

Privacy Policy

Effective from 10 October 2025

Preamble

SETECH FLOTTA Kft considers it important to protect personal data of those who come into contact with it and to respect the right to informational self-determination.

To this end, SETECH FLOTTA Kft, taking into account the relevant

- the acts in force in the European Union, primarily Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, hereinafter: **GDPR**), as well as
- domestic legislation, including Act CXII of 2011 on the right to self-determination in relation to information and freedom of information (hereinafter: **Info Act**), Act CVIII of 2001 on certain issues relating to electronic commerce services and information society services,
- Act LXVII of 2013 on the distance-based toll payable for the use of motorways, expressways and main roads (hereinafter: **Udvt**) and its implementing decrees, in particular Government Decree 209/2013. (VI. 18.) Government Decree (hereinafter: **Udvt**)

, establishes the following data protection policy:

1. Subject matter of the policy

The subject matter of this Policy is to regulate the personal data processing practices of SETECH FLOTTA Kft. as a data controller as defined in Article 4(7) of the GDPR (hereinafter: **Company** or **Data Controller**).

2. Scope of the policy

The scope of these Regulations extends to the members, officers and agents of the Company, as well as all data recorded by legal and non-legal entities for the purpose of achieving the Company's objectives and carrying out its activities.

3. Interpretative provisions

For the purposes of these Regulations:

3.1. *Personal data:*

Any information relating to an identified or identifiable natural person ('data subject'); A natural person can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (Article 4(1) of the GDPR).

3.2. *Data processing:*

Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (GDPR Article 4(2)).

3.3. *Data controller:*

A natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law (GDPR Article 4(7)).

3.4. *Processor:*

A natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller (GDPR Article 4(8)).

3.5. *Consent of the data subject:*

Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her (Article 4(11) of the GDPR).

3.6. *Data breach:*

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed (GDPR Article 4(12)).

3.7. Enterprise:

A natural or legal person engaged in economic activity, regardless of its legal form, including partnerships and companies engaged in regular economic activity (GDPR Article 4(18)).

4. Data controller, data processors and their contact details

Data controller's details and contact information:

- Name: **SETECH FLOTTA Kft**
- Represented by: Csaba Potoczky, managing director
- Registered office: 2161 Csomád, Liget utca 40.
- Postal address: u.a
- Registration number: 13 09 207970
- Name of registering court: Budapest District Court Company Registry
- Tax number: 2411272-2-13
- E-mail: info@setechflotta.hu

Data protection officer of the data controller:

- Name: **Ádám Gönci**
- Postal address: 2161 Csomád, Liget utca 40.
- Email: info@setechflotta.hu

Data processor's details and contact information (Hosting):

- Name: **DOCCA Ltd.**
- Represented by: Szilveszter Bálint Bekény
- Registered office: 1123 Budapest, Győri út 2/C 2nd floor, door 6
- Postal address: as above
- Registration number: 01 10 141530
- Name of the registering court: Budapest Metropolitan Court of Registration
- Tax number: 27428014-2-43
- E-mail: kontakt@docca.hu

Data processor details and contact information (Hosting):

- Name: **HUNET Kft.**
- Represented by: János Lőke, managing director
- Registered office: 1123 Budapest, Győri út 2/C 2nd floor, door 6
- Postal address: as above
- Registration number: 01 09 462043
- Name of the registering court: Budapest Metropolitan Court of Registration
- Tax number: 12060245-2-43
- E-mail: cegkapu@hunet.ugykezekelo.hu

Additional data processors:

Data processing related to accounting:

Name of data processor: G.G.L.L.I Service Kft.

Registered office: 1117 Budapest, Irinyi József utca 4-20.

Data processing related to hosting services and correspondence:

Microsoft Corporation (Redmond, Washington 98052, USA)

<https://privacy.microsoft.com/hu-HU/>

Data processor related to fleet tracking services:

Name of data processor: Mobile LBS Limited Liability Company

Registered office: 7625 Pécs, István utca 7. 1. em. 6.

Data processor related to the corporate CRM system:

Name of data processor: MiniCRM Zrt.

Registered office: 1075 Budapest, Madách Imre út 13-14

5. Principles of data processing

5.1. *Lawfulness, fairness and transparency:*

Personal data must be processed lawfully, fairly and transparently to the data subject.

5.2. *Purpose limitation:*

Personal data shall be collected for specific, explicit and legitimate purposes and shall not be processed in a manner that is incompatible with those purposes; in accordance with Article 89(1), further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered incompatible with the initial purposes.

