security management system under
ISO/IEC 27001 is under way with the aim of certification in 2027); it provides their current
overview on request. A change to an individual measure is not a breach of this agreement if the
overall level of security does not decrease.
5.2 The Service's data are hosted in the EU (DigitalOcean, Frankfurt region).
5.3 The obligations under Art. 4, Art. 5 and Art. 8.3 continue for as long as the Provider retains
personal data, including after this agreement ends.
5.4 Document links without login (Art. 11b of the General Terms) are a departure from the principle of
least privilege which the Controller enables and uses on its own instruction. For such links the
Provider ensures: a random key bound to a single document, storage of its fingerprint

only, limited
validity, immediate revocation individually and in bulk, a record of every access (time, IP address)
and the exclusion of caching and indexing. The Controller is responsible for disclosure of content to a
person who obtained the link outside the Provider's environment; the Provider's notification
obligation under Art. 33 para. 2 GDPR in the event of an incident within its environment remains
unaffected.

Art. 6: Sub-processors
6.1 The Controller grants a general authorisation for the engagement of sub-processors.
Current list as at the date of signature:

- DigitalOcean LLC: cloud infrastructure, Frankfurt region (EU)
- Brevo (Sendinblue SAS), France: transactional e-mails
- Sentry (Functional Software, Inc. / Sentry GmbH): error monitoring, EU data region (Germany)
- Anthropic PBC, USA: language model for the AI functions of the Service (chat assistant and preparation of draft replies to enquiries and support tickets)
- Websupport, s. r. o., Slovakia: e-mail sending infrastructure (SMTP server)
- Cloudflare, Inc.: bot and DDoS protection to the technically necessary extent

In the processing of card payments (prepaid credit top-ups, the intermediary listing fee), Stripe Payments Europe, Ltd. acts as an independent controller and is not a sub-processor under this agreement.
6.2 The Provider shall give notice of the engagement of a new or the replacement of an existing
sub-processor at least 30 days in advance, by e-mail to the account's contact address and
simultaneously by publication at /gdpr. If the Controller raises a reasoned objection within that
period and no solution is found, it is entitled to terminate the agreement on the Service without sanction as at the effective date of the change.
6.3 The Provider shall impose on every sub-processor, by contract, data protection obligations
equivalent to those in this agreement and is liable for the performance of its obligations.

Art. 7: Transfers to third countries
Processing takes place primarily in the EU/EEA. For sub-processors established in the

USA
(Anthropic; the parent companies of DigitalOcean, Cloudflare, Sentry), any transfer takes place on the basis of an adequacy decision (EU-U.S. Data Privacy Framework) or, as the case may be, standard contractual clauses (SCC) with supplementary measures.

Art. 8: Assistance
8.1 Taking into account the nature of the processing, the Provider shall assist the Controller
in fulfilling its obligations towards data subjects (Art. 12 to 23 GDPR) by appropriate technical means (exports, access to documents via the portal and the API, account deletion).
8.2 The Provider shall assist in ensuring compliance with Art. 32 to 36 GDPR (security, breach notification, impact assessment), taking into account the information available to it. Assistance beyond the ordinary operation of the Service (in particular extensive
extracts and analyses, participation in an impact assessment, assistance with an audit under Art. 9)
is provided against reimbursement of reasonably incurred costs at the usual rate.
8.3 The Provider shall notify the Controller of a personal data breach without undue delay after becoming aware of it, as a rule within 72 hours of that
moment, with a description of the nature of the breach, its likely consequences and the measures
taken or proposed; the information may be provided in phases as it becomes available.

Art. 9: Audit
9.1 The Provider shall make available to the Controller the information necessary to demonstrate
compliance with the obligations under Art. 28 GDPR and shall allow for audits, including inspections, conducted by the Controller or an auditor mandated by it.
9.2 An audit is conducted upon written notice given at least 30 days in advance, during working
hours, at most once a year (this does not apply after a security incident or on the instruction of a
supervisory authority), in a manner that does not unreasonably disrupt operations, and with
protection of the confidential information of the Provider and of third parties (the auditor may not
be a competitor of the Provider and shall sign a confidentiality undertaking). The costs of the audit,
including the Provider's reasonably incurred costs of assistance, are borne by the

Controller.
9.3 The Provider may also fulfil the obligation under Art. 9.1 by making available current reports, certifications or a completed security questionnaire if they adequately demonstrate
compliance; an on-site audit is in that case conducted only if those documents are reasonably insufficient.

