solidtime

Data Processing Agreement

Customer completion & countersignature form

How to complete this form

1. Fill in your company details below and review the Agreement.
2. Sign the **Customer** block on the Signatures page.
3. Email the completed PDF to hello@solidtime.io.
4. We countersign and return a fully executed copy for your records.

Customer details

The company identified below is the "Customer" (Controller) under this Agreement. Complete every field, then sign on the Signatures page.

LEGAL ENTITY NAME

REGISTERED ADDRESS

COUNTRY

COMPANY / REGISTRATION NO.

DATA-PROTECTION CONTACT NAME

CONTACT EMAIL

This Data Processing Agreement ("DPA") forms part of the Agreement between:
(1) the customer identified in the Agreement ("**Customer**" or "**Controller**"); and

(2) solidtime GesbR, an Austrian civil-law partnership represented by its partners Gregor Vostrak and Constantin Graf, with its office at Türkenstraße 19/1b, 1090 Wien, Austria ("**Solidtime**" or "**Processor**"),

each a "**Party**" and together the "**Parties**".

1. Definitions

1.1 Terms such as "**Personal Data**", "**Processing**", "**Controller**", "**Processor**", "**Data Subject**", "**Personal Data Breach**", "**Supervisory Authority**" and "**Special Categories of Personal Data**" have the meanings given in the GDPR.

1.2 "**Agreement**" means the terms of service, subscription agreement, or other contract between the Parties governing the Customer's use of the Service.

1.3 "**Customer Personal Data**" means Personal Data that Solidtime Processes on behalf of the Customer under the Agreement, as described in **Annex 1**.

1.4 "**Sub-processor**" means any third party engaged by Solidtime to Process Customer Personal Data.

1.5 "**Data Protection Law**" means the GDPR and any national implementing or supplementary legislation applicable to the Processing.

2. Roles and Scope

2.1 The Customer is the Controller and Solidtime is the Processor with respect to Customer Personal Data. Where the Customer is itself a processor acting on behalf of a third-party controller, Solidtime is a sub-processor and the Customer warrants it has the necessary authority to engage Solidtime on those terms.

2.2 Subject to clauses 2.4 and 2.7, Solidtime Processes Customer Personal Data only to provide and improve the Service and only as set out in this DPA and the Agreement.

2.3 The subject matter, duration, nature and purpose of the Processing, the types of Personal Data and the categories of Data Subjects are set out in **Annex 1**.

2.4 For a limited and exhaustive set of purposes, Solidtime acts as an independent Controller rather than as the Customer's Processor, determining the purposes and means of Processing under its own legal basis and its own privacy notice. These purposes are: (a) billing, account administration, and managing the contractual relationship; (b) securing and monitoring the Service, including detecting and preventing abuse, fraud, and security threats; and (c) sending service communications to users, and sending product communications and newsletters only to users who have opted in. The Processor obligations in this DPA do not apply to this Processing; Solidtime is responsible for complying with Data Protection Law as Controller in respect of it.

2.5 The Customer warrants that it will not enter, and will ensure its users do not enter, into the Service any Special Categories of Personal Data (Article 9 GDPR) or personal data relating to criminal convictions and offences (Article 10 GDPR), absent Solidtime's prior written agreement. The Customer is solely responsible for the accuracy, quality, and lawfulness of Customer Personal Data and of the instructions it gives.

2.6 The Customer is responsible for: (a) ensuring that its use of the Service complies with Data Protection Law; (b) providing all notices to, and obtaining all consents, permissions, and legal bases from, Data Subjects required for the Processing; (c) ensuring that Customer Personal Data entered into the Service is appropriate for the Service; (d) configuring and using the Service in a secure and lawful manner; and (e) ensuring that the users it authorises comply with the Agreement and this DPA.

2.7 The Customer instructs and authorises Solidtime, as Processor, to Process Customer Personal Data not only to provide the Service but also to analyse, maintain, develop, and improve the Service and its features. This Processing is carried out on the Customer's documented instructions under this DPA.