5.3. *Data minimisation:*

Personal data must be adequate, relevant and limited to what is necessary for processing purposes.

5.4. *Accuracy:*

Personal data must be accurate and, where necessary, kept up to date; every reasonable effort shall be made every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

5.5. *Storage limitation:*

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes, subject to the implementation of appropriate technical and organisational measures provided for in this Regulation in order to safeguard the rights and freedoms of data subjects.

5.6. Integrity and confidentiality:

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

5.7. Accountability:

The Data Controller shall be responsible for compliance with the principles set out in points 5.1 to 5.6 and shall be able to demonstrate such compliance.

6. Scope of data processed, purpose, legal basis and duration of data processing

6.1. Data relating to the registration of the Company's employees

The Company processes employee data as specified in Act I of 2012 on the Labour Code (hereinafter: Mt.) and in the provisions of the relevant tax and social security legislation.

The legal basis for the processing of data provided during the establishment of the employment relationship is the consent of the data subject and the fulfilment of a legal obligation.

The scope of personal data processed:

- the employee's name,
- the employee's place and date of birth,
- the employee's address,
- the employee's telephone number,
- the employee's e-mail address
- additional data specified by tax and social security legislation.

Time of deletion of processed data:

- In the event of termination of employment, the Company, as the employer, is obliged to retain the employee's data for the period specified in the relevant legal provisions; after the retention period has expired, the employer shall delete the data.

6.2. Personal data that may be processed in the course of the Company's fleet tracking activities

The Company provides tracking (fleet tracking) services to its contractual partners (customers) for motor vehicles or other assets.

By default, the system does not process personal data, but in individual cases, the customer, as the user, may assign a natural person (e.g. a driver) to the given device, in which case the Company may process this personal data as a data processor on behalf of the customer, as the data controller, on the basis of the service contract .

The content and duration of data processing is determined exclusively by the customer, who may use the service at any time in the form made available by the service provider, and it is the customer's responsibility to inform the data subjects about such data processing.

In all other respects, the provisions of the service contract shall apply to the processing of data in the fleet tracking system. Following the termination of the service contract and the transfer of the data to the customer, the service provider shall delete the data after 5 years from the date of termination of the contract.

6.3. Data relating to the registration of the Company's officers

The managing director and representative of the Company is the current managing director of the Company, i.e. the chief executive officer of the Company.

Legal basis for data processing:

Voluntary consent and compliance with legal obligations

- The data of senior officers are processed in accordance with Section 3:22 and Section 3:26(2) of the Civil Code.

Scope of personal data processed:

- the name of the managing director,
- the managing director's place and date of birth,
- the name of the managing director's mother,
- the managing director's address,

Time of deletion of processed data:

The Company shall delete the data of former senior officers within five years of the termination of their appointment, in accordance with Sections 3:24 and 3:86(2) of the Civil Code.

6.4. Personal data of the representatives and contact persons of the Company's contractual partners

Purpose of data processing:

Personal data of the representatives and contact persons of the Company's contractual partners, provided by the contractual partner in connection with the performance of the contract

Legal basis for data processing:

Data processing for the performance of a contract to which the Company is a party, pursuant to Article 6(1)(b) of the GDPR

Scope of data processed:

- names of representatives and contact persons of contractual partners,
- the telephone numbers of the representatives and contact persons of the Company's contractual partners,
- e-mail addresses or any other electronic contact details of the representatives and contact persons of contractual partners.

The Company shall delete the data provided by the data subject after the provision of the service or the performance of the contract, but no later than 5 years after the termination of the contract.

6.5 Personal data of persons involved in tax return assistance activities

The Company performs its tax return assistance activities pursuant to the Udtv, Udvhr, and its agreement with the National Toll Payment Services Ltd. (hereinafter: NÚSZ) and on the basis of individual contracts concluded with customers.

In these legal relationships, the Company is considered a data processor commissioned by NÚSZ as the data controller, which is accepted by the customer in the legal relationship between the customer and NÚSZ. As a declaration intermediary, the Company does not process personal data, with the following exceptions, as the GPS coordinates and registration numbers of vehicles assigned to specific customers cannot be linked to natural persons or any of their data at the Company level.

The Company may only process personal data as a data controller in specific cases where any natural person concerned becomes identifiable to the Company during a customer service call, a report relating to this activity of the Company, or the investigation of a complaint, or if the customer is a private individual and also the user (driver) of the vehicle in question.

The Company shall retain the data for the duration of the service provision or contract performance, but for no longer than 5 years after the termination of the contract.

