Privacy Policy – IPMFlow.com

Last updated: 2025.11.23.

Trapshop Kft.

1. Introduction

Trapshop Kft. (Registered seat: 8797 Batyk, Fő utca 34, Tax number: 32050547-2-20, Company registration number: 2009078346) (hereinafter: **Service Provider**, **Controller**) submits itself to the following policy:

We provide the following information in accordance with REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 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** or **GDPR**).

This Privacy Policy governs data processing on the following websites/mobile applications: https://ipmflow.com/

The Privacy Policy is available at: Ipmflow.com/adatvedelem, Ipmflow.com/privacy

Amendments to the policy shall enter into force upon publication at the above address.

2. The Controller and Contact Details

- **Name:** Trapshop Kft.
- **Registered seat:** 8797 Batyk, Fő utca 34
- **E-mail:** hello@ipmflow.com
- **Phone:** +36 30 220 9884

3. Definitions

- **“Personal data”:** means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who 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;
- **“Processing”:** means 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;
- **“Controller”:** means the natural or legal person, public authority, agency or 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 such 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;
- **“Processor”:** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- **“Recipient”:** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;
- **“Consent of the data subject”:** means 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;
- **“Personal data breach”:** means 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.
- **“Profiling”:** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

4. Principles Relating to Processing of Personal Data

Personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject (**"lawfulness, fairness and transparency"**);
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (**"purpose limitation"**);
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**"data minimisation"**);
- accurate and, where necessary, kept up to date; 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 (**"accuracy"**);
- 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, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (**"storage limitation"**);
- 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 (**"integrity and confidentiality"**).

The Controller shall be responsible for, and be able to demonstrate compliance with, the above (**"accountability"**). The Controller declares that its data processing is carried out in accordance with the principles set out in this section.

5. Data Processing Related to Sales/Use f Service

1. The fact of data collection, the scope of processed data, and the purpose of processing:

Personal Data	Purpose of Processing	Legal Basis
Vezeték-és keresztnév (Surname and First name)	Necessary for contact, purchasing, and issuing a compliant invoice.	GDPR Art. 6(1)(b)
E-mail address	Keeping contact. Sending messages and invoices.	GDPR Art. 6(1)(b)
Phone number	Keeping contact, efficient coordination of billing questions.	GDPR Art. 6(1)(b)
Billing name and address	Issuing a compliant invoice, creating the contract, defining its content, modification, monitoring performance, billing fees arising from it, and enforcing related claims.	GDPR Art. 6(1)(c): Legal obligation: Section 169 (2) of Act C of 2000 on Accounting.
Date of order/purchase	Execution of technical operation.	GDPR Art. 6(1)(b)
IP address of order/purchase	Execution of technical operation.	GDPR Art. 6(1)(b)

2. Scope of Data Subjects

All data subjects purchasing on the website.

3. Duration of processing, deadline for deletion

Processing lasts until the data subject's request for deletion, provided one of the nditions in Article 17(1) of the GDPR applies. The Controller shall inform the data subject ctronically of the deletion of any personal data provided by them pursuant to Article 19

of the GDPR. If the data subject's deletion request extends to the email address provided, the Controller shall also delete the email address following the notification. **Exception:** Accounting documents must be retained for 8 years pursuant to Section 169 (2) of Act C of 2000 on Accounting. Contractual data of the data subject may be deleted after the expiration of the civil limitation period upon the data subject's deletion request.

Accounting documents supporting the accounting records directly and indirectly (including general ledger accounts, analytical and detailed records) must be kept in legible form for at least 8 years, retrievable via accounting references.

4. Identity of potential data controllers entitled to access the data, recipients of personal data

The personal data may be processed by the sales and marketing staff of the Controller, respecting the above principles.

5. Description of data subjects' rights regarding processing

- The data subject may request from the Controller access to, rectification, erasure or restriction of processing of personal data concerning them, and
- the data subject has the right to data portability and the right to withdraw consent at any time.

6. Initiation of rights

The data subject may initiate access to, deletion, modification, restriction of processing, or portability of personal data in the following ways:

- by post at: 8797 Batyk, Fő utca 34,
- by e-mail at: hello@ipmflow.com,
- by phone at: +36 30 220 9884.

7. Legal basis for processing

1. GDPR Article 6(1) points (b) and (c).

2. Section 13/A (3) of Act CVIII of 2001 on certain issues of electronic commerce services and information society services (Elker Act):
   The service provider may process personal data that are technically strictly necessary for providing the service…
3. In case of issuing an invoice compliant with accounting laws: Article 6(1)(c).
4. In case of enforcement of claims arising from the contract: 5 years according to Section 6:21 of Act V of 2013 on the Civil Code.

8. We inform you that:

- The processing is necessary for the performance of a contract.
- You are obliged to provide personal data so that we can fulfill your order.
- Failure to provide data will result in our inability to process your order.

