VatForge DPA v2

Data Processing Addendum

Version: 2 **Effective date:** September 6, 2026 **Supersedes:** DPA v1 (dated July 22, 2026)

This Data Processing Addendum ("**DPA**") forms part of the VatForge Terms of Service (the "**Agreement**") entered into between:

- **Vatforge AB**, a Swedish limited company with organisation number 559433-7981, registered office at Vasagränd 13, lgh 1201, 177 53 Järfälla, Sweden ("**Vatforge**", "**we**", "**us**", or the "**Processor**"); and
- **the Customer** identified in the applicable ordering document or account registration ("**Customer**", "**you**", or the "**Controller**").

It governs the processing of Personal Data by Vatforge on behalf of the Customer in the course of providing the VatForge platform and related services (the "**Services**"), as required by Article 28 of Regulation (EU) 2016/679 (the "**GDPR**").

If there is any conflict between this DPA and the Agreement, this DPA controls with respect to the processing of Personal Data.

---

1. Definitions

Capitalised terms used in this DPA have the meanings given in the GDPR unless defined below.

- **"Applicable Data Protection Law"** means the GDPR and any national laws implementing or supplementing the GDPR in EU/EEA Member States, including the Swedish Data Protection Act (Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning).
- **"Customer Data"** means any Personal Data that Vatforge processes on behalf of the Customer under the Agreement.
- **"Data Subject"** means an identified or identifiable natural person to whom the Customer Data relates.
- **"Personal Data Breach"** has the meaning given in Article 4(12) GDPR.
- **"Sub-processor"** means any third party engaged by Vatforge to process Customer Data on behalf of the Customer.
- **"Standard Contractual Clauses"** or **"SCCs"** means the Standard Contractual Clauses adopted by the European Commission under Decision (EU) 2021/914 of 4 June 2021.
- **"Services"** has the meaning given in the Agreement.

Terms such as "Personal Data", "Processing", "Controller", "Processor", "Data Subject", and "Supervisory Authority" have the meanings given in the GDPR.

2. Roles of the parties

The parties acknowledge that, for the purposes of the GDPR:

- The **Customer** is the **Controller** of the Customer Data.
- **Vatforge** is the **Processor** acting on behalf of the Customer, and processes Customer Data only on documented instructions from the Customer.
- The Agreement (including this DPA and the Customer's use of the Services in accordance with the Agreement's documentation) constitutes the Customer's documented instructions to Vatforge for the processing of Customer Data.

Where Vatforge processes Personal Data as a Controller in its own right (for example, account-level identifiers, billing records, telemetry required to secure and operate the Services), such processing is governed by the Vatforge Privacy Policy and is outside the scope of this DPA.

---

3. Subject matter, duration, nature, and purpose of processing

The subject matter, duration, nature, and purpose of the processing, together with the types of Personal Data and categories of Data Subjects, are described in **Annex A** of this DPA.

Processing continues for the term of the Agreement, and for such further period as is required by law or as is necessary for Vatforge to comply with its obligations under §12 (Deletion or return of Personal Data) of this DPA.

---

4. Processor obligations

Vatforge shall:

1. Process Customer Data only on the documented instructions of the Customer, including with regard to transfers of Personal Data to a third country or an international organisation, unless required to do so by EU or Member State law to which Vatforge is subject, in which case Vatforge shall inform the Customer of that legal requirement before processing (unless the law prohibits such information on important grounds of public interest);
2. Ensure that persons authorised to process the Customer Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
3. Take all measures required pursuant to Article 32 GDPR (Security of processing), as further described in §5 and **Annex C** of this DPA;
4. Respect the conditions referred to in Article 28(2) and (4) GDPR for engaging Sub-processors, as further described in §6 and **Annex B** of this DPA;

5. Assist the Customer, taking into account the nature of the processing and by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising Data Subjects' rights under Chapter III GDPR;
6. Assist the Customer in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR, taking into account the nature of processing and the information available to Vatforge;
7. At the choice of the Customer, delete or return all Customer Data to the Customer after the end of the provision of Services relating to processing, and delete existing copies unless EU or Member State law requires storage of the Personal Data, as further described in §12 of this DPA;
8. Make available to the Customer all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR, and allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer, as further described in §10 of this DPA;
9. Immediately inform the Customer if, in Vatforge's opinion, an instruction from the Customer infringes the GDPR or other Applicable Data Protection Law.

