Privacy Policy – IPMFlow.com - IPMflow

Last updated: 2026.02.24.

Trapshop Kft. Privacy Policy

Download

1. Introduction

Trapshop Kft. (registered seat: 8797 Batyk, Fő utca 34, Hungary; tax number: 32050547-2-20; company registration number: 2009078346) (hereinafter referred to as: Service Provider, Controller) submits itself to the following policy:

Pursuant to 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), we provide the following information.

This privacy policy governs the data processing of the following websites/mobile applications: https://ipmflow.com/

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

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

2. The Controller and its contact details

Name: Trapshop Kft.

Registered seat: 8797 Batyk, Fő utca 34, Hungary

E-mail: hello@ipmflow.com

Phone: +36 30 220 9884

3. Definitions

- personal data: 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: 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: 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: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- recipient: 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: 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: 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: 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 of services

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

- Personal data: First name and last name. Purpose of processing: Necessary for contact, purchase, and issuing a compliant invoice. Legal basis: Article 6(1)(b) of the GDPR.
- Personal data: E-mail address. Purpose of processing: Contact. Sending messages, invoices. Legal basis: Article 6(1)(b) of the GDPR.
- Personal data: Phone number. Purpose of processing: Contact, more efficient reconciliation of questions related to billing. Legal basis: Article 6(1)(b) of the GDPR.
- Personal data: Billing name and address. Purpose of processing: Issuing a compliant invoice, as well as the conclusion of the contract, determination and modification of its content, monitoring its performance, invoicing the fees arising from it, and enforcing claims related to it. Legal basis: Article 6(1)(c) of the GDPR: Legal obligation based on Section 169 (2) of Act C of 2000 on Accounting.
- Personal data: Date and time of order / purchase. Purpose of processing: Execution of technical operation. Legal basis: Article 6(1)(b) of the GDPR.
- Personal data: IP address of order / purchase. Purpose of processing: Execution of technical operation. Legal basis: Article 6(1)(b) of the GDPR.

2. Scope of data subjects: All data subjects purchasing on the website.

3. Duration of data processing, deadline for deleting data: If any of the conditions set out in Article 17(1) of the GDPR is met, it lasts until the data subject's request for erasure. The controller shall inform the data subject electronically of the erasure of any personal data provided by the data subject pursuant to Article 19 of the GDPR. If the data subject's request for erasure also covers the e-mail address provided by them, the controller shall also erase the e-mail address following the notification. Except in the case of accounting records, as pursuant to Section 169 (2) of Act C of 2000 on Accounting, these data must be retained for 8 years. The contractual data of the data subject may be deleted upon the data subject's request for erasure after the expiry of the civil law limitation period.

The accounting document directly and indirectly supporting the accounting records (including ledger accounts, analytical and detailed records) must be kept in legible form for at least 8 years, retrievable by reference to the accounting records.

4. Identity of potential controllers entitled to access the data, recipients of personal data: Personal data may be processed by the sales and marketing staff of the controller, respecting the above principles.

5. Description of data subjects' rights related to data processing:

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

6. The data subject may initiate access to, deletion, modification, or restriction of the processing of

personal data, and data portability in the following ways:

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

7. Legal basis for data processing:

- Article 6(1)(b) and (c) of the GDPR.
- Section 13/A (3) of Act CVIII of 2001 on certain issues of electronic commerce services and information society services (hereinafter: Elker tv.): The service provider may process personal data that are strictly technically necessary for the provision of the service. The service provider must, all other conditions being equal, select and in any case operate the means applied in the provision of the information society service in such a way that the processing of personal data occurs only if strictly necessary for the provision of the service and for the fulfillment of the other purposes specified in this Act, but even in this case, only to the necessary extent and duration.
- In the case of issuing an invoice in compliance with accounting legislation, Article 6(1)(c) of the GDPR.
- In the case of enforcing claims arising from the contract, 5 years in accordance with Section 6:21 of Act V of 2013 on the Civil Code.

Section 6:22 [Limitation of claims]

- (1) Unless otherwise provided in this Act, claims shall lapse in five years.
- (2) The limitation period shall commence when the claim becomes due.
- (3) An agreement to change the limitation period must be in writing.
- (4) An agreement excluding the limitation of claims is null and void.