6. Provision of Service (Use of IPMFlow Tools)

Purpose of Processing: Ensuring the operation of IPMFlow intelligent pest control tools (e.g., Risk Assessment Module), processing data entered by the User, generating analyses and reports, including the provision of AI (Google Gemini) based functions.

Scope of Processed Data: Data provided by the User within the framework of the Service, specifically (but not limited to):

- **Facility Data:** Name of facility, description, environmental risk factors (water, green area, neighbors, waste), seasonal factors, general notes, and measures.
- **Location Data:** Location name, description, risk category, service intervals, list of potential pests, indicator system description, quantity of traps, structural/hygiene/entry point risks, location-specific notes, and measures.
- **Assessment Data:** Assessment date, identified pest, type and description of hazard, probability and severity values, calculated risk level, proposed/implemented measures, assessment notes.

Legal Basis: GDPR Art. 6(1)(b) (performance of a contract regarding the provision of the Service). By registering and using the service, the User accepts that the Controller processes the entered data for the purpose of operating the service.

7. AI (Google Gemini) Based Data Processing

- Certain functions of the Service (e.g., report generation) operate using artificial intelligence (Google Gemini, via the OpenRouter API).
- Data entered by the User into the relevant modules is transmitted to the Google Gemini service for processing (e.g., generating report text).
- The Controller ensures the secure storage and handling of API keys and other credentials through appropriate technical measures.
- AI-generated results (e.g., reports) are stored in the Service's system linked to the User's account.
- **The Controller declares that it does not use the data entered by the User to train its own AI models without the express, prior consent of the User.** The data is transmitted solely to the Google Gemini API for the purpose of executing the requested operation (e.g., report generation). The processing of data received by Google via the API, including its potential use for developing Google's own services or training its models, is subject to Google's currently effective privacy policies and terms of service.
- **Important:** It is the User's responsibility to ensure that data entered into the Service does not contain unnecessary or unlawfully processed personal data.

8. Contact

1. The fact of data collection, the scope of processed data, and the purpose of processing:

Personal Data	Purpose of Processing	Legal Basis
Name	Identification	GDPR Art. 6(1) (a)
E-mail address	Contact, sending replies	–
Phone number	Contact	–

Personal Data	Purpose of Processing	Legal Basis
Content of message	Necessary for replying (if it contains personal data)	–

It is not necessary for the email address to contain personal data.

2. Scope of Data Subjects: All data subjects sending a message via the contact form.

3. Duration of processing: Maximum 2 years, or until withdrawal/deletion request.

4. Legal basis: Consent of the data subject, GDPR Art. 6(1)(a). By contacting us, you consent to the processing of your personal data.

9. Cookie Handling

1. No prior consent required: For “password-protected session cookies”, “shopping cart cookies”, “security cookies”, “Essential cookies”, “Functional cookies”, and “website statistics cookies”.

2. Data processed: Unique identification number, dates, times.

3. Purpose: User identification, visitor tracking, ensuring customized operation.

4. Duration:

Cookie Type	Legal Basis	Duration
Session cookies / Essential	–	Until the browser is closed (session end).
Statistical, marketing cookies	GDPR Art. 6(1)(a)	1 day – 2 years, or until consent withdrawal.

5. Browser Settings: You can manage cookies in your browser settings:

- Google Chrome
- Internet Explorer
- Firefox

- Safari

10. Use of Google Ads Conversion Tracking

The Controller uses “Google Ads” and its conversion tracking. When a User reaches the website via a Google ad, a cookie is placed. These contain no personal data. Google uses this to create conversion statistics.

Google Consent Mode v2: Google uses `ad_user_data` and `ad_personalization` cookies based on consent. The Controller ensures appropriate consent acquisition via a cookie banner.

More info: https://policies.google.com/privacy

11. Use of Google Analytics

This website uses Google Analytics. It uses cookies to analyze website usage. IP anonymization is active. You can prevent cookie storage via browser settings or by downloading the browser plugin: https://tools.google.com/dlpage/gaoptout?hl=en

12. Newsletter, Direct Marketing (DM) Based on Consent

Service Provider does not send unsolicited advertising messages. The User may unsubscribe free of charge at any time.

Data collection details:

Personal Data	Name, e-mail address.
Purpose	Identification, subscription, sending ads/news.
Legal Basis	Consent (GDPR Art. 6(1)(a)).

Unsubscribing: Users can unsubscribe free of charge at any time by clicking the link in the message.

13. Complaint Handling

Personal Data	Name, Email, Phone, Billing Address.
Purpose	Handling quality objections/complaints.
Legal Basis	GDPR Art. 6(1)(c) and Consumer Protection Act.
Duration	3 years (for the minutes of the objection).

14. Recipients / Data Transfer (Online Payment)

1. **Activity:** Online payment.
2. **Recipient:** Stripe (Stripe Payments Europe, Ltd.). Privacy Policy
3. **Data processed:** Billing details, name, e-mail address.
4. **Purpose:** Conducting payment and fraud-monitoring.
5. **Legal Basis:** GDPR Art. 6(1)(b).