Art. 10: Final provisions
10.1 This agreement is an integral part of the contractual relationship concerning the Service; in
case of conflict, this agreement prevails in matters of personal data protection. Stricter obligations of the Provider, or obligations more favourable to the Controller, agreed in the
Intermediary Terms and Conditions or individually (in particular the 48-hour deadline for notifying
a personal data breach and the 45-day advance notice period for sub-processors) are not in conflict
with this agreement and prevail over its general wording. The Parties' liability for damage
is governed by the agreement on the Service, including any agreed limitation of compensation for
damage; this is without prejudice to the mandatory provisions of the GDPR on liability towards data
subjects.
10.2 The Provider may amend the wording of this agreement for agreements concluded by reference under
the same regime as the General Terms: by notice at least 30 days before the change takes effect
(e-mail + /zmluvy); if the Controller does not agree with the change, it may terminate the contractual
relationship concerning the Service as at the effective date of the change without sanction. The
Provider makes previous versions of the wording available on request.
10.3 The agreement is governed by the law of the Slovak Republic. It ends upon the end of the
contractual relationship concerning the Service; Art. 1.2, Art. 4, Art. 5 and Art. 8.3 survive its
end to the extent set out in Art. 5.3.

Art. 11: Relationship between processor and further processor (Art. 28 para. 4 GDPR)
11.1 If the Customer uses the Service as a processor for its own clients

(controllers), in particular as an Intermediary under the Intermediary Terms and Conditions, the Provider acts in the position of a further processor under Art. 28 para. 4 GDPR (in commercial practice also referred to as a sub-processor; sub-processors under Art. 6 of this agreement means the Provider's suppliers). The processing chain is thus as follows: the Customer's client is the controller, the Customer is the processor and the Provider is the further processor. In such a case this agreement applies mutatis mutandis so that the rights and obligations of the Controller under this agreement are exercised by the Customer as processor in its own name, for the benefit of and on the documented instructions of its controllers; no separate document is required, and at the Customer's request the parties shall also conclude a separate signed copy.

11.2 The Customer in the position of processor declares and is responsible for ensuring that the instructions it gives to the Provider are covered by the instructions and legal basis of its controllers and by its contracts under Art. 28 para. 3 GDPR; Art. 3.4 applies accordingly. The Provider performs the obligations under this agreement (including notification of breaches, notification of sub-processors, assistance and audit) towards the Customer; towards the Customer's controllers the Customer performs them itself.

11.3 The deadlines agreed in the Intermediary Terms and Conditions (notification of a personal data breach within 48 hours of detection, notice of the engagement of a new sub-processor at least 45 days in advance with a right of objection) apply to this relationship instead of the general deadlines under Art. 6.2 and Art. 8.3 of this agreement.

11.4 For personal data that the Provider processes to fulfil its own statutory obligations or for its own legitimate purposes, the Provider acts as an independent controller. These are exclusively the following purposes: (a) tax reports and related records under Act No. 385/2025 Coll. and the binding Peppol framework, including mandatory reports to the Peppol authority and the coordinating authority of the Peppol network; (b) security records and records of access and events under Art. 5.1; (c) invoicing of the Provider's services and keeping its own accounting and tax documents under Act No. 431/2002 Coll.; (d) the assertion and defence of the Provider's legal claims. This list is exhaustive;

its extension is an amendment of this agreement under Art. 10.2. The Provider is responsible for
processing under this point as controller and does not pass on to the Customer a sanction imposed on
it for such processing; this does not apply to the extent that its cause was a breach of the
Customer's obligations, the inaccuracy of data provided by it, its unlawful instruction or the content
of its clients' documents. Art. 3.4, Art. 11.2 and recourse claims under Art. 82 para. 5 GDPR
remain unaffected.

11.5 The position of independent controller under Art. 11.4 does not extend to the content of
the transmitted documents: in relation to it the Provider always acts only in the position under
Art. 11.1, and the Customer's client as controller is responsible for the accuracy, completeness and
lawfulness of the content of the documents. Processing under Art. 11.4 does not give the Provider the
right to use personal data processed for the Customer for other purposes; the Provider does not use
them for its own marketing purposes, for profiling or for training machine learning models.

11.6 The allocation of roles under this article is declaratory and applies exclusively for the
purposes of the GDPR. The position of the parties is determined by the actual influence over the
purposes and means of processing; if the nature of a specific processing operation reveals a
different position, the GDPR applies and the parties shall adjust the wording without undue delay so
that it corresponds. The allocation of roles has no effect on the scope of the parties' obligations
and liability under the Intermediary Terms and Conditions, in particular under their Art. 4 and
Art. 5, and does not establish liability of the Provider for sanctions, costs or claims caused by
the conduct of the Customer, its customers or the content of their documents. At the Customer's
request the Provider shall provide it free of charge with a written statement on the

allocation of
roles under this article so that it can present it to its controllers.

In ....., on .....

Controller: ..... Provider: .....