8. We inform you that:

- The data processing is necessary for the performance of a contract.
- You are obliged to provide the personal data so that we can process your order.
- Failure to provide the data has the consequence that we cannot process your order.

6. Provision of the Service (Use of IPMFlow Tools)

Purpose of data processing: To ensure the operation of IPMFlow intelligent pest control tools (e.g., Risk Assessment module), process data entered by the User, and generate 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, in particular (but not exclusively):

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

Legal basis for data processing: Article 6(1)(b) of the GDPR (performance of a contract for the provision of the Service). By registering and using the service, the User accepts that the entered data will be processed by the Service Provider for the purpose of operating the service.

7. AI (Google Gemini) based data processing

Certain features of the Service (e.g., report generation) operate using artificial intelligence (Google Gemini, via the OpenRouter API).

The data entered by the User into the relevant modules (see above under “Scope of processed data”) are transmitted to the Google Gemini service for processing (e.g., generating report text).

The Controller ensures the secure storage and management of API keys and other credentials through appropriate technical measures.

The results generated by the AI (e.g., reports) are stored in the Service’s system in connection with 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 User’s explicit, prior consent. The data is exclusively transmitted 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 governed by Google’s prevailing privacy policies and terms of service, which the User can review on Google’s platforms.

Important: It is the User’s responsibility to ensure that the data entered into the Service does not contain unnecessary or unlawfully processed personal data (e.g., names of third-party employees if there is no appropriate legal basis for processing them).

8. Contacting us

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

- Personal data: Name. Purpose of processing: Identification. Legal basis: Article 6(1)(a) of the GDPR.
- Personal data: E-mail address. Purpose of processing: Contact, sending response messages. Legal basis: Article 6(1)(a) of the GDPR.
- Personal data: Phone number. Purpose of processing: Contact. Legal basis: Article 6(1)(a) of the GDPR.
- Personal data: Content of the message, if it contains personal data. Purpose of processing: Necessary to provide a reply. Legal basis: Article 6(1)(a) of the GDPR.

In the case of the e-mail address, it does not need to contain personal data.

2. Scope of data subjects: All data subjects sending a message through the contact form.

3. Duration of data processing, deadline for deleting data: The controller processes the personal data until the purpose of the processing is fulfilled, but for a maximum of 2 years. If any of the conditions set out in Article 17(1) of the GDPR is met, the processing lasts until the data subject’s request for erasure.

4. Description of data subjects’ rights related to data processing:

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

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

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

6. Legal basis for data processing: consent of the data subject, Article 6(1)(a). If you contact us, you consent to the processing of your personal data (name, phone number, e-mail address) obtained by us during the contact, in accordance with this policy.

7. We inform you that:

- This data processing is based on your consent and is necessary to provide an offer.
- You are obliged to provide the personal data so that you can contact us.
- Failure to provide the data has the consequence that you cannot contact the controller.
- The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

9. Cookie management

1. The use of so-called “password-protected session cookies”, “shopping cart cookies”, “security cookies”, “Necessary cookies”, “Functional cookies”, and “cookies responsible for managing website statistics” does not require prior consent from data subjects.

2. The fact of data processing, the scope of processed data: Unique identification number, dates, times.

3. Scope of data subjects: All data subjects visiting the website.

4. Purpose of data processing: Identifying users, tracking visitors, ensuring customized operation.

5. Duration of data processing, deadline for deleting data:

- Cookie type: Session cookies or other cookies essential for the operation of the website. Legal basis for data processing: No data processing occurs by using the cookie. Duration: The period lasting until the end of the relevant visitor session; thus, it remains on the computer only until the browser is closed.
- Cookie type: Statistical, marketing cookies. Legal basis for data processing: Article 6(1)(a) of the GDPR. Duration: 1 day to 2 years, according to the cookie policy, or until the data subject’s consent is withdrawn.

6. Description of data subjects’ rights related to data processing: Data subjects have the option to delete cookies in the Tools/Settings menu of browsers, generally under the Privacy menu item settings.

