

Data Processing Agreement

Last updated: 17.8.2026

This Data Processing Agreement ("DPA") forms part of the Terms of Service ("Agreement") between:

- **Aiso Oy** ("Aiso", "Processor"), Business ID 2960709-2, Insinöörinkatu 30, 2nd floor, 33720 Tampere, Finland; and
- **The Customer** identified in the Aiso account ("Customer", "Controller")

By accepting the Terms of Service, the Customer also accepts and agrees to this DPA. This DPA governs the processing of Personal Data by Aiso on behalf of the Customer in connection with the TimeNTable service.

In the event of any conflict between this DPA and the Agreement, this DPA prevails in matters relating to the processing of Personal Data.

1. Definitions

Capitalised terms not defined here have the meaning given in the GDPR or in the Agreement.

- **Personal Data:** Any information relating to an identified or identifiable natural person processed by Aiso on behalf of the Customer through the Service.
- **Data Subject:** The individual to whom Personal Data relates, primarily Guests.
- **Sub-processor:** Any third party engaged by Aiso to process Personal Data on behalf of the Customer.
- **Service:** The TimeNTable reservation management service.
- **Privacy Policy:** The Aiso privacy policy available at <https://timentable.fi/privacy>, as updated from time to time.

2. Roles and scope

Aiso processes Personal Data only on behalf of the Customer for the purpose of providing the Service. The Customer is the Controller of such Personal Data, and Aiso is the Processor.

The subject matter, duration, nature, purpose, categories of data, and categories of Data Subjects are described in **Annex 1** (Processing Details).

This DPA does not apply to:

- Personal Data of the Customer's End Users and staff, for which Aiso is a Controller (see Privacy Policy)

- Aggregated and anonymised data generated by Aiso under the Agreement, which does not constitute Personal Data
- Personal data that Aiso processes as a Controller for its own purposes, namely cookieless measurement of the use of the Service, security and abuse prevention, and billing. Such processing is described in the Privacy Policy and is not carried out on behalf of the Customer.

3. Customer responsibilities

The Customer:

- Determines the purposes and means of processing Personal Data through the Service
- Ensures that a valid legal basis exists for processing Personal Data, including any sensitive data such as allergy or dietary information
- Provides Data Subjects with appropriate privacy information
- Responds to Data Subjects' requests to exercise their rights
- Ensures that any Personal Data provided to the Service complies with applicable law

4. Aiso's obligations

Aiso shall:

- Process Personal Data only as documented in this DPA and the Agreement.
- Ensure that personnel authorised to process Personal Data are bound by confidentiality obligations
- Implement appropriate technical and organisational measures as set out in **Annex 2** (Technical and Organisational Measures)
- Assist the Customer in responding to Data Subject requests, to the extent reasonably practicable through the Service
- Assist the Customer with compliance obligations under Articles 32 to 36 of the GDPR, taking into account the nature of processing and information available to Aiso

Data Subject rights in respect of Personal Data processed on behalf of the Customer are exercised against the Customer as Controller, and Aiso does not respond to such requests on the merits. If Aiso receives a request from a Data Subject directly, Aiso shall forward the request to the Customer without undue delay and shall not respond except to confirm receipt and refer the Data Subject to the Customer.

Unlawful instructions. Aiso shall inform the Customer without undue delay if, in Aiso's opinion, an instruction given by the Customer infringes the GDPR or other applicable data protection law. Aiso may suspend performance of the instruction until the Customer confirms or withdraws it.

Instructions. The Customer may give additional documented instructions concerning the processing of Personal Data by written notice to info@timentable.fi. Aiso shall implement instructions that are consistent with the Service and with applicable law, and may decline

instructions that are technically unfeasible or that would require changes to the Service. Where an instruction, or assistance with a Data Subject request, requires work beyond the standard functionality of the Service, Aiso may charge for the work at its then-current hourly rate.

Integrations. Where an integration with a third-party service is activated for the Customer, whether by the Customer or by Aiso at the Customer's request, that constitutes the Customer's documented instruction to Aiso to disclose to that third party the reservation data necessary for the integration. A request to activate an integration shall be made in writing or through the Service. The third party processes that data as an independent controller and is not a Sub-processor.

5. Sub-processors

The Customer authorises Aiso to engage Sub-processors to process Personal Data, subject to this Section.

A current list of approved Sub-processors is set out in **Annex 3** (Approved Sub-processors).