2.8 Solidtime may create aggregated, de-identified, or anonymised data from its Processing of Customer Personal Data, provided that such data cannot, by any means reasonably likely to be used, be used to identify, single out, or re-link to any Data Subject or Customer. Such data is not Customer Personal Data, and Solidtime may retain and use it for any lawful purpose, including operating, analysing, developing, and improving its products and services. This right survives termination or expiry of the Agreement.

3. Processing on Documented Instructions

3.1 Solidtime Processes Customer Personal Data only on the Customer's documented instructions, including with regard to international transfers, unless required to do otherwise by Union or Member State law. Where such a legal requirement applies, Solidtime informs the Customer of that requirement before Processing, unless the law prohibits this on important grounds of public interest.

3.2 The Agreement, this DPA, and the Customer's configuration and use of the Service constitute the Customer's complete documented instructions. Additional or alternative instructions must be agreed in writing.

3.3 Solidtime informs the Customer if, in its opinion, an instruction infringes Data Protection Law, and may suspend the affected Processing until the Customer withdraws, amends, or confirms the instruction in writing.

Solidtime is not obliged to assess the lawfulness of the Customer's instructions generally.

3.4 If a court, law enforcement, or other competent authority makes a legally binding demand for Customer Personal Data, Solidtime will, unless legally prohibited, notify the Customer before disclosing and, where lawful, direct the authority to request the data from the Customer directly. Solidtime discloses only the minimum Customer Personal Data legally required and may challenge demands that it considers unlawful, overbroad, or inconsistent with Data Protection Law.

4. Confidentiality

4.1 Solidtime ensures that persons authorised to Process Customer Personal Data are bound by an appropriate obligation of confidentiality (whether contractual or statutory) and that access is limited to personnel who need it to perform their duties.

5. Security Measures

5.1 Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of Processing, as well as the risks to Data Subjects, Solidtime implements appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as set out in **Annex 2** (Art. 32 GDPR).

5.2 Solidtime may update its security measures from time to time, provided the level of protection is not materially reduced.

6. Sub-processors

6.1 The Customer gives **general written authorisation** for Solidtime to engage Sub-processors. The Sub-processors engaged as at the date of this DPA are identified in **Annex 3**.

6.2 Solidtime imposes on each Sub-processor, by written contract, data-protection obligations that are substantially equivalent to those set out in this DPA, to the extent applicable to the nature of the services the Sub-processor provides, in particular providing sufficient guarantees of appropriate technical and organisational measures.

6.3 Solidtime remains fully liable to the Customer for the performance of each Sub-processor's obligations.

6.4 Solidtime gives the Customer at least **14 days'** prior notice of any intended addition or replacement of a Sub-processor (for example via email or a published Sub-processor page), thereby giving the Customer the opportunity to object.

6.5 The Customer may object to an intended addition or replacement within that period on reasonable data-protection grounds, by written notice explaining its specific reasons. Solidtime will use commercially reasonable efforts to address the objection and, where it cannot reasonably do so, may at its option: (a) provide the affected part of the Service without the relevant Sub-processor, where technically and commercially feasible; (b) allow the Customer to terminate the affected part of the Service; or (c) where use of the Sub-processor is necessary to the continued provision of the Service, terminate the affected part of the Service. If the Customer does not object within the notice period, the addition or replacement is deemed authorised.

6.6 In an emergency affecting the security or availability of the Service, or where a change is required for legal compliance or the continuity of the Service, Solidtime may engage or replace a Sub-processor on shorter notice or without prior notice, in which case it informs the Customer of the change without undue delay afterwards.

6.7 The removal of a Sub-processor without an addition or replacement does not require prior notice and may be reflected by updating the Sub-processor page.

7. Assistance with Data Subject Rights

7.1 Taking into account the nature of the Processing, Solidtime assists the Customer by appropriate technical and organisational measures, insofar as possible, in fulfilling the Customer's obligation to respond to requests to exercise Data Subject rights (Chapter III GDPR).