7. Most browsers used by our users allow setting which cookies should be saved and allow for (specific) cookies to be deleted again. If you restrict the saving of cookies on certain websites or do

not allow third-party cookies, this may, under certain circumstances, lead to our website no longer being fully usable. Here you can find information on how to customize cookie settings for standard browsers:

- Google Chrome (https://support.google.com/chrome/answer/95647)
- Microsoft Edge (https://support.microsoft.com/...)
- Firefox (https://support.mozilla.org/en-US/kb/enable-and-disable-cookies-website-preferences)
- Safari (https://support.apple.com/guide/safari/sfri11471/mac)

10. Use of Google Ads conversion tracking

The controller uses the online advertising program called “Google Ads”, and within its framework, utilizes Google’s conversion tracking service. Google conversion tracking is an analytics service of Google Inc. (1600 Amphitheatre Parkway, Mountain View, CA 94043, USA; “Google”).

When a User accesses a website via a Google ad, a cookie necessary for conversion tracking is placed on their computer. The validity of these cookies is limited, and they do not contain any personal data, so the User cannot be identified by them.

When the User browses certain pages of the website and the cookie has not yet expired, both Google and the controller can see that the User clicked on the ad.

Every Google Ads customer receives a different cookie, so they cannot be tracked across the websites of Ads customers.

The information obtained using conversion tracking cookies serves the purpose of creating conversion statistics for Ads customers who have opted for conversion tracking. This is how customers find out the number of users who clicked on their ad and were redirected to a page tagged with a conversion tracking tag. However, they do not obtain information that could be used to identify any user.

If you do not wish to participate in conversion tracking, you can reject this by disabling the option to install cookies in your browser. You will then not be included in the conversion tracking statistics.

Based on Google Consent Mode v2, Google also uses two new types of cookies: ad_user_data and ad_personalization, which are based on the data subject’s consent and relate to the use and sharing of data. ad_user_data is used to grant consent for user data to be sent to Google for advertising purposes. ad_personalization controls whether data can be used for personalized advertising (e.g., remarketing). The Controller ensures the collection and withdrawal of appropriate consents on its cookie banner/panel. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

Further information and Google’s privacy policy are available at the following page: https://policies.google.com/privacy

11. Use of Google Analytics

This website uses Google Analytics, a web analytics service provided by Google Inc. (“Google”). Google Analytics uses so-called “cookies”, text files placed on your computer, to help analyze how the User uses the visited website.

The information generated by the cookies about the User's use of the website is generally transmitted to and stored on a Google server in the USA. By activating IP anonymization on the website, Google will beforehand truncate the User's IP address within Member States of the European Union or in other state parties to the Agreement on the European Economic Area.

Only in exceptional cases will the full IP address be transmitted to a Google server in the USA and truncated there. On behalf of the operator of this website, Google will use this information to evaluate how the User used the website, to compile reports on website activity for the website operator, and to provide other services relating to website activity and internet usage.

The IP address transmitted by the User's browser within the framework of Google Analytics is not merged with other Google data. The User may refuse the storage of cookies by selecting the appropriate settings on their browser; however, please note that if you do this, you may not be able to use the full functionality of this website. Furthermore, you can prevent Google's collection and processing of data generated by the cookie and related to the User's use of the website (including the IP address) by downloading and installing the browser plug-in available at the following link: https://tools.google.com/dlpage/gaoptout

12. Newsletter, Direct Marketing activity based on consent

1. Pursuant to Section 6 of Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities, the User may expressly consent in advance to the Service Provider contacting them with its advertising offers and other mailings at the contact details provided upon registration.

2. Furthermore, keeping in mind the provisions of this policy, the Client may consent to the Service Provider processing their personal data necessary for sending advertising offers.

3. The Service Provider does not send unsolicited advertising messages, and the User may unsubscribe from receiving offers free of charge, without restriction or justification. In this case, the Service Provider will delete all their personal data necessary for sending advertising messages from its records and will not contact the User with further advertising offers. The User can unsubscribe from advertisements by clicking the link in the message.

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

- Personal data: Name, e-mail address. Purpose of processing: Identification, enabling subscription to the newsletter / promotional coupons. Legal basis: Consent of the data subject, Article 6(1)(a) of the GDPR.
- Personal data: Date and time of subscription. Purpose of processing: Execution of technical operation. Legal basis: Consent of the data subject, Article 6(1)(a) of the GDPR.
- Personal data: IP address at the time of subscription. Purpose of processing: Execution of technical operation. Legal basis: Consent of the data subject, Article 6(1)(a) of the GDPR.