---

5. Security of processing

Vatforge shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk to Data Subjects, in accordance with Article 32 GDPR. A description of the measures in place as at the effective date of this DPA is set out in **Annex C**.

Vatforge may update the measures from time to time provided that the updates do not result in a material reduction of the security of Customer Data.

Vatforge shall ensure that any natural person acting under its authority who has access to Customer Data does not process the data except on instructions from the Customer, unless required to do so by EU or Member State law.

---

6. Sub-processors

The Customer provides a **general authorisation** for Vatforge to engage Sub-processors to process Customer Data. The Sub-processors engaged by Vatforge as at the effective date of this DPA are listed in **Annex B** of this DPA and at https://vatforge.com/security/subprocessors.

Where Vatforge engages a new Sub-processor or replaces an existing Sub-processor, Vatforge shall:

1. Give the Customer at least **30 days' prior notice** of the intended addition or replacement, by updating the public sub-processor list at https://vatforge.com/security/subprocessors and, where the Customer has subscribed to notifications, by email to the Customer's designated privacy contact;

2. Impose on the Sub-processor, by way of contract, the same data protection obligations as set out in this DPA, in particular providing sufficient guarantees to implement appropriate technical and organisational measures such that the processing meets the requirements of the GDPR;
3. Remain fully liable to the Customer for the performance of the Sub-processor's obligations.

The Customer may object to the addition or replacement of a Sub-processor on reasonable data protection grounds by notifying Vatforge in writing within the notice period. If the objection cannot be resolved, either party may terminate the Agreement in respect of the affected Services and Vatforge shall refund any prepaid fees for the terminated portion of the Services.

---

7. International transfers

Where the provision of the Services requires the transfer of Customer Data to a country outside the European Economic Area (EEA) or an international organisation, Vatforge shall ensure that such transfer is subject to appropriate safeguards under Chapter V GDPR, which may include:

1. The country having been the subject of an adequacy decision by the European Commission;
2. The EU-US Data Privacy Framework, where the recipient is certified under the framework;
3. The Standard Contractual Clauses, incorporated into the relevant Sub-processor agreement.

Where the SCCs apply, the parties agree that Module Three (Processor to Processor) or Module Four (Processor to Controller) applies to the relevant transfer, as appropriate. The specific optional clauses and choices of Module are set out in the relevant Sub-processor agreement.

The current cross-border transfer position for each Sub-processor is described in **Annex B**.

---

8. Data Subject requests

Taking into account the nature of the processing, Vatforge shall assist the Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the Data Subject's rights under the GDPR, including rights of access, rectification, erasure, restriction of processing, data portability, and objection.

If Vatforge receives a request directly from a Data Subject relating to Customer Data, Vatforge shall not respond to the request directly (except to confirm receipt and to identify the relevant Customer as the Controller), and shall promptly forward the request to the Customer's designated privacy contact.

---

9. Personal Data Breach notification

Vatforge shall notify the Customer without undue delay and in any event **no later than 72 hours** after becoming aware of a Personal Data Breach affecting Customer Data.

The notification shall describe, to the extent known at the time:

1. The nature of the Personal Data Breach, including where possible the categories and approximate number of Data Subjects and Personal Data records concerned;
2. The name and contact details of the Vatforge contact from whom more information can be obtained;
3. The likely consequences of the Personal Data Breach;
4. The measures taken or proposed to be taken by Vatforge to address the Personal Data Breach and to mitigate its possible adverse effects.

Where and insofar as it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

Vatforge shall cooperate with the Customer to enable the Customer to fulfil its own notification obligations to Supervisory Authorities and Data Subjects under Articles 33 and 34 GDPR.

---

10. Audits and inspections

Vatforge shall make available to the Customer all information reasonably necessary to demonstrate compliance with this DPA and Article 28 GDPR.

To fulfil this obligation, Vatforge shall make available to the Customer, upon written request:

1. Its most recent independent third-party assessments or attestation reports concerning the security controls applied by its Sub-processors (for example, the SOC 2 Type II reports maintained by Supabase, Stripe, and other applicable Sub-processors);
2. Its own security documentation, including the description of technical and organisational measures set out in **Annex C**;
3. Reasonable responses to written security questionnaires from the Customer, to the extent that responding does not risk the security of other customers' data.