Aiso shall:

- Impose contractual obligations on Sub-processors no less protective than those in this DPA
- Remain liable to the Customer for the acts and omissions of its Sub-processors, subject to Section 11

Aiso shall notify the Customer of any intended addition or replacement of a Sub-processor at least **fifteen (15) days** before the change takes effect. The Customer may object to the change on reasonable, documented data protection grounds within that period. If the Customer objects, the parties shall discuss in good faith. If no resolution is reached, the Customer may terminate the Agreement before the new Sub-processor begins processing, and Aiso shall refund the pro-rata portion of prepaid subscription fees for the period after termination. This is the Customer's sole remedy in respect of a change of Sub-processor.

Where a change of Sub-processor is required urgently to address a security threat, or because a Sub-processor ceases to provide its service, Aiso may make the change and notify the Customer as soon as practicable thereafter.

6. Location of processing and international transfers

Aiso hosts the Service, including its database and file storage, on infrastructure located within the European Union.

In addition to the Service, Aiso uses business tools for customer support, internal communication, and document storage. Personal Data may be processed in those tools where it is transmitted to Aiso by the Customer, an End User, or a Data Subject, or where it is included in support or incident material. Those tools are listed in **Annex 3**.

Personal Data may be transferred outside the European Economic Area (EEA) where an integration with a third party located outside the EEA is activated for the Customer, whether by the Customer or by Aiso at the Customer's request, or where a Sub-processor listed in Annex 3 is established outside the EEA or belongs to a group established outside the EEA.

Where Personal Data is transferred outside the EEA, the transfer is carried out on the basis of an adequacy decision or, where no adequacy decision applies or ceases to apply, the European Commission's Standard Contractual Clauses or another transfer mechanism permitted under Chapter V of the GDPR.

7. Security

Aiso implements and maintains the technical and organisational measures described in **Section 8 of the Privacy Policy** (<https://timentable.fi/privacy>) to ensure a level of security appropriate to the risk. Those measures are incorporated into this DPA by reference and form part of Aiso's obligations as Processor.

The Customer acknowledges that those measures are adequate for the Personal Data processed through the Service. Where the Customer determines that additional measures are required, the parties shall discuss in good faith.

8. Personal data breach

Aiso shall notify the Customer of any Personal Data breach affecting Personal Data processed on behalf of the Customer without undue delay after becoming aware of it. For the purposes of this Section, Aiso becomes aware of a Personal Data breach when it has established a reasonable degree of certainty that a security incident has occurred that has led to Personal Data being compromised.

The notification shall include, to the extent known:

- The nature of the breach, including the categories and approximate number of Data Subjects and records affected
- The likely consequences of the breach
- The measures taken or proposed to address the breach and mitigate adverse effects
- Contact information for further inquiries

Aiso shall reasonably assist the Customer in fulfilling its breach notification obligations under Articles 33 and 34 GDPR.

Aiso shall document Personal Data breaches, including their effects and the remedial action taken, and shall make that documentation available to the Customer on request to the extent it concerns Personal Data processed on behalf of the Customer.

Aiso shall not notify a supervisory authority or any Data Subject of a Personal Data breach on the Customer's behalf, and shall not communicate with the Customer's Guests about a

breach, unless the Customer instructs Aiso in writing to do so or Aiso is required to do so by law in its own capacity.

A notification under this Section is not an admission of fault or liability.

9. Audits and inspections

Aiso shall make available to the Customer information necessary to demonstrate compliance with this DPA and shall allow for audits conducted by the Customer or a third-party auditor mandated by the Customer, subject to the following:

- Audits may be carried out **once per calendar year**, except where required more frequently by a supervisory authority or following a confirmed Personal Data breach
- The Customer shall give Aiso at least **30 days' written notice** before any audit
- Audits shall be conducted during normal business hours and shall not unreasonably interfere with Aiso's operations
- Audits shall not include penetration testing or vulnerability scanning, or access to systems, data, or premises to the extent that such access would compromise the security or confidentiality of another customer's data or of Aiso's own confidential information
- The auditor must be bound by appropriate confidentiality obligations, and shall not be a competitor of Aiso
- The Customer bears the costs of the audit, including Aiso's reasonable costs for time spent supporting it and any charges imposed by a Sub-processor for providing information or supporting the audit, except where the audit reveals material non-compliance by Aiso
- Aiso may satisfy the audit obligation by providing the Customer with a written response to a reasonable security questionnaire, or a recent independent audit report or certification (such as SOC 2 or ISO 27001), where available

Aiso shall procure from its Sub-processors information and audit rights equivalent to those in this Section, and shall make the resulting information available to the Customer, so that the Customer's rights under Article 28(3)(h) GDPR are satisfied in respect of Sub-processors. Audits of Sub-processors are conducted through Aiso and not directly by the Customer, unless a supervisory authority requires otherwise.

