> *Note: This English text is provided for convenience. The Dutch version is authoritative where translations differ.*

Data processing agreement

This data processing agreement (“DPA”) forms part of your **Agreement** with TimeChimp.

Capitalised words have the meaning in this DPA or in the General terms and conditions. Other terms under the **GDPR** (EU privacy law) have the meaning under that law.

Why this agreement?

1. We provide the TimeChimp platform as a SaaS service.
2. You use the platform; we process personal data on your behalf.
3. The **GDPR** requires us to set out rights and obligations in writing.

Article 1. Definitions

1.1 Terms such as “personal data”, “data subject”, “personal data breach”, and “processing” have the meaning under the **GDPR**.

1.2 Other capitalised terms have the meaning in the General terms and conditions.

1.3 **You** / **Customer** = the controller who places personal data in the platform.

1.4 **We** / **Processor** = TimeChimp.

1.5 This DPA implements the requirements of GDPR Article 28(3) and is the written agreement between Controller and **Processor** as referred to there. Annex A version 01-06-2026 forms an integral part of this DPA.

1.6 EEA: the European Economic Area.

Article 2. What do we process for?

2.1 We process personal data only to perform the Agreement, in line with this DPA and the **GDPR**.

2.2 We process only what is needed to deliver the Services. The purpose is set out in Annex A version 01-06-2026.

2.3 Does the purpose change? Let us know.

Article 3. How do we process?

3.1 You guarantee that your data and instructions are lawful and do not infringe third-party rights.

3.2 We are responsible for processing on your behalf under this DPA. We are not responsible for:

i. how you collect data;
ii. processing by you for other purposes;
iii. processing by third parties you choose yourself.

3.3 If you change the purpose or instructions and we cannot reasonably comply for business reasons, we will discuss this in good faith.

3.4 On request, we will explain which measures we take (if not already in Annex A version 01-06-2026).

3.5 Our obligations also apply to anyone processing data under our authority.

3.6 We may use subprocessors (for example data centres) if they accept the same terms. Overview: terms.timechimp.com/en/subprocessors.

a. We inform you at least one **Calendar month** in advance about new or changed subprocessors by email and via an updated list on that page. You may object within that period. If we cannot offer another solution, you may end the **Agreement** under Article 8 of the general terms and conditions.

3.7 We process personal data on your instructions under the **Agreement**: by accepting our terms, using the platform, or otherwise giving us directions (for example via support or a **Notice**). If we believe an instruction infringes the **GDPR** or other applicable privacy law, we will notify you without undue delay before carrying out the instruction.

Article 4. Confidentiality

4.1 All personal data we receive from you is treated confidentially. Our staff sign confidentiality undertakings.

4.2 Exceptions: with your consent, where needed for the Agreement, or where the law requires disclosure. If the law requires disclosure, we will inform you where possible. Costs of legal steps are yours.

Article 5. Security

5.1 We implement appropriate technical and organisational measures against loss and misuse. See Annex A version 01-06-2026.

5.2 No measure is 100% foolproof. We aim for a level that fits the state of the art, the sensitivity of the data, and reasonable cost.

Article 6. Incidents and personal data breaches

6.1 In case of a suspected or actual personal data breach or breach of confidentiality ("Incident"), we will inform you without undue delay and no later than 48 hours after we become aware of the Incident.

6.2 We follow our support procedure (Severity 1 or 2): service ticket, updates in the portal, and phone contact with your known contact person.

6.3 We take reasonable steps to prevent further harm.

6.4 We provide information that is as complete and accurate as possible at the time of notification.

6.5 If a breach is due to us, we help you with notifications to authorities and data subjects. We may charge reasonable costs.

6.6 You remain responsible for your notification duties under the **GDPR**.

Article 7. Data outside the EEA

7.1 We process in the EEA and Switzerland, and in countries with an adequate level of protection under the **GDPR**. Some subprocessors process data outside the EEA (for example in the United States). We ensure appropriate safeguards, including Standard Contractual Clauses (SCCs) under **GDPR** Article 46(2)(c). See our subprocessors.