Where the information described above is not sufficient to demonstrate compliance, the Customer (or an independent auditor mandated by the Customer that is not a competitor of Vatforge) may conduct an on-site audit of Vatforge's data-processing activities, subject to:

1. Reasonable advance written notice (not less than 30 days, except in the case of an actual Personal Data Breach where a shorter notice period is agreed);
2. Reasonable frequency (not more than once per calendar year, except where required by a Supervisory Authority or triggered by an actual Personal Data Breach);
3. Compliance with Vatforge's on-site security and confidentiality policies;

4. Conducting the audit in a manner that does not disrupt Vatforge's normal business operations or compromise the security of other customers' data;
5. The Customer bearing all costs of the audit unless the audit reveals a material breach of this DPA, in which case Vatforge shall bear the reasonable costs.

The Customer shall share any audit reports with Vatforge on a confidential basis.

---

11. Data Protection Impact Assessments and prior consultation

Vatforge shall provide reasonable assistance to the Customer with any Data Protection Impact Assessments and prior consultations with Supervisory Authorities that the Customer is required to conduct under Articles 35 and 36 GDPR in relation to the Services.

---

12. Deletion or return of Personal Data

On termination or expiry of the Agreement, or on the earlier written request of the Customer, Vatforge shall, at the Customer's choice:

1. **Return** all Customer Data to the Customer in a structured, commonly used, and machine-readable format (typically CSV or JSON export); or
2. **Delete** all Customer Data from Vatforge's live systems within **30 days** of the termination date or request, and from backup systems within a further reasonable period consistent with Vatforge's backup rotation schedule (typically no more than 90 days).

The obligation to delete does not apply where Applicable Data Protection Law or other applicable law requires storage of the Personal Data. In particular:

1. Vatforge is required to retain certain records of transactions and accounting data for **10 years** in order to satisfy the record-keeping obligations set out in Article 369k of the VAT Directive (Council Directive 2006/112/EC) for the Union One-Stop Shop scheme;
2. Vatforge is required to retain certain accounting records for **7 years** in order to satisfy the record-keeping obligations set out in the Swedish Bookkeeping Act (Bokföringslagen (1999:1078)).

Any Customer Data retained under these obligations shall be kept in a manner that limits its accessibility, is used only for the specific legal purpose for which it is retained, and is deleted at the end of the applicable retention period.

Vatforge shall provide the Customer with written confirmation of deletion upon request.

---

13. Liability

Each party's liability arising out of or related to this DPA is subject to the limitation of liability provisions set out in the Agreement.

Nothing in this DPA excludes or limits either party's liability where such exclusion or limitation is prohibited by Applicable Data Protection Law.

---

14. Term and termination

This DPA takes effect on the effective date set out at the top of this document and continues in force for the term of the Agreement. It automatically terminates when the Agreement terminates, subject to Vatforge's continuing obligations under §12 (Deletion or return of Personal Data) and any obligations that by their nature are intended to survive termination.

---

15. Governing law and jurisdiction

This DPA is governed by the laws of Sweden. Any dispute arising out of or in connection with this DPA shall be subject to the non-exclusive jurisdiction of the courts of Stockholm, Sweden.

---

16. Contact

Questions about this DPA, sub-processor changes, or data protection matters generally should be directed to:

Data Protection contact: Vatforge AB Vasagränd 13, lgh 1201, 177 53 Järfälla, Sweden dpa@vatforge.com

---

Annex A — Details of processing

Subject matter of processing: Provision of the VatForge platform, which supports EU VAT compliance operations for the Customer, including tracking of cross-border sales against the Article 59c €10,000 threshold, aggregation of quarterly One-Stop Shop return data, monitoring of Article 24b location evidence, monitoring of CESOP exposure, and related audit-trail retention.

Duration of processing: For the term of the Agreement, and thereafter for the retention periods described in §12 of this DPA.

Nature and purpose of processing: Automated processing (ingestion, normalisation, VAT determination, threshold calculation, aggregation, storage, transmission, and display via the Services' user interfaces and reports) required to provide the compliance functionality described in the Services documentation.