5. The sending of newsletters is carried out in compliance with the provisions of Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities.

6. Scope of data subjects: All data subjects subscribing to the newsletter.

7. Purpose of data processing: Sending electronic messages containing advertising (e-mail, sms, push message) to the data subject, providing information on current information, products, promotions, new functions, etc.

8. Duration of data processing, deadline for deleting data: The data processing lasts until the withdrawal of consent (unsubscribing, the data subject's request for erasure) or until the termination of the newsletter.

9. Description of data subjects' rights related to data processing:

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

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

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

11. The data subject may unsubscribe from the newsletter at any time, free of charge.

12. We inform you that:

- The data processing is based on your consent.
- You are obliged to provide the personal data if you wish to receive a newsletter from us.
- Failure to provide the data has the consequence that we cannot send you a newsletter.
- We inform you that you can withdraw your consent at any time by clicking on unsubscribe.
- The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

13. Complaint handling

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

- Personal data: First name and last name. Purpose of processing: Identification, contact. Legal basis: Compliance with a legal obligation, Article 6(1)(c) of the GDPR. (The relevant legal obligation is Section 17/A (7) of Act CLV of 1997 on Consumer Protection).
- Personal data: E-mail address. Purpose of processing: Contact. Legal basis: Compliance with a legal obligation, Article 6(1)(c) of the GDPR.
- Personal data: Phone number. Purpose of processing: Contact. Legal basis: Compliance with a legal obligation, Article 6(1)(c) of the GDPR.
- Personal data: Billing name and address. Purpose of processing: Identification, handling quality complaints, questions, and problems arising in connection with the ordered products/ services. Legal basis: Compliance with a legal obligation, Article 6(1)(c) of the GDPR.

2. Scope of data subjects: All data subjects purchasing on the website and filing a quality complaint or grievance.

3. Duration of data processing, deadline for deleting data: Copies of the report taken on the complaint, the transcript, and the reply given thereto must be kept for 3 years pursuant to Section 17/A (7) of Act CLV of 1997 on Consumer Protection.

4. Description of data subjects' rights related to data processing:

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

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

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

6. We inform you that:

- The provision of personal data is based on a legal obligation.
- The processing of personal data is a prerequisite for concluding the contract.
- You are obliged to provide the personal data so that we can handle your complaint.
- Failure to provide the data has the consequence that we cannot process your received complaint.

14. RECIPIENTS TO WHOM PERSONAL DATA ARE DISCLOSED (DATA TRANSFER)

Online payment

1. Activity performed by the Recipient: Online payment

2. Name and contact details of the Recipient: Stripe (Stripe Payments Europe, Ltd. Secure processing of online payment transactions. https://stripe.com/privacy)

3. The fact of data processing, the scope of processed data: Billing data, name, e-mail address

4. Scope of data subjects: All data subjects choosing payment on the website.

5. Purpose of data processing: Execution of online payment, confirmation of transactions, and fraud-monitoring performed to protect users.

6. Duration of data processing, deadline for deleting data: It lasts until the execution of the online payment.

7. Legal basis for data processing: Article 6(1)(b) of the GDPR. Processing is necessary for the performance of the online payment at the request of the data subject.

8. Rights of the data subject:

- a. You can be informed about the circumstances of the data processing.
- b. You have the right to obtain confirmation from the controller as to whether or not personal data concerning you are being processed, and to access all information related to the processing.
- c. You have the right to receive the personal data concerning you in a structured, commonly used and machine-readable format.
- d. You have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning you upon request.

15. Processors used

Hosting provider

1. Activity performed by the Processor: Hosting service

2. Name and contact details of the Processor: Rackhost Zrt. (6722 Szeged, Tisza Lajos körút 41., Hungary; e-mail: info@rackhost.hu, phone: +36 1 445 1200) https://www.rackhost.hu/privacy-policy

3. The fact of data processing, the scope of processed data: All personal data provided by the data subject.

4. Scope of data subjects: All data subjects using the website/mobile application.

5. Purpose of data processing: Making the website/mobile application available and ensuring its proper operation.

6. Duration of data processing, deadline for deleting data: The processing lasts until the termination of the agreement between the controller and the hosting provider, or until the data subject's request for erasure addressed to the hosting provider.

