LEGAL

Personal Data Processing Policy

Effective from 16 November 2026

This policy describes the processing of personal data by Verteco digital services, s. r. o. in operating the Verteco Peppol portal and providing Peppol services, in accordance with Regulation (EU) 2016/679 of the European Parliament and of the Council (hereinafter the "**GDPR**") and Act No. 18/2018 Coll. on the Protection of Personal Data (hereinafter the "**Act**").

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

1. Controller and contact details

Verteco digital services, s. r. o.

with registered office at Daniela Dlabača 21, 010 01 Žilina, Slovak Republic; Company ID (IČO): 53412834, VAT ID (IČ DPH): SK2121358349

registered in the Commercial Register of the District Court Žilina, section: Sro, file no. 75936/L

Peppol Seat ID: PSK001128

contact person: Mgr. Miriama Mrkávková, peppol@verteco.digital, +421 944 488 269

(hereinafter the "**Controller**"). The Controller has not appointed a data protection officer (DPO), as this obligation does not arise for it from the Act/GDPR; for data protection matters please use the contact above.

2. Categories of data subjects

- registered users (account holders);
- contact and authorised persons of the managed companies;
- natural persons listed as senders, recipients or contacts in the exchanged documents.

3. Categories and sources of personal data

- **Account data:** e-mail address, password hash, date of registration and e-mail verification, account status.

- **Company data:** Company ID (IČO), VAT ID (IČ DPH), business name, registered office, Peppol participant identifier.
- **Document data (metadata):** sender/recipient identifiers, document number and date, amount, currency, delivery status; the substantive content of the documents to the extent necessary for their transmission through the Peppol network.
- **Technical and operational data:** IP address, timestamps, token identifiers, access and operation logs.
- **Security log (audit):** for refused, failed or restricted requests, for changes of data and for access to sensitive data we record the IP address, the time, the interface address used, the result, the browser identification (user-agent) and the e-mail of the account concerned (for a failed login, the e-mail that was entered). It serves solely to protect the Service against abuse and to investigate security incidents; we keep it for at most 12 months, after which it is deleted automatically.
- **Registration check:** when an account is created we determine the country from the IP address using a table stored in our system (DB-IP.com data, CC BY 4.0 licence; the IP address is not sent anywhere in the process). A registration from a country outside the EU/EEA, Switzerland and the United Kingdom, or an unusual number of registrations from one address, leads to a manual verification of the account (by telephone or e-mail); we keep the reason and the result of the verification in the security log.
- **Messages from the contact form and support tickets** (including e-mails delivered to peppol@verteco.digital, from which a ticket bound to the sender’s address is created automatically): name, e-mail and the content of the message; to prepare a reply they may be processed by the AI sub-processor Anthropic; a simple first question may be answered directly by our assistant using artificial intelligence without a person checking the reply beforehand (by replying to such a message you reach a colleague), other replies are written or approved by a person; we keep them while the matter is being handled and subsequently for at most 24 months for the purposes of follow-up support. A sender without an account receives a confirmation with a link that gives access only to their one request (the link is intended for them alone); we record every opening of the link in the security log with the IP address (see below).
- **Phone calls to our support line** (+421 222 200 067): the caller's number, the time, duration and outcome of the call, who spoke, and for a recorded call its recording, its transcript and a short summary (name, company, contact and request as stated). Callers are told about the recording at the start of the call; the call may be answered by an automated voice assistant, which introduces itself as such. The transcript and summary are kept as a support record for at most 24 months; the recording is kept by the telephony provider under our setting for at most 12 months.
- **Subscription to service changes (changelog):** e-mail address and the chosen areas (e.g. API, webhooks) based on your sign-up on the /changelog page; we process them only to send notices about changes to the service. We add the address only after confirmation via

the link in the e-mail (double opt-in); we delete an unconfirmed sign-up after 30 days, and every message contains an unsubscribe link that deletes the record.