6.6. Processing of data of persons requesting information

The Company maintains a website and customer service for information purposes. If a visitor requests further information via the website or customer service, they must provide their name, email address, telephone number and, in the case of contact on behalf of a company, the name of the company in order to be contacted. The legal basis for data processing is the consent of the data subject pursuant to Article 6(1)(a) of the GDPR. The Company will process this data for 6 months from the date of receipt, unless another legal basis arises.

7. Data protection and data security measures

The Company shall select and operate the IT tools used for the processing of personal data in the course of providing its services in such a way that the data processed is

accessible to those authorised to do so (availability), its authenticity and verification are ensured (authenticity of data processing), its unchanged nature can be verified (data integrity), and it is protected against unauthorised access (data confidentiality).

The Company shall take technical, organisational and administrative measures to ensure the security of data processing, providing a level of protection appropriate to the risks associated with data processing.

The Company shall protect the data by appropriate measures, in particular against unauthorised access, alteration, transmission, disclosure, deletion or destruction, as well as against accidental destruction, damage or inaccessibility resulting from changes in the technology used.

In order to protect the data files processed electronically in various registers, the Company, as the data controller, and the data processor, within the scope of its activities, shall ensure, by means of appropriate technical solutions, that the data stored in the registers cannot be directly linked to and assigned to the data subject, unless permitted by law.

In order to ensure an adequate level of security for the personal data processed, the Company shall take technical and organisational measures commensurate with the risks posed by data processing, in particular those associated with the processing of special data of data subjects, and shall take into account all circumstances of data processing, in particular the state of the art, the costs of implementing the measures, the nature, scope and purposes of the processing, and the varying likelihood and severity of the risks to the rights of data subjects posed by the processing.

The measures shall ensure

- deny unauthorised persons access to the means used for data processing (hereinafter referred to as the data processing system)
- the prevention of unauthorised reading, copying, modification or removal of data carriers,
- the unauthorised entry of personal data into the data processing system and the unauthorised disclosure, modification or deletion of personal data stored therein,
- preventing unauthorised persons from using data processing systems via data transmission equipment,
- ensuring that persons authorised to use the data processing system have access only to the personal data specified in their access authorisation,
- to ensure that it is possible to verify and establish to which addressee personal data have been or may be transmitted or made available by means of data transmission equipment,
- ensuring that it is possible to subsequently verify and establish which personal data were entered into the data processing system, at what time and by whom,
- the prevention of unauthorised access, copying, modification or deletion of personal data during transmission or transport of the data medium,
- that the data processing system can be restored in the event of a malfunction, and
- that the data processing system is operational, that reports are made on errors occurring during its operation, and that stored personal data cannot be altered even if the system is operated incorrectly.

8. Rights of the data subject

The data subject shall have the right, with regard to personal data processed by the Data Controller and by the data processor acting on its behalf or on its instructions, to:

- to be informed about the facts related to data processing prior to the commencement of data processing (right to prior information),
- upon request, have their personal data and information related to the processing thereof made available to them by the Data Controller (right of access),
- upon request, have your personal data corrected or supplemented by the Data Controller in the cases specified in Act CXII of 2011 on the right to self-determination and freedom of information (right to correction),
- upon request, and in the cases specified in Act CXII of 2011 on the right to self-determination and freedom of information, the Data Controller shall restrict the processing of his/her personal data (right to restriction of processing),
- upon request, and in other cases specified in Act CXII of 2011 on the right to self-determination and freedom of information, the Data Controller shall erase his or her personal data (right to erasure).

The Data Controller shall ensure and fulfil the rights of data subjects and their requests to exercise these rights in accordance with the provisions of the law.

8.1. Right to prior information

Prior to data processing, the person concerned may obtain information from the Data Controller about facts related to data processing. At the request of the data subject, the Data Controller shall inform him or her whether his or her personal data is processed by the Data Controller itself or by a data processor acting on its behalf or on its instructions.

If personal data relating to the data subject

- is collected from the data subject, the information and data to be provided to the data subject at the time of obtaining the personal data are set out in Article 13(1)-(4) of the GDPR.
- is not obtained from the data subject, the information to be provided to the data subject by the Company is contained in Article 14 (1)-(5) of the GDPR.

The right to information may be exercised in writing via the contact details provided by the Company.

Upon request, the data subject may also be provided with information verbally, after verification of their identity.