7. Legal basis for data processing: Article 6(1)(c) and (f) of the GDPR, and Section 13/A (3) of Act CVIII of 2001 on certain issues of electronic commerce services and information society services. The legitimate interest is the proper operation of the website, protection against attacks and fraud.

Other processors (if any)

1. General administration, invoicing and communication

- Processor name: KBOSS.hu Kft. (Számlázz.hu). Headquarters / Contact: 1031 Budapest, Záhony utca 7., Hungary. Company reg. no.: 01-09-303201. Tax number: 13421739-2-41. Represented by: Balázs Ángyán. E-mail: info@szamlazz.hu. DPO: Dr. Éva Istvánovics (dpo@kboss.hu). Description of activity: Invoicing service, issuing and storing electronic invoices. Privacy policy: https://www.szamlazz.hu/adatvedelem/
- Processor name: Billingo Technologies Zrt. Headquarters / Contact: 1133 Budapest, Árbóc utca 6. III. emelet, Hungary. E-mail: hello@billingo.hu. Description of activity: Invoicing service, issuing and storing electronic invoices. Privacy policy: https://www.billingo.hu/adatkezelesi-tajekoztato
- Processor name: Kutyavilág Kft. and Animadó Kft. Headquarters / Contact: Based on a contract concluded with the Controller. Description of activity: Bookkeeping. Fulfillment of the Controller's accounting and taxation obligations. Privacy policy: Regulated by contract.
- Processor name: Bithuszárok Bt. (Listamester). Headquarters / Contact: 2053 Herceghalom, Liget utca 3., Hungary. E-mail: info@listamester.hu. Description of activity: Sending newsletters to subscribers, e-mail marketing. Privacy policy: https://listamester.hu/adatkezelesi-tajekoztato.php
- Processor name: Resend Labs Inc. Headquarters / Contact: 2261 Market Street #4816, San Francisco, CA 94114, USA. Description of activity: Technical transmission of transactional e-mails (e.g., order confirmation) (SMTP provider). Privacy policy: https://resend.com/legal/privacy-policy

2. Online payment providers

- Processor name: Barion Payment Zrt. Headquarters / Contact: 1117 Budapest, Infopark sétány

1. I. ép. 5. em. 5., Hungary. License number: H-EN-I-1064/2013. Description of activity: Processing online credit card payments, fraud prevention. Privacy policy: https://www.barion.com/hu/adatvedelmi-tajekoztato/
- Processor name: Stripe Payments Europe, Ltd. Headquarters / Contact: 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, Ireland. Description of activity: Secure processing of online payment transactions. Privacy policy: https://stripe.com/privacy

3. Analytics, marketing and Artificial Intelligence (AI)

- Processor name: Google Ireland Limited. Headquarters / Contact: Gordon House, Barrow Street, Dublin 4, Ireland. Description of activity: Google Analytics 4: Visitor statistics, web analytics. Google Ads: Ad serving, conversion tracking, remarketing. Google Workspace: Business email, document storage. Privacy policy: https://policies.google.com/privacy
- Processor name: Google LLC (Gemini) and OpenRouter Inc. Headquarters / Contact: Google: 1600 Amphitheatre Pkwy, Mountain View, CA 94043, USA. OpenRouter: San Francisco, CA, USA. Description of activity: Generating text content (e.g., reports) based on data entered by the User through the integration of the Google Gemini service and the OpenRouter platform. Privacy policy: Google: https://policies.google.com/privacy; OpenRouter: https://openrouter.ai/privacy

4. IT Security and External Service Providers

To maintain the security of the Website, ensure continuous availability of the service, and prevent malicious attacks (e.g., DDoS, hacking attempts, data theft), the Controller uses specialized external partners.

Due to technical necessity, these services may log visitors' IP addresses, browsing data (User-Agent), and request metadata. The services may place security cookies essential for operation on the user's device, which do not serve marketing purposes.

Legal basis for data processing: The legitimate interest of the Controller (Article 6(1)(f) of the GDPR), which is related to protecting the integrity, confidentiality, and availability of the system, and to business continuity.

Data retention: Security log files are automatically deleted by the providers after neutralizing the threat or following a specified technical period (usually 30 days).