10. Retention and deletion

Aiso retains Personal Data only for the periods set out in **Section 4 of the Privacy Policy** (<https://timentable.fi/privacy>), which are incorporated into this DPA by reference.

Aiso may delete Personal Data earlier upon a valid Data Subject request handled through the Customer.

Upon termination of the Agreement, Personal Data is deleted in accordance with Section 4 of the Privacy Policy and the switching and exit provisions of the Agreement, unless retention is required by law.

11. Liability

The liability of each party under this DPA is governed by, and counts towards, the limitation of liability provisions in **Section 14 of the Agreement**. Claims under this DPA and under the Agreement are subject to a single aggregate cap.

As between the parties, Aiso is liable for damage caused by processing only where Aiso has not complied with obligations of the GDPR specifically directed to processors, or has acted outside or contrary to the Customer's lawful instructions, in accordance with Article 82(2) GDPR.

12. Term

This DPA takes effect on acceptance of the Agreement and remains in effect for as long as Aiso processes Personal Data on behalf of the Customer.

13. Changes to this DPA

Aiso may update this DPA, including its Annexes. Changes that do not reduce the Customer's rights or increase its obligations, including clarifications, corrections, structural changes, and changes required by law or by a competent authority, take effect when published.

Other changes take effect fifteen (15) days after Aiso notifies the Customer by email or in-product notice.

Changes to Annex 3 (Sub-processors) are governed by Section 5.

Where this DPA incorporates sections of the Privacy Policy by reference, Aiso may amend that content only in accordance with this Section, and no amendment shall materially reduce the level of protection of Personal Data or extend a retention period applicable to Personal Data processed on behalf of the Customer.

14. Governing law

This DPA is governed by the laws of Finland and is subject to the jurisdiction provisions set out in the Agreement.

Annex 1: Processing Details

Item	Description
Subject matter	Provision of the TimeNTable reservation management service to the Customer

Item	Description
Duration	For the term of the Agreement, plus the retention periods set out in the Privacy Policy
Nature of processing	Storage, transmission, display, organisation, and deletion of Personal Data through a reservation system
Purpose	Enabling the Customer to receive, manage, and track table reservations from its Guests
Categories of Data Subjects	Guests (individuals who make reservations at the Customer's restaurant)
Categories of Personal Data	Name, email address, phone number, reservation records (date, time, party size, table assignment, status, language, free-text notes), optional dietary or allergy information
Special categories of data	The Customer may collect dietary or allergy information from Guests where Guests choose to provide it. Such data may include information that constitutes data concerning health under Article 9 GDPR, and is retained for the period set out in Section 4 of the Privacy Policy. The Customer is responsible for the lawful basis for such processing, including obtaining explicit consent where required.
Frequency of processing	Continuous during the term of the Agreement
Retention	As set out in Section 4 of the Privacy Policy
Independent recipients	Where an integration is activated for the Customer, whether by the Customer or by Aiso at the Customer's request, reservation data is disclosed to the third party concerned, which processes it as an independent controller. Such third parties are not Sub-processors and are not listed in Annex 3.

Annex 2: Technical and Organisational Measures

The technical and organisational measures implemented by Aiso to protect Personal Data are described in detail in **Section 8 of the Privacy Policy** (<https://timentable.fi/privacy>). Those measures are incorporated into this DPA by reference.

The Privacy Policy describes measures across the following areas:

- Confidentiality (encryption in transit, encryption at rest where supported by the infrastructure provider, authentication and credential storage, restriction of personnel access, separation of each Customer's data)
- Integrity (application-level access controls, separate credentials for administrative and application access to the database)
- Availability (backups taken by the hosting infrastructure provider, monitoring of availability and performance)
- Testing and maintenance (periodic review of access rights and security practices, regular installation of updates and security patches)
- Organisational measures (confidentiality obligations for personnel, instruction and training on data protection and security, documented procedure for handling Personal Data breaches)

Annex 3: Approved Sub-processors

The following Sub-processors are approved as of the date of this DPA.

Sub-processor	Role	Location
Scaleway SAS	Hosting, managed database, object storage, and transactional email delivery	France (EU)
Google Cloud EMEA Limited	Business productivity tools used in customer support and incident handling: document storage, spreadsheets, and email	Ireland (EU), with transfers to the United States
Slack Technologies Limited	Internal communication used in customer support and incident handling	Ireland (EU), with transfers to the United States

Aiso may update this list in accordance with Section 5 of this DPA.

Aiso Oy Business ID: 2960709-2 VAT: FI29607092 Insinöörinkatu 30, 2nd floor, 33720 Tampere, Finland info@timentable.fi