7.2 If Solidtime receives a request directly from a Data Subject relating to Customer Personal Data, it does not respond substantively other than to confirm the request relates to the Customer, and forwards the request to the Customer without undue delay.

8. Assistance with Compliance Obligations

8.1 Solidtime assists the Customer, taking into account the nature of Processing and the information available to it, in ensuring compliance with the Customer's obligations under Articles 32 to 36 GDPR (security of processing, breach notification, data protection impact assessments, and prior consultation).

8.2 The Customer bears the reasonable costs incurred by Solidtime in providing the assistance described in clauses 7 and 8, save to the extent the need for assistance arises from Solidtime's breach of this DPA.

9. Personal Data Breach Notification

9.1 Solidtime notifies the Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer Personal Data.

9.2 The notification describes, to the extent known: the nature of the breach, the categories and approximate number of Data Subjects and records concerned, the likely consequences, and the measures taken or proposed. Where information is not available at once, it may be provided in phases without undue further delay.

9.3 A notification under this clause is not an acknowledgement by Solidtime of fault or liability in respect of the Personal Data Breach.

10. Return and Deletion of Data

10.1 On termination or expiry of the Agreement, Solidtime, at the Customer's choice, deletes or returns all Customer Personal Data and deletes existing copies, unless Union or Member State law requires continued storage.

10.2 Customer Personal Data is deleted without undue delay, subject to clause 10.1. Backups are deleted in the ordinary course of Solidtime's backup-rotation cycle, during which they remain inaccessible for ordinary use.

10.3 The Customer is responsible for exporting Customer Personal Data before termination or expiry of the Agreement where the Service makes export functionality available.

11. Audits

11.1 Solidtime makes available to the Customer the information reasonably necessary to demonstrate compliance with its obligations under Article 28 GDPR. Where that information does not reasonably address the Customer's audit request, Solidtime allows for and contributes to an audit conducted by the Customer or an auditor it mandates, subject to the conditions in this clause.

11.2 Audits take place on reasonable prior notice (at least 30 days, except where a Supervisory Authority requires otherwise), during business hours, no more than once per year (unless a Personal Data Breach or Supervisory Authority requirement justifies more), subject to confidentiality, and subject to measures to avoid disruption to Solidtime's operations and to protect the data, systems, security, confidentiality, and trade secrets of other customers. Solidtime may satisfy audit requests by providing relevant certifications, third-party audit reports, or documentation of its security measures where these reasonably address the Customer's request.

11.3 Any audit or inspection is conducted at the Customer's expense, including Solidtime's reasonable costs of supporting it, and in a manner that minimises disruption to Solidtime's operations.

12. International Transfers

12.1 Solidtime shall not transfer Customer Personal Data outside the European Economic Area unless appropriate safeguards are in place in accordance with Data Protection Law.

12.2 Some Sub-processors may be established outside the European Economic Area even where Customer Personal Data is stored or primarily processed in the European Union. Where Customer Personal Data is transferred to or accessed from a country outside the EEA that is not subject to an adequacy decision, Solidtime shall ensure that appropriate safeguards are in place in accordance with Data Protection Law, such as the European Commission's Standard Contractual Clauses and, where required, supplementary measures.

13. Liability

13.1 Each Party's liability under or in connection with this DPA is subject to the limitations and exclusions of liability set out in the Agreement.

13.2 Nothing in this DPA limits either Party's liability where, and to the extent that, such limitation is not permitted by Data Protection Law.

13.3 Solidtime is not liable for any claim, loss, or damage arising from the Customer's instructions, the Customer's configuration or use of the Service, the Customer's failure to comply with Data Protection Law, or any use of the Service outside the scope of the Agreement.

14. Term

14.1 This DPA takes effect on the date the Agreement comes into force and continues for as long as Solidtime Processes Customer Personal Data, notwithstanding expiry or termination of the Agreement.

15. General

15.1 This DPA is governed by the law specified in the Agreement, or failing that, the law of Austria.

15.2 If any provision is held invalid, the remainder continues in effect.

15.3 The Annexes form an integral part of this DPA.

15.4 In the event of a conflict between this DPA and the Agreement, this DPA prevails with respect to the Processing of Customer Personal Data.

