Fundify Invest OÜ

PERSONAL DATA PROCESSING TERMS

(Privacy Policy)

Version 3.2 • Effective date: 08.12.2026

Document information	
Controller	Fundify Invest OÜ
Registry code	12741150
E-mail	info@gpslahendused.ee
Website	gpslahendused.ee / mynav.gpslahendused.ee
Document version	3.2
Valid from	08.12.2026

1. General provisions and regulation

This privacy policy explains how Fundify Invest OÜ (hereinafter the "Company") collects, processes, stores and protects personal data in the provision of the tracking service on the MyNav platform.

Personal data are processed in accordance with:

- Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation, GDPR), applicable from 25 May 2018;
- the Estonian Personal Data Protection Act (IKS);
- the Estonian Electronic Communications Act;
- other applicable legislation of the European Union and Estonia.

2. Definitions

The following definitions are used in this privacy policy:

- Personal data – any information relating to an identified or identifiable natural person, including location data that enable a person to be identified directly or indirectly.
- Controller – Fundify Invest OÜ, which determines the purposes and means of the processing of personal data.
- Processor – a company or person that processes personal data on behalf of and on the instructions of the controller.
- Data subject – a natural person whose personal data are processed (e.g. a driver).
- Client – a legal or natural person who uses the tracking service on the MyNav platform.
- Service – MyNav, the vehicle tracking platform, including the web interface and mobile application.

3. Role and responsibility of the data processor

In the provision of the GPS tracking service, the Company acts in two roles:

3.1 As a processor in relation to clients: The Company processes, on behalf of clients (controllers), the location data of their employees and drivers, on the basis of the data processing agreement concluded with the clients (GDPR Article 28).

3.2 As a controller: The Company processes clients' contact data, user account data and other information necessary for the provision of the service on its own responsibility. If a Client (a natural person) uses the Service solely to track their own vehicle(s) and has not created additional users in the Service, the Company is also the controller of their location data. If the Client creates additional users in the Service or tracks vehicles used by other persons (e.g. family members, employees, drivers), the Company is the processor of those persons' data (see clause 3.1).

3.3 Source of data in the case of drivers and employees

The personal data of drivers and employees are not collected by the Company directly from the data subjects, but are transmitted to the Company by the Clients (employers). The Client is responsible for informing the data subjects (employees, drivers) in accordance with GDPR Articles 13–14 before the data are transmitted to the Company. The Company processes these data solely on the basis of the agreement and the data processing agreement concluded with the Client.

4. Categories of personal data processed

4.1 Data of clients' representatives

- Name, e-mail address, telephone number
- Login data (username, encrypted password)
- User activity log in the service
- Billing data: invoices, billing address and data on the service package and payment history (the Company does not process or store payment card data)

4.2 Data of drivers and employees (on behalf of the client)

- GPS location data in real time and historically
- Vehicle movement data: speed, direction, stops, route
- Vehicle technical status: ignition state, engine operating hours, mileage
- Events related to the vehicle: alarms, warnings, limit exceedances
- Time usage data: working time, rest time, duration of stops
- Driver identification data: the driver's name and driver identifier (driver card or button), if the Client has taken driver identification into use
- Mobile cell positioning (LBS) data: the identifiers of the mobile cell towers visible to the device, on the basis of which an approximate location is calculated when the GPS signal is unavailable

4.3 For technical purposes of the service

- Log files and security incident data
- The log files contain the IP address, the time of the request, the browser or application used and the result of the request; logs are retained for up to 90 days
- Service usage statistics (anonymous)

5. Purposes and legal bases of data processing

Purpose	Legal basis (GDPR Art. 6)	Retention period
Provision of the GPS tracking service	Art. 6(1)(b) – contract	According to the client's settings (default 3 months)
Management of the client relationship	Art. 6(1)(b) – contract	Duration of the agreement + 3 years
Ensuring the security of the service	Art. 6(1)(f) – legitimate interest	Up to 90 days
Legal obligations (accounting)	Art. 6(1)(c) – legal obligation	7 years (Accounting Act)
Sending notifications and alarms	Art. 6(1)(b) – contract	According to the client's settings
User activity log in the service	Art. 6(1)(f) – legitimate interest	According to the security policy

Clarification of legitimate interest (Art. 6(1)(f)): In ensuring the security of the service, the Company has a legitimate interest in protecting the service against misuse, unauthorised access and technical faults. The data subject has the right to receive information on the results of the balancing test carried out, by contacting info@gpslahendused.ee.