Types of Personal Data processed:

- Customer account data (name, business name, email address, VAT identification number, country of establishment)
- End-customer transaction data imported from the Customer's connected payment platforms (buyer country, buyer type (B2C or B2B), buyer VAT identification number where applicable, transaction amount, currency, date, transaction identifier)
- Communications data (emails to hello@vatforge.com or other Vatforge inboxes containing personal data of the Customer's contacts or end customers)
- Authentication data (email addresses used for account sign-in)
- Support and audit-trail data (log entries recording actions taken within the Services)

Categories of Data Subjects:

- The Customer's authorised users (typically the Customer's founder, employees, contractors, or accountant)
- End customers of the Customer whose transactions are ingested into the VatForge platform (typically identified only by country, buyer type, and where applicable a business VAT identification number; not by individual name)

Annex B — Sub-processors

The Sub-processors engaged by Vatforge as at the effective date of this DPA are listed below. The current list is also published at https://vatforge.com/security/subprocessors with a change log.

SUB-PROCESSOR	PURPOSE	LOCATION	TRANSFER SAFEGUARD
Supabase, Inc.	Database, authentication, and backend services (Edge Functions)	European Union (Ireland, eu-west-1)	EU processing — no third-country transfer
Stripe Payments Europe, Ltd / Stripe, Inc.	Payment processing for Vatforge subscriptions; read-only transaction imports for connected accounts	Ireland / United States	EU-US Data Privacy Framework + Standard Contractual Clauses
Vatstack GmbH	EU VAT rate reference data (daily rate sync). Receives country-code queries only; no Personal Data is transmitted	European Union (Austria)	EU processing — no third-country transfer

SUB-PROCESSOR	PURPOSE	LOCATION	TRANSFER SAFEGUARD
Resend, Inc.	Transactional and service-related email	European Union	EU processing — no third-country transfer
Lovable AB	Application hosting and site delivery	European Union + CDN edge network	EU processing — no third-country transfer
Amazon Web Services EMEA SARL (Route 53)	DNS resolution for vatforge.com and vatforge.eu	United States (global anycast network)	EU-US Data Privacy Framework + Standard Contractual Clauses
Plausible Insights OÜ	Privacy-friendly website analytics (cookieless, aggregate only; no Personal Data is collected)	European Union	EU processing — no third-country transfer
Zoho Corporation B.V.	Business email hosting for hello@vatforge.com and khumakh@vatforge.com; receives customer support and general inquiry emails	European Union (Zoho EU data centre)	EU processing — no third-country transfer

Notice mechanism for sub-processor changes: 30 days' advance notice via update to https://vatforge.com/security/subprocessors, as described in §6 of this DPA.

Annex C — Technical and organisational measures

Vatforge has implemented the following technical and organisational measures to ensure a level of security appropriate to the risk, in accordance with Article 32 GDPR.

Confidentiality — measures preventing unauthorised access to Personal Data:

- Encryption of Personal Data at rest using AES-256 (provided by the Supabase Ireland region on which Vatforge's Personal Data is stored)
- Encryption of Personal Data in transit using TLS 1.2 or higher between all client applications, Vatforge servers, and Sub-processors
- Multi-factor authentication required for all Vatforge personnel with administrative access to production systems
- Role-based access controls, enforced at the database layer via Row-Level Security

- Principle of least privilege applied to internal access, with access reviewed on a periodic basis
- Contractual confidentiality obligations imposed on all Vatforge personnel and contractors

Integrity — measures ensuring that Personal Data cannot be modified in an unauthorised manner:

- Immutable append-only audit log (`ledger_events`) recording each material change to transaction data, enforced at the database layer via triggers
- Version control for all code changes to the Services, with all production deployments recorded and traceable
- Separation of production and non-production environments

Availability and resilience — measures ensuring the availability and resilience of processing systems and Services:

- Managed database backup provided by Supabase, with point-in-time recovery available
- Redundant hosting via Lovable and its CDN edge network
- Monitored uptime, with security alerts routed to on-call personnel

Ability to restore — measures ensuring the ability to restore the availability of and access to Personal Data in a timely manner in the event of a physical or technical incident:

- Point-in-time database recovery via Supabase
- Documented incident-response procedures

Regular testing — measures for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing:

- Regular internal security reviews by Vatforge personnel
- Sub-processor security posture reviewed at engagement and periodically thereafter
- Reliance on Sub-processor security attestations (for example, Supabase SOC 2 Type II) where applicable

Personnel measures:

- Confidentiality obligations for all personnel with access to Customer Data
- Training on data protection responsibilities appropriate to each role

Physical security: Physical security of hosting infrastructure is the responsibility of the underlying hosting Sub-processor (primarily Supabase, which operates from Amazon Web Services facilities in Ireland). Vatforge does not operate its own data centre.

End of Data Processing Addendum v2.