

FOR CUSTOMERS

Data processing agreement

FinnStella service · Version 1.0 · 23 October 2026

This data processing agreement is part of the FinnStella service agreement. It describes how Namu Solutions OÜ processes personal data on behalf of a customer company that uses FinnStella. It meets the requirements of Article 28 of the EU General Data Protection Regulation (GDPR).

1. Parties and roles

The **controller** is the customer company that uses FinnStella. It decides what data is stored in the service and what it is used for.

The **processor** is Namu Solutions OÜ (registry code 16190853, Lootsi 3a, Tallinn, Estonia), which provides the FinnStella service and processes data only on the customer's behalf.

2. Subject matter, nature and duration

Personal data is processed so that the customer can plan and run its activity services: departures, bookings, pickups, staff rotas and hours, equipment maintenance, animal farm work and safety records. Processing includes storing, organising, showing data to users, sending notifications, backing up and deleting.

Processing lasts for as long as the customer has a valid FinnStella agreement, and after that for the period set out in section 10.

3. Data subjects and categories of data

- **The customer's staff** (guides, drivers, planners and other users): name, contact details, role, shifts, hours, absences, login data and authorship of entries.
- **The customer's guests** (safari participants and bookers): the booker's name and contact details, booking details, number of people, hotel and pickup details, and guide messages.
- **Health data** (special category): health or safety information given by the guest, such as allergies or limitations. It is removed from everyday view after the safari within a time chosen by the customer.
- **Safety and maintenance records**: observations, incidents, fault reports and photos, with their timestamps and authors.

4. Customer instructions

We process personal data only on the customer's documented instructions. These consist of the FinnStella agreement, this agreement and the choices the customer makes in the service. If we believe an instruction infringes data protection law, we will tell the customer without delay.

5. Confidentiality

Personal data is processed only by people whose duties require it, and they are bound by confidentiality.

6. Security

- Each customer company's data is isolated at database level with row-level access rules.
- Access is role-based: everyone sees only what their work needs.
- Traffic is encrypted (TLS), and the database is encrypted at rest.
- Administrators sign in with two-factor authentication.
- Health data is removed from everyday view automatically within the time chosen by the customer.
- Safety records cannot be changed afterwards.
- Data is backed up daily, and backups are kept in the EU.

7. Sub-processors

The customer gives general authorisation to use the sub-processors listed below. Each of them is bound by data protection obligations at least equal to those in this agreement.

Sub-processor	Purpose	Location
Supabase, Inc.	Database, authentication and file storage	EU (Sweden)
Cloudflare, Inc.	Delivery of the app and website, security	Global network; transfers under DPF / SCCs
Functional Software, Inc. (Sentry)	Error monitoring	USA; transfers under DPF / SCCs
Sendinblue SAS (Brevo)	System emails	EU (France)
Google (Google Workspace)	Support correspondence by email	EU / USA; transfers under DPF / SCCs

We will notify the customer of new or replaced sub-processors at least 30 days in advance. The customer may object on reasonable grounds, and if the matter cannot be resolved, the customer may terminate the agreement.

8. Transfers outside the EU

The database is located in the EU. Where a sub-processor processes data outside the EU, the transfer is based on the EU–US Data Privacy Framework (DPF) or the European Commission's standard contractual clauses.

9. Assistance and personal data breaches

- We help the customer respond to data subject requests, such as access, rectification and erasure. The customer can do most of this directly in the app.
- We help, where needed, with security assessments and data protection impact assessments.

- We notify the customer of a personal data breach we become aware of without undue delay and no later than 48 hours. The notice describes what happened, what data is affected and what we have done.

10. Return and deletion of data

The customer can export all of its data from the app as JSON at any time. When the agreement ends, the data is deleted from the service within 30 days unless the law requires it to be kept. Data is removed from backups as they rotate.

If the FinnStella service is ever discontinued, we will give at least six months' notice, and the customer will receive all of its data.

11. Audits

On request we give the customer the information needed to demonstrate compliance with this agreement. The customer may have an audit carried out at its own cost, agreed reasonably in advance.

12. Liability and governing law

Liability and governing law are set out in the FinnStella agreement. If this agreement and the FinnStella agreement conflict regarding the processing of personal data, this agreement prevails.

Contact

Data protection questions: info@finnstella.com