- Processor name: Cloudflare, Inc. Headquarters / Contact: 101 Townsend St, San Francisco, CA 94107, USA. Description of activity and Processed data: Content Delivery Network (CDN), Web Application Firewall (WAF), DDoS protection. Processed data: IP address, system configuration information, traffic data, necessary cookies. Privacy policy / Data transfer: The company participates in the EU-US Data Privacy Framework.
- Processor name: Defiant, Inc. (Wordfence). Headquarters / Contact: 800 5th Ave Ste 4100, Seattle, WA 98104, USA. Description of activity and Processed data: Endpoint-based website protection, intrusion detection system, malicious code filtering. Processed data: IP address, data of login attempts, log of blocked requests, necessary cookies. Privacy policy / Data transfer: Data transfer is based on Standard Contractual Clauses (SCC) approved by the European Commission.

16. Social media platforms

The fact of data collection, the scope of processed data: Name registered on Twitter/Pinterest/Youtube/Instagram/TikTok/Linkedin etc. social media platforms, and the user's public profile

picture.

Scope of data subjects: All data subjects who have registered on Twitter/Pinterest/Youtube/ Instagram/TikTok/Linkedin etc. social media platforms and “liked” the Service Provider’s social media page, or contacted the controller through the social media platform.

Purpose of data collection: Sharing, “liking”, following, or promoting certain content elements, products, promotions of the website, or the website itself on social media platforms.

Duration of data processing, deadline for deleting data, identity of potential controllers entitled to access the data, and description of data subjects’ rights related to data processing: The data subject can obtain information about the source of the data, their processing, the method of transfer, and its legal basis on the given social media platform. Data processing takes place on the social media platforms, thus the duration and method of data processing, as well as the possibilities for deleting and modifying data, are subject to the regulations of the respective social media platform.

Legal basis for data processing: the data subject’s voluntary consent to the processing of their personal data on social media platforms.

17. Facebook / Meta joint controllership

The Controller has a Facebook / Meta profile related to its activity. Data processing for statistical purposes carried out on the Facebook social media platform constitutes joint controllership between the Controller and Facebook Ireland Ltd. (4 Grand Canal Square, Grand Canal Harbour, D2 Dublin, Ireland). Detailed information on the joint controllership agreement is provided by the Page Insights Controller Addendum. The addendum is available at the following link: https:// www.facebook.com/legal/terms/page_controller_addendum

The Controller only communicates via private messages on the social media platform if you contact us there.

1. Categories of data subjects:

- Data subjects who registered on the social media platform and “liked” the Controller’s profile page.
- Data subjects who contact the Controller via private message on the social media platform.

2. Purpose of data processing: The purpose of data processing is to share and promote the Controller’s activities and services on the Facebook social media platform. The Controller may use the data provided by the data subject in a private message to reply to the message; otherwise, the Controller does not collect or extract data from social media platforms.

3. Legal basis for data processing: Data processing is based on Article 6(1)(a) of the GDPR; the legal basis is the data subject’s consent to the processing of their personal data on the Facebook social media platform.

4. Scope of processed data:

- Data subject’s registered name,
- Data subject user’s public profile picture,
- Other public data provided or shared by the data subject on the social media platform.

5. Source of processed personal data: The source of the processed data is the data subject.

6. Withdrawal of consent: You can withdraw your consent to data processing at any time, and you can delete your post or comment. Data processing takes place via social media platforms operated by third parties. If you withdraw your consent, the Controller will delete the conversation held with you. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

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

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

7. Duration of data processing:

- Until the withdrawal of the data subject's consent,
- If an exchange of messages takes place, for 2 years.

8. Transfer of personal data, recipients, and categories of recipients: See Article 4(9) of the GDPR for the definition of recipient. The Controller only hands over the Data Subject's personal data to state bodies or authorities—in particular to courts, public prosecutor's offices, investigating authorities, infringement authorities, and the National Authority for Data Protection and Freedom of Information—in exceptional cases and based on a legal obligation.

9. Possible consequences of failure to provide data: In case of failure to provide data, the data subject cannot obtain information about the Controller's activities and services via the Facebook social media platform or send a message to the Controller via Facebook Messenger.

10. Automated decision-making (including profiling): Automated decision-making, including profiling, does not take place during data processing.