- **Tips and reminders for users:** after a company is activated we send the account owner a few short e-mails (first steps, a feedback question after three weeks, an overview after six weeks), and accounts whose activation is not finished get a reminder of the selection on the Financial Administration portal. Every such e-mail carries an unsubscribe link, which we remember for that address (a table of opt-outs with no further data); the same setting is in the account under Notifications. Operational messages (received invoices, delivery receipts, account security, payments) are not affected by unsubscribing; they are part of the service.
- **Messages from the chat assistant ("Pepo"):** the content of questions and answers including the page on which the assistant was used; we keep them for at most 180 days for the purposes of improving the Service and support. If the assistant's AI mode is switched on, the content of the messages may be processed by the sub-processor Anthropic (language model provider). Do not enter sensitive personal data into the assistant.

We obtain the data directly from the data subjects (registration, entry of companies, use of the API), automatically during operation, and from the documents the User sends or receives.

Provider selection on the Financial Administration portal (VPDS): if a taxable person selects us as the provider (or intermediary) of the delivery service in the application at vpds.financnasprava.sk, the Financial Directorate of the Slovak Republic transfers to us, once, the business name, tax ID (DIČ), contact e-mail and telephone number of the entity together with the verification token. We use these data exclusively to set up and verify the account, to verify the entity's authorisation to send documents for the given tax ID, to register in the central SMP (if the record for the given tax ID is not held by another provider) and to communicate with the entity. The Financial Directorate of the Slovak Republic informs the entity about this transfer directly at the time of selection in the document Notice to the Entity under the GDPR (PDF, financnasprava.sk); according to it, the Financial Directorate of the Slovak Republic anonymises the data in its own system after transferring them to the selected provider.

4. Purposes and legal bases of processing

- **Provision of the Service** (management of the account and companies, receiving and sending documents, validation): performance of a contract under Art. 6 para. 1 point (b) GDPR.
- **Record-keeping and retention of records** in the Peppol network, tax reporting and keeping accounting/tax documents: compliance with legal obligations under Art. 6 para. 1 point (c) GDPR.
- **Security, prevention of abuse, rate limiting and traceability**: legitimate interest under Art. 6 para. 1 point (f) GDPR (interest in secure and reliable operation).
- **E-mail verification and operational communication**: performance of a contract under Art. 6 para. 1 point (b) and legitimate interest under Art. 6 para. 1 point (f) GDPR.

- **Tips, reminders and the feedback question**: legitimate interest under Art. 6 para. 1 point (f) GDPR (help with adopting the service and its improvement); you may object to this processing at any time through the unsubscribe link in the e-mail or in the account settings.
- **Error monitoring and application diagnostics**: legitimate interest under Art. 6 para. 1 point (f) GDPR (stable and secure operation of the Service).
- **Handling of enquiries and support, including the AI preparation of draft replies and the chat assistant**: legitimate interest under Art. 6 para. 1 point (f) GDPR (efficient and prompt handling of requests; a simple first question may be answered directly by an assistant using artificial intelligence, other replies are written or approved by a person).
- **Establishment and defence of legal claims**: legitimate interest under Art. 6 para. 1 point (f) GDPR.

5. Roles of the contracting parties in the processing

In relation to the account data and the operation of the Service (registration, login, security logs, support) the Controller acts as controller. In relation to the **content of the exchanged documents** which the User sends, receives, stores or exports through the Service, the Controller acts as a **processor under Art. 28 GDPR** on the documented instruction of the User; the conditions are governed by the Data Processing Agreement (DPA), which is concluded automatically upon the establishment of the contractual relationship (by reference in the General Terms and Conditions). The Controller acts as an independent controller only where the processing is imposed on it by law or by the binding Peppol framework, or where it carries it out for its own legitimate purpose, and exclusively for the purposes listed in Art. 11.4 of the DPA: tax reports to the Financial Administration and mandatory reports in the Peppol network, security logs, invoicing and its own accounting, and the establishment and defence of legal claims. In relation to the content of the exchanged documents the Controller always acts only as a processor or a sub-processor, and it does not use the personal data processed for the User for its own marketing purposes, for profiling or for training machine learning models; the division of roles in the chain of controller, processor and sub-processor (partners with their own brand) is governed by Art. 11 of the DPA. The User, as their controller, is responsible for the lawfulness and content of the data in the documents.