6. Retention and deletion of data

Location data are retained according to the period configured by the client. The default retention period is 3 months from the collection of the data. The retention period is 3 – 12 months according to the package chosen by the client.

Upon termination of the service agreement, the client's data are deleted within 30 days, except where a longer retention obligation arises from law. For a self-service subscription, the account and data are deleted in accordance with clause 16.7 of the Service Terms.

The notification dispatch log is retained for 30 days. The last 50 notifications per user are displayed to the user in the Service. Automatic deletion of data takes place daily according to the configured retention period.

7. Data security

The Company applies appropriate technical and organisational measures to protect personal data in accordance with GDPR Article 32. The measures applied include:

- Encryption of data in transit (TLS 1.2/1.3 protocol)
- Role-based access control and automatic blocking of login attempts
- Regular backups, which are encrypted (GPG) before being stored at a sub-processor
- System access protection and monitoring
- Regular security updates and audits
- Network-level protection: firewall and traffic filtering
- Retention of access logs for auditing
- Security incident handling procedure

More detailed technical security measures are not disclosed for security reasons.

7a. Automated processing and profiling

The Service processes location and telematics data automatically in order to generate notifications (e.g. speeding, geofence events, ignition state, start and end of movement). Such automated processing does not constitute automated decision-making within the meaning of GDPR Article 22 that would produce significant legal effects concerning the data subject. Automatically generated notifications are of an informational nature only, and final decisions are always made by the Client (the employer).

8. Transfer of data to third parties

The Company does not sell or rent personal data to third parties. Data may be transferred:

- To data processors (sub-processors) providing services to the Company (e.g. cloud infrastructure, push notifications, mobile cell positioning, storage of encrypted backups, e-mail delivery) – protected by a data processing agreement under GDPR Art. 28; some of them are located outside the EEA (see the end of this clause);
- To state authorities, where this is a legal obligation;
- To the Client itself regarding its own data.

Some of the data processors used by the Company (cloud infrastructure, push notifications, mobile cell positioning, storage of encrypted backups) are located in the United States, and personal data may be transferred through them outside the European Economic Area (EEA). For all such transfers, appropriate safeguards under Chapter V of the GDPR are ensured: the EU-US Data Privacy Framework (DPF) and additionally the European Commission standard contractual clauses (SCC, implementing decision 2021/914). The remaining data processing takes place in the European Union. The Company does not transfer personal data to countries lacking an adequate level of data protection without appropriate safeguards. An up-to-date list of data processors is available from the Company upon written request.

For the protection and delivery of web traffic, the Company uses the service provider Cloudflare, which processes the IP addresses of requests made to the Service. The safeguards referred to in this clause also apply to that transfer.

To process payments for self-service subscriptions, the Company uses the service provider Stripe. The client enters payment card details directly on Stripe's page, and the Company neither sees nor stores them. Stripe processes payment data in accordance with its own privacy policy.

8.1 Sharing of location at the Client's own choice

The Service allows the Client to share the location of a vehicle with persons of the Client's own choosing by means of a sharing code, a link or a QR code. Sharing is started and ended by the Client, and the shared view displays only the location and movement of the vehicle selected by the Client during the period the Client has specified. Sharing can be revoked at any time, after which the code and the link no longer work. The Company does not use the shared data for any other purpose.

In addition, as an additional service, the Client can create a link and QR code to a public live map. Anyone who has the link can view this map without logging in and without a code, and the link remains valid until the Client deletes it. The map displays the location, movement status and direction of the vehicles selected by the Client, together with the name and icon set by the Client. The Client can stop sharing at any time and set a schedule for when sharing starts and ends. The Client is responsible for ensuring that making the location public is permitted.

9. Rights of the data subject

In accordance with the GDPR, the data subject has the following rights:

- Right to be informed – the right to know which data are processed and for what purpose (Art. 13–14);
- Right of access to data – the right to receive a copy of one's personal data (Art. 15);
- Right to rectification of data – correction of inaccurate data (Art. 16);
- Right to erasure of data – the so-called “right to be forgotten” (Art. 17);
- Right to restrict processing (Art. 18);
- Right to data portability (Art. 20);
- Right to object to processing (Art. 21). Where personal data are processed on the basis of legitimate interest (Art. 6(1)(f)), the data subject has the right to object on grounds relating to their particular situation. In that case the Company ceases the processing of the data, unless there are compelling legitimate grounds for the processing which override the interests of the data subject.