8.2. Right of access of the data subject

The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries and international organisations;
- the envisaged period for which the personal data will be stored;

- the right to rectification, erasure or restriction of processing and the right to object;
- the right to lodge a complaint with a supervisory authority;
- information about the sources of the data;
- the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

In the case of the transfer of personal data to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer.

The Company shall provide the data subject with a copy of the personal data undergoing processing. The Company may charge a reasonable fee based on administrative costs for any further copies requested by the data subject. At the request of the data subject, the Company shall provide the information in electronic form.

8.3. Right to rectification

In the event of inaccuracy, incorrectness or incompleteness of the personal data processed by the Company, the data shall be corrected or rectified without delay, in particular at the request of the data subject, or, if compatible with the purpose of the data processing, supplement it with additional personal data provided by the data subject or with a statement by the data subject attached to the personal data processed (hereinafter collectively referred to as "rectification").

The Company shall be exempt from the obligation to rectify if

- it does not have accurate, correct or complete personal data at its disposal and the data subject does not make such data available to it, or
- the authenticity of the personal data provided by the data subject cannot be established beyond doubt.

8.4. Right to restriction of processing

In addition to storage, the Company shall perform other data processing operations solely for the purpose of enforcing the legitimate interests of the data subject or as specified by law, international treaty or binding legal act of the European Union, if

- the data subject disputes the accuracy, relevance or completeness of the personal data processed by the Company, and the accuracy, relevance or completeness of the personal data processed cannot be established beyond doubt, for the duration of the clarification of the existing doubt,
- the data should be erased due to the unlawfulness of the data processing, but based on the data subject's written statement or the information available to the data controller, it can be reasonably assumed that the erasure of the data would violate the legitimate interests of the data subject, for the period during which the legitimate interest justifying the non-erasure exists,
- the data should be deleted due to unlawful data processing, but it is necessary to retain the data as evidence in the course of investigations or proceedings specified by law, in particular criminal proceedings, conducted by or with the participation of the data controller or another body performing a public task, until the final and legally binding conclusion of such investigation or proceedings,

- the data should be deleted due to the unlawfulness of the data processing, but the data must be retained for the purpose of complying with the documentation obligation set out in Section 12(2) until the date specified in Section 25/F(4).

If data processing is subject to restrictions, personal data may only be processed, with the exception of storage, with the consent of the data subject, or for the purpose of submitting, enforcing or defending legal claims, or for the protection of the rights of another natural or legal person, or for reasons of important public interest of the Union or of a Member State.

In the event of the lifting of the restriction on data processing, the Company shall inform the data subject in advance of the lifting of the restriction on data processing.

8.5. Right to erasure ('right to be forgotten')

The Company shall, without undue delay, erase the data subject's data, except in cases specified in European Union legislation or law, if

- the data processing is unlawful, in particular if the data processing
 - contrary to the established principles,
 - the purpose of the processing has ceased to exist, or further processing of the data is no longer necessary for the fulfilment of the purpose of the processing,
 - the period specified in a law, international treaty or binding legal act of the European Union has expired, or
 - the legal basis has ceased to exist and there is no other legal basis for the processing of the data,
- the data subject withdraws his or her consent to the processing of the data or requests the erasure of his or her personal data, unless the processing of the data is based on Section 5(1)(a) or (c) or Section 5(2)(b) of the Info Act,
- the deletion of the data has been ordered by law, a legal act of the European Union, the Authority or a court, or
- the period specified in Section 19 (1) b)-d) of the Info Act has elapsed.

The Data Controller shall assess any request submitted by the data subject to exercise his or her rights as soon as possible, but within a maximum of 25 days, and shall notify the data subject in writing, or electronically if the request was submitted electronically.

The Data Controller shall perform its tasks related to the enforcement of the rights of the data subject free of charge, except for the exceptions specified in the GDPR and in the law.

9. Legal remedies

The data subject shall have the right to lodge a complaint with a supervisory authority if

- the Data Controller restricts the exercise of the rights of the data subject or rejects a request for the exercise of those rights, the data subject may initiate an investigation by the National Authority for Data Protection and Freedom of Information (NAIH, 1055 Budapest, Falk Miksa utca 9-11., ugyfelszolgalat@naih.hu) in order to examine the lawfulness of the Data Controller's action,
- If, in your opinion, the Data Controller violates the provisions of the law or binding legal acts of the European Union on the processing of personal data in the course of processing your personal data, you may request the NAIH to conduct a data protection authority procedure or you may turn to the court.

In the latter case, the data subject may decide whether to file a lawsuit with the court of their place of residence or place of stay.