6. Recipients and processors

- **Peppol network**: other Peppol service providers and the access points of the senders/recipients (necessary for the delivery of documents).
- **Financial Directorate of the Slovak Republic** (Peppol Authority): to the extent of tax reporting and supervision under the Peppol framework.
- **Brevo (Sendinblue SAS)**, France: processor for sending transactional e-mails.
- **DigitalOcean**: processor providing the cloud infrastructure (hosting, Frankfurt region, EU).

- **Sentry (Functional Software, Inc. / Sentry GmbH)**: processor for error monitoring and operational diagnostics of the application; EU data region (Germany).
- **Websupport, s. r. o.**, Slovakia: provider of the server infrastructure for the Controller's outgoing mail server (transmission of e-mail notifications including document attachments).
- **Anthropic PBC**, USA: processor for the AI functions of the Service (the chat assistant "Pepo" in AI mode and the preparation of draft replies to messages from the contact form and to customer support tickets). The content of the message, the subject and the sender's e-mail are processed and, for a signed-in user or a ticket of a registered customer, also a brief summary of their account (name and status of the companies, Peppol ID, Data Archive setting and the record data of the last three documents: number, direction, counterparty and status); the content of documents (XML, lines, amounts) and attachments are never handed over. Anthropic also prepares the summary of a phone call transcript (what the caller wanted, contact details and the next step). A simple first question may be answered directly by our assistant using artificial intelligence without a person checking the reply beforehand (by replying to such a message you reach a colleague); other replies are written or approved by a person.
- **CloudTalk** (the CloudTalk group: CloudTalk s.r.o., Bratislava, and its affiliates): processor for telephone support; it processes the caller's number, the time and duration of the call and the call recording, and runs the automated voice assistant that answers the call, replies to basic questions and takes down the request. Call recordings and AI data are stored in Germany (EU); for the voice assistant and speech recognition it uses its own sub-processors in the USA (per its published list, for example ElevenLabs, Deepgram, OpenAI), bound by standard contractual clauses.
- **OpenAI, L.L.C.**, USA: processor for transcribing call recordings into text (automatic speech recognition). The audio of the call is transferred; OpenAI does not use API data to train its models and keeps it for at most 30 days for abuse monitoring, then deletes it.
- **Stripe Payments Europe, Ltd.**, Ireland: when processing card payments (top-ups of prepaid credit, the intermediary registration fee) it acts as an independent controller under its own privacy policy.
- **Cloudflare, Inc.**: bot and DDoS protection to the extent technically necessary.
- **OpenAI, L.L.C.**, USA: measurement pixel for evaluating advertising in ChatGPT (the address of the visited public page without parameters, the completed-registration event and, at registration, a SHA-256 hash of the e-mail and, if entered, of the name and phone typed into the form so that OpenAI can attribute the registration to an ad; never plain values, never anything from your documents), only with your consent in the cookie bar; it is never loaded in the signed-in part of the portal.
- **Meta Platforms Ireland Limited**, Ireland (data is also made available to Meta Platforms, Inc., USA): Meta measurement pixel for evaluating advertising on Facebook and Instagram (the address of the visited public page and the completed-registration event, without your e-mail or any other data about you), only after your consent in the cookie bar; never loaded in the signed-in part of the portal.

- **Ahrefs Pte. Ltd.**, Singapore (outside the EU): Ahrefs Web Analytics service for traffic statistics of the public pages (address of the visited page without tokens and without parameters other than utm_, referring page, browser and device type; no cookies), only after your consent in the cookie bar; it is not loaded in the signed-in part of the portal, in the administration or on pages with sign-in links.
- **Intermediaries of the delivery service (white-label partners)**: if the company was set up with us by a partner entered in the Financial Administration provider selection, the data of the company and of the documents are also accessible to that partner, who acts towards the company as its contractual provider.