15.5 Where the European Commission's Standard Contractual Clauses apply to a transfer of Customer Personal Data, those clauses prevail over this DPA to the extent of any conflict in respect of that transfer.

16. Acceptance

This DPA is incorporated into and forms part of the Agreement and takes effect when the Customer accepts the Agreement — no signature is required for it to be binding. A Customer that requires a countersigned copy may request one at hello@solidtime.io.

Annex 1 — Details of the Processing

Subject matter: Provision of the Solidtime time-tracking Service to the Customer.

Duration: For the term of the Agreement and any post-termination period required to return or delete data (clause 10).

Nature and purpose of Processing: Hosting, storage, organisation, retrieval, transmission, and deletion of Customer Personal Data for the purpose of enabling the Customer's authorised users to record, manage, and report on time, projects, and tasks.

Categories of Data Subjects:

- The Customer's employees, contractors, and freelancers
- Other individuals the Customer authorises to access or who are recorded in the Service (e.g. team members, project members)

Types of Personal Data:

- Identification and contact data: name, email address, user ID
- Authentication data: hashed passwords, session/access tokens
- Organisational data: team/organisation membership, role, billable rate (where entered)
- Time-tracking data: time entries, start/end timestamps, durations, descriptions of work, project and task assignments, tags
- Technical and usage data: IP address, device/browser information, log data

Special Categories of Personal Data: None. As set out in clause 2.5, the Customer must not enter Special Categories of Personal Data or criminal-offence data into the Service absent Solidtime's prior written agreement.

Annex 2 — Technical and Organisational Measures

This Annex describes the technical and organisational measures in place at the date of this DPA. Measures may be updated over time, provided the level of protection is not materially reduced.

Encryption and transmission

- Customer Personal Data is encrypted in transit using TLS.

Access control

- Access to production systems and the database is limited to authorised personnel.
- Within the Service, role-based access control assigns users to roles (e.g. organisation owner, member) with distinct permissions, governing what each user can access and do.

Logging and monitoring

- The Service logs user actions on data, including create, update, and delete operations, and logs equivalent administrative actions.
- Application errors and performance issues are monitored via Sentry (EU region).

Tenant separation

- The Service operates on a shared, multi-tenant database. Each customer's data is logically separated and scoped to its organisation, with separation enforced at the application layer.

Software and vulnerability management

- Source code is developed in a public repository; security issues can be reported to the partners, who review and address them.
- Dependencies and systems are kept up to date, with security-relevant updates applied.

Confidentiality and personnel

- Personnel with access to Customer Personal Data are bound by confidentiality. At present this is limited to the two partners; any future staff or contractors with such access will be subject to equivalent confidentiality obligations.

Availability and resilience

- Regular backups are maintained and stored offsite (OVH).
- Backups are stored encrypted at rest.

Sub-processor and datacentre security

- Production infrastructure and data are hosted with established European providers (Scaleway, OVH, Hetzner) that provide physical and environmental security for their datacentres.

Incident response

- Personal Data Breaches affecting Customer Personal Data are notified to the Customer without undue delay, in accordance with clause 9.

Annex 3 — Authorised Sub-processors

The current, authoritative list of authorised Sub-processors — including each Sub-processor's purpose and location — is published on our Sub-processor page. Solidtime notifies the Customer of any addition or replacement of a Sub-processor in accordance with clause 6.4, and the published page governs.

Signatures

This Data Processing Agreement is binding once the Customer accepts the Agreement; a signature is not required for it to take effect (clause 16). This page is provided for customers that require a countersigned copy. Complete and sign below, then email the PDF to hello@solidtime.io — we will countersign and return a fully executed copy.

The Customer

SIGNATURE

FULL NAME

TITLE

DATE

solidtime GesbR

To be countersigned by solidtime on receipt.

Gregor Vostrak — Partner

SIGNATURE

DATE

Constantin Graf — Partner

SIGNATURE

DATE