15. Data Processors Used

Hosting Provider

- **Name:** Rackhost Zrt. (6722 Szeged, Tisza Lajos körút 41.). Privacy Policy
- **Purpose:** Making the website/app available.
- **Legal Basis:** Legitimate interest (proper operation, security).

Other Data Processors

- **Stripe Payments Europe, Ltd.:** Online payments.
- **Bithuszárok Bt. (Listamester):** Newsletter sending.
- **Kutyavilág Kft. and Animadó Kft.:** Accounting.

- **Google Ireland Limited:** Google Charts/Analytics.
- **Google (Gemini via OpenRouter):** AI text generation.
- **KBOSS.hu Kft. (Számlázz.hu):** Invoicing service.

IT Security and Third-Party Service Providers

To maintain the security of the Website, ensure continuous service availability, and prevent malicious attacks (e.g., DDoS, hacking attempts, data theft), the Data Controller (Service Provider) engages specialized third-party partners.

Due to technical necessity, these services may record visitors' IP addresses, browsing data (User-Agent), and request metadata. These services may place strictly necessary security cookies on the user's device, which are not used for marketing purposes.

Legal basis for processing: The Legitimate Interest of the Data Controller (GDPR Art. 6(1)(f)), which concerns the protection of system integrity, confidentiality, and availability, as well as business continuity.

Data retention: Security log files are automatically deleted by the providers after the threat has been mitigated or following a specific technical retention period (typically 30 days).

Security Data Processors engaged:

Provider Name	**Cloudflare, Inc.**
Headquarters	101 Townsend St, San Francisco, CA 94107, USA
Activity	Content Delivery Network (CDN), Web Application Firewall (WAF), DDoS protection.
Processed Data	IP address, system configuration info, traffic data, necessary cookies.
Data Transfer	The company participates in the EU-US Data Privacy Framework (DPF), ensuring an adequate level of data protection.

rovider Name	**Defiant, Inc. (Wordfence)**

Headquarters	800 5th Ave Ste 4100, Seattle, WA 98104, USA
Activity	Endpoint website protection, intrusion detection system, malware filtering.
Processed Data	IP address, login attempt data, blocked request logs, necessary cookies.
Data Transfer	Data transfer is based on Standard Contractual Clauses (SCCs) approved by the European Commission.

16. Social Media

Data processing regarding posts, likes, and follows happens on the respective social media platforms (Twitter, Facebook, LinkedIn, etc.). Their privacy policies apply.

17. Facebook / Meta Joint Controllership

Statistical data processing on the Facebook page is considered Joint Processing between the Controller and Facebook Ireland Ltd.

Communication: We only communicate via private message if you contact us first.

Rights: You can withdraw consent (unlike/delete post) at any time.

18. Customer Relations and Other Processing

Data provided during inquiries (phone/email) is deleted after a maximum of **2 years**. We only transfer data to authorities based on strict legal obligations.

19. Rights of Data Subjects

- **Right of access:** You can ask if we are processing your data.
- **Right to rectification:** You can ask us to correct wrong data.
- **Right to erasure:** You can ask us to delete data (Right to be forgotten).

- **Right to restriction:** You can ask us to pause processing.
- **Right to data portability:** You can ask for your data in a machine-readable format.
- **Right to object:** You can object to processing based on legitimate interest or direct marketing.
- **Automated decision-making:** You have the right not to be subject to automated decisions with legal effects.

20. Deadline for Action

We will respond within **1 month**. This can be extended by 2 months if necessary.

21. Security of Processing

We implement technical and organizational measures (encryption, physical locks, password protection, backups) to protect your data.

22 & 23. Data Breaches

We will notify the Authority within 72 hours of a breach. We will notify You if there is a high risk to your rights.

24. Review

We review the necessity of mandatory data processing every 3 years.

25. Right to Lodge a Complaint

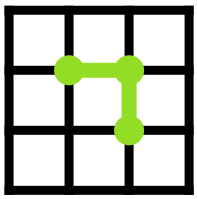
Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH)
Address: 1055 Budapest, Falk Miksa utca 9-11.
Mailing address: 1363 Budapest, Pf. 9.
E-mail: ugyfelszolgalat@naih.hu

26. Closing

.s policy is based on GDPR, Infotv., and other relevant Hungarian and EU legislation.

Previous versions

- Privacy Policy – IPMFlow.com – 2025.06.12.
- Privacy Policy – IPMFlow.com – 2025.06.16.
- Privacy Policy – IPMFlow.com – 2025.11.19.



IPMFlow.com

Email: hello@ipmflow.com

Company: Trapshop Kft.

Address: H-8797 Batyk, Fő utca 34.

Informations

Home
RAP
Help Center
Contact
Cookie Policy
Privacy Policy
Terms and conditions

Account

User Account
Log out

Payment Methods

stripe