The Controller has concluded data processing agreements under Art. 28 GDPR with the processors. We do not disclose personal data to third parties for marketing purposes and we do not sell them.

7. Transfers to third countries

We process personal data primarily within the EU/EEA (Brevo in France, DigitalOcean in Frankfurt, Sentry with the Germany data region, Stripe in Ireland). For the AI functions of the Service (chat assistant in AI mode, preparation of draft replies to enquiries and support tickets) the content of the messages is processed **in the USA** (Anthropic PBC); this transfer relies on an adequacy decision (Anthropic's certification under the EU-US Data Privacy Framework) and, subsidiarily, on the standard contractual clauses (SCC). Some other processors or their parent companies (DigitalOcean, Cloudflare, Sentry) are established in the USA and may also access the data outside the EU/EEA; such a transfer takes place on the basis of an adequacy decision (e. Call recordings are transcribed into text by OpenAI, L.L.C. **in the USA** on the basis of standard contractual clauses (SCC) or, where the recipient is certified under the EU-US Data Privacy Framework, an adequacy decision.g. the EU-US Data Privacy Framework, if the recipient is certified), otherwise on the basis of the standard contractual clauses (SCC) adopted by the European Commission. We will provide a copy of the appropriate safeguards (SCC) on request at peppol@verteco.digital.

8. Retention period

- **Account and company data**: for the duration of the contractual relationship and subsequently for at most the limitation period of claims (as a rule 4 years); then they are deleted or anonymised.
- **Records of provider selections from the Financial Administration portal (FS webhooks)**: for the duration of the contractual relationship with the company concerned and subsequently 4 years (proof of the authorisation of the registration in the Peppol network).
- **Operation and document logs**: for the period laid down by legislation, but at least 3 months in line with the requirements of the Peppol framework.

- **Tax and accounting documents**: we keep the content of the documents (original XML, PDF preview, attachments) for the duration of the contractual relationship if the company has the Data archive switched on (by default for companies added from 13 September 2026, separately for received and sent documents; 1 GB included). With the Data archive switched off (maximum encryption mode) we automatically delete the readable copies after the chosen period from delivery has elapsed (14 days by default, 1 to 90 days), and the customer ensures the archiving of the originals for the statutory period (General Terms and Conditions (VOP) Art. 11a). We keep the operational metadata of the document and the delivery receipt as proof of delivery even after the content has been deleted. When the cooperation ends, on request we hand over to you all stored documents (original XML + CSV) and delete our copies (to the extent the law does not require us to keep them).
- **Deleted accounts**: after an account is deleted, the account data are anonymised immediately; we keep the original e-mail address and the IP address from which the account was deleted for 12 months to handle support and protect against abuse, after which only a one-way fingerprint (hash) of the address remains.
- **Security log (audit)**: 12 months, then deleted automatically.
- **Chat assistant messages**: 180 days, then deleted automatically.

After the periods have expired, the data are deleted or anonymised.

We keep a permanent record of changes to the document retention settings and to the settings of document links without login (date and time, account, e-mail and IP address of the person who made the change) for the entire duration of the contractual relationship and for 3 years after its end: it is the proof of the controller's instruction under Art. 28 GDPR. If the company switches on document links without login (General Terms and Conditions (VOP) Art. 11b), we record every use of a link (time, IP address, request type) in the security journal: successful uses for 90 days, refused ones for at most 365 days; this information is also intended for persons without an account who use such a link (Art. 14 GDPR).