7.2 Processing outside the EEA only on your written request and with appropriate safeguards (for example standard contractual clauses).

Article 8. Audit

8.1 You may request one audit per year (with 2 weeks' notice) to verify compliance with this DPA. If there is a reasonable suspicion of a serious breach of this DPA or the **GDPR**, you may also request an audit outside the annual cycle, after written justification.

8.2 Audit costs are yours.

8.3 We agree in advance whether results are binding or discussed first.

8.4 The auditor signs confidentiality. Audits during business hours, without unreasonable disruption. No admin rights on our systems.

8.5 We cooperate and provide relevant information within 2 weeks, unless urgent.

8.6 No agreement on the outcome? An independent auditor may decide; we share costs equally.

Article 9. Data subject rights

9.1 If someone asks us for access, erasure, or other **GDPR** rights, we refer them to **You**; you handle the request.

Article 10. Liability

10.1 Our liability is limited to direct damage.

10.2 We are not liable for indirect damage (such as loss of revenue or data).

10.3 Maximum: what you paid us in the 12 **Calendar months** before the claim (excl. VAT), and not more than our liability insurance pays out.

10.4 Exception: intent or deliberate recklessness by our management (you must prove this).

10.5 You indemnify us against third-party claims about processing under this DPA.

10.6 Report damage within one **Calendar month**. Claims expire after 12 **Calendar months**, except where the law says otherwise.

Article 11. Force majeure

11.1 For force majeure affecting our processing obligations under this DPA, Article 12 of the general terms and conditions applies.

Article 12. Term and termination

12.1 This DPA applies for as long as the Agreement runs.

12.2 When the Agreement ends, this DPA ends, unless we still process data — then the DPA remains until processing stops.

12.3 If we cannot implement a change in purpose or instructions, we may terminate after consultation.

12.4 We return or delete data no later than 30 days after termination of the **Agreement**, unless otherwise agreed in writing. We confirm deletion to you in writing.

12.5 Articles that survive termination (such as confidentiality) remain in force.

Article 13. Miscellaneous

13.1 If a provision is invalid, the rest remains in force.

13.2 This is the entire agreement on this subject.

13.3 We may amend this DPA when the law requires, or when we agree this with you in writing. Changes to Annex A version 01-06-2026 also require written agreement. Obvious errors or evident omissions may be corrected without separate consent. All other changes require written agreement.

13.4 Failure to enforce a right is not a waiver.

13.5 This DPA binds successors and assignees.

Annex A — Purpose and security

Version 01-06-2026

This annex forms an integral part of the DPA.

Purpose of processing

Providing and maintaining the TimeChimp platform: time tracking, expenses, invoicing, user management, and support.

Types of personal data

Account data, contact data, time/expense/invoice data, and other personal data you enter in the platform.

Categories of data subjects

Your employees, contacts, and other persons whose data you enter.

Retention periods

Data category	Retention period
Account data	No later than 30 days after termination of the **Agreement**
Time, expense, and invoice data	7 years after the financial year (statutory accounting retention obligation)
Log data (access, system, and security logs)	12 months
Backups	Up to 3 months after termination of the **Agreement**

Security measures

We implement the following technical and organisational measures, among others:

a. Access control: role-based access (RBAC), multi-factor authentication (MFA) for administrators and user accounts where available, and periodic access reviews.

b. Encryption: TLS 1.2 or higher for data in transit; encryption at rest (AES-256 or equivalent) for storage of personal data in production environments.
c. Backups: daily backups of production data; backup retention in line with the retention periods in this annex.
d. Logging and monitoring: logging of system access and security-relevant events; log retention 12 months; monitoring for anomalous behaviour and availability.
e. Patch policy: security patches and updates are assessed and applied regularly under a defined maintenance process.
f. Staff: access to personal data is limited to staff with a need-to-know; confidentiality duties and privacy training.

Additional documentation: Visma Trust Centre.

(This data processing agreement is effective as of 01-06-2026.)