To exercise your rights, please contact: info@gpslahendused.ee

We respond to requests within 30 days. For more complex requests, the period may be extended up to 60 days, of which we will notify you.

10. Personal data breaches

As a controller, in the event of a personal data breach the Company notifies the Data Protection Inspectorate within 72 hours of becoming aware of the breach, where the breach poses a risk to the rights and freedoms of individuals (GDPR Art. 33). As a processor (in respect of the data of clients' employees and drivers), the Company notifies the relevant Client (controller) of the breach without undue delay, but no later than within 48 hours of becoming aware of the breach, so that the Client can fulfil its 72-hour obligation under GDPR Art. 33(1).

If the breach poses a high risk to the data subjects, the data subjects concerned are also notified without undue delay (GDPR Art. 34).

11. Cookies and use of the website

In the use of the MyNav web service, only session cookies necessary for the functioning of the service are used:

Cookie	Purpose	Duration
JSESSIONID / session cookie	User authentication and session management	Until the end of the session (browser is closed)

Statistical, advertising or tracking cookies are not used. Session cookies are deleted automatically when the browser is closed. As these cookies are strictly necessary for the functioning of the service, no separate consent is required for their use (Electronic Communications Act § 103[1]).

12. Lodging complaints

The data subject has the right to lodge a complaint with the Data Protection Inspectorate if they consider that the processing of their personal data infringes the requirements of the GDPR.

Supervisory authority	
Name	Data Protection Inspectorate (AKI)

Address	Tatari 39, 10134 Tallinn, Estonia
E-mail	info@aki.ee
Website	www.aki.ee
Telephone	+372 627 4135

13. Amendment of the privacy policy

The Company has the right to amend this privacy policy. In the case of material changes, we notify clients by e-mail at least 30 days in advance. The current version is always available on the website gpslahendused.ee.

14. Contact details

Contact for data processing matters	
Company	Fundify Invest OÜ
E-mail	info@gpslahendused.ee
Website	gpslahendused.ee
Service admin interface	mynav.gpslahendused.ee
Data protection officer (DPO)	The Company has assessed the need to designate a data protection officer under GDPR Art. 37. Considering the volume of data processed and the size of the company, the designation of a DPO is not currently mandatory. For data protection matters, please contact: info@gpslahendused.ee

15. Mobile applications

The Company provides two mobile applications, the data processing of which differs.

15.1 MyNav

MyNav is the management application of the Service. The application requests the location permission in order to display the user's own position on the map and to use navigation, ride recording and the SOS alert. For display on the map, location is used only on the device. Location is sent to the Company's server only when the user uses the following functions. During navigation, the start point, destination, direction and speed are sent in order to calculate the route, and they remain in the log files together with the user identifier for the period stated in clause 4.3. When the “My location” function is used, the coordinates are sent in order to find the address. The track of a saved ride is kept in the user's account. When an SOS alert is sent, the user's location is stored for 30 days and forwarded to the users with whom they have shared a vehicle. During navigation, the application also uses location with the screen locked and when connected to Android Auto or CarPlay; at other times the application does not collect location in the background. The camera is used for reading the QR code of a sharing code and

for photographing roadbook pages. Roadbook images are sent to the Company's server to read the text and are not passed on to third parties; temporary files are deleted within 6 hours at the latest, and a roadbook saved by the user remains in their account. For the delivery of notifications, the notification identifier of the device (push token) is processed. If the application fails, a technical error report is sent to the Firebase Crashlytics service (Google), which is used solely for fixing errors.

15.2 MyNav Client

MyNav Client is intended for using a phone as a tracking device. The application collects precise location only after the user has started tracking themselves, and sends it solely to the user's own MyNav account on the Company's server. Location is also collected in the background, including when the screen is switched off, for as long as tracking is switched on; this is the core function of the application. The battery level and charging state of the device are transmitted together with the location. Motion sensor data are used solely in order to determine whether the device is moving and to reduce the number of location requests; these data are neither stored nor transmitted. The camera is used only for reading the QR code used for pairing. The PIN code is set by the owner in MyNav; the Company's server keeps only a hash of it and verifies the PIN code entered. For the delivery of notifications and server control commands, the notification identifier of the device (push token) is processed. To resolve faults, the application sends a technical diagnostic log to the server, which is retained for up to 30 days. The user can stop tracking and unpair the device at any time, after which the application no longer sends location.

15.3 Common principles

Neither application uses advertising identifiers, displays advertising or transmits personal data to third parties for advertising or analytics purposes. The deletion of data can be requested at info@gpslahendused.ee.