9. Rights of the data subject

To the extent provided by the GDPR and the Act, the data subject has the right:

- to access their personal data and to have them rectified;
- to erasure ("right to be forgotten") and to restriction of processing;
- to portability of the data processed on the basis of a contract or consent;
- to object to processing based on legitimate interest;
- to withdraw consent at any time, if the processing is based on consent (without affecting the lawfulness of the processing before the withdrawal);
- to lodge a motion to initiate proceedings or a complaint with the supervisory authority.

We handle requests without undue delay, as a rule within one (1) month; for complex or numerous requests the period may be extended by a further two months (Art. 12 para. 3 GDPR),

of which we inform the data subject. We accept requests at peppol@verteco.digital. Some rights may be limited by the Controller's legal obligations (e.g. the mandatory retention of documents).

10. Automated decision-making and profiling

The Controller does not carry out automated individual decision-making, including profiling, which produces legal effects concerning the data subject or similarly significantly affects them under Art. 22 GDPR.

11. Cookies and similar technologies

We use only **strictly necessary** cookies and technical files: the login cookie `portal_session` (httpOnly, Secure, SameSite=Lax; duration ~7 days) to keep you signed in and the technical cookies of the network provider (e.g. Cloudflare `__cf_bm`; duration ~30 minutes) for bot protection. The chat assistant keeps a technical conversation identifier `pepo.sessionId` in the browser storage (localStorage) so that the conversation survives a page refresh; it does not serve for tracking across websites. Measurement cookies are used **only with your consent**, given in the bar on your first visit. After consent, the Ahrefs Web Analytics service (Ahrefs Pte. Ltd., Singapore) for traffic statistics is also loaded on public pages (never in the signed-in part of the portal); it uses no cookies and sends Ahrefs the address of the visited page without parameters (other than utm_) and basic technical data about the visit. After consent the OpenAI measurement pixel is loaded on public pages (never in the signed-in part of the portal); it stores the cookies `__obref` and `__oppref` (a browser identifier and an ad-click identifier) and sends OpenAI, in the USA, the address of the visited page without parameters and the completed-registration event; it serves to evaluate advertising in ChatGPT. At registration it may also pass a SHA-256 hash of the e-mail and, if entered, of the name and phone typed into the registration form so that OpenAI can attribute the registration to an ad; plain values are never passed, nor anything from your documents. After consent the Meta measurement pixel is also loaded on public pages; it stores the cookies `_fbp` and `_fbc` (a browser identifier and an ad-click identifier) and sends Meta the address of the visited page and the completed-registration event; it serves to evaluate advertising on Facebook and Instagram. Your choice is stored in the `vp_consent` cookie for 12 months and can be changed any time via "Cookie settings" in the footer. Without consent nothing is measured. The bar always says which tools your consent covers; if you agreed and we add another measurement tool, we ask for your consent again, and when you withdraw consent we delete the cookies of these tools. Beyond that, the browser keeps only technical data in the device's local storage: the chosen language and display settings of the portal, the conversation identifier of the chat assistant (only once you write to it), the code of the partner whose link brought you here and, within a single browser tab, the source of the visit (referring domain or campaign parameters) if there is one. None of this is sent anywhere automatically and none of it tracks you across websites.

12. Security of processing

The Controller takes appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in particular encryption in transit (TLS), password hashing, access control, separation of environments, rate limiting and access logging. In the event of a personal data breach the Controller proceeds under Art. 33 and 34 GDPR.

13. Obligation to provide data

The provision of the account data and of the identification data of the companies is a contractual or statutory requirement necessary for the provision of the Service; without them the Service cannot be provided (setting up an account, registering a company, sending/receiving documents).

14. Supervisory authority

The supervisory authority is the **Office for Personal Data Protection of the Slovak Republic**(Úrad na ochranu osobných údajov Slovenskej republiky), Hraničná 12, 820 07 Bratislava, uoou.sk, with which the data subject has the right to lodge a motion to initiate proceedings.

15. Changes to the policy and contact

The Controller may update this policy; it will inform about material changes in an appropriate manner. Please direct questions and requests to peppol@verteco.digital.