11. Joint controllership agreement with Facebook Ireland Ltd.: The Page Insights feature displays aggregated data that helps understand how data subjects use the Facebook page. Facebook Ireland Limited ("Facebook Ireland") and the Controller are joint controllers concerning the processing of insights data. The Page Insights Addendum defines the responsibilities of Facebook and the Controller regarding the processing of insights data. Facebook Ireland assumes primary responsibility under the GDPR for the processing of insights data and to comply with all applicable obligations under the GDPR with respect to the processing of insights data. Facebook Ireland also makes the essence of the Page Insights Addendum available to data subjects. The Controller ensures that it has an appropriate legal basis under the GDPR for processing insights data, identifies the controller of the page, and complies with any other applicable legal obligations. The sole responsibility of Facebook Ireland is the processing of personal data in connection with the Page Insights feature, except for data falling within the scope of the Page Insights Addendum. The Page Insights Addendum does not grant the Controller the right to request personal data of Facebook users processed by Facebook Ireland in connection with Facebook, including page insights data. The Controller cannot act on behalf of or respond on behalf of Facebook Ireland in fulfilling data protection requests.

18. Customer relations and other data processing operations

If a question arises or the data subject has a problem while using the controller's services, they can contact the controller via the methods provided on the website (phone, e-mail, social media platforms, etc.).

The Controller deletes incoming e-mails, messages, and data provided via phone, Meta, etc., along with the name and e-mail address of the inquirer and any other voluntarily provided personal data, after a maximum of 2 years from the date of data communication.

Information regarding data processing operations not listed in this policy will be provided at the time the data is collected.

Upon exceptional official requests or requests from other bodies authorized by law, the Service Provider is obliged to provide information, disclose or transfer data, or make documents available.

In such cases, provided that the requesting party has indicated the exact purpose and scope of the data, the Service Provider will only release personal data to the extent and in the measure that is strictly necessary for the realization of the purpose of the request.

19. Rights of data subjects

1. Right of access

You have the right to obtain from the controller confirmation as to whether or not personal data concerning you are being processed, and, where that is the case, access to the personal data and the information listed in the Regulation.

2. Right to rectification

You have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning you. Taking into account the purposes of the processing, you have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

3. Right to erasure

You have the right to obtain from the controller the erasure of personal data concerning you without undue delay and the controller shall have the obligation to erase personal data concerning you without undue delay where certain conditions apply.

4. Right to be forgotten

Where the controller has made the personal data public and is obliged to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that you have requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

5. Right to restriction of processing

You have the right to obtain from the controller restriction of processing where one of the following applies:

- The accuracy of the personal data is contested by you, for a period enabling the controller to verify the accuracy of the personal data;
- The processing is unlawful and you oppose the erasure of the personal data and request the restriction of their use instead;
- The controller no longer needs the personal data for the purposes of the processing, but they are required by you for the establishment, exercise or defence of legal claims;

- You have objected to processing; in this case, the restriction applies for the period pending the verification whether the legitimate grounds of the controller override your legitimate grounds.

6. Right to data portability

You have the right to receive the personal data concerning you, which you have provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided (...)

7. Right to object

In the case of data processing based on legitimate interest or public authority powers as legal bases, you have the right to object, on grounds relating to your particular situation, at any time to processing of personal data concerning you (...), including profiling based on those provisions.

8. Objection in the case of direct marketing

Where personal data are processed for direct marketing purposes, you have the right to object at any time to processing of personal data concerning you for such marketing, which includes profiling to the extent that it is related to such direct marketing. Where you object to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

9. Automated individual decision-making, including profiling

You have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or similarly significantly affects you.

The preceding paragraph shall not apply if the decision:

- is necessary for entering into, or performance of, a contract between you and a data controller;
- is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard your rights and freedoms and legitimate interests; or
- is based on your explicit consent.

20. Time limit for action

The controller shall provide information on action taken on a request to you without undue delay and in any event within 1 month of receipt of the request.

That period may be extended by 2 further months where necessary. The controller shall inform you of any such extension within 1 month of receipt of the request, together with the reasons for the delay.

If the controller does not take action on your request, the controller shall inform you without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

21. Security of processing

Taking into account the state of the art, the costs of implementation and the nature, scope, context

and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- the pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The processed data must be stored in such a way that unauthorized persons cannot access it. In the case of paper-based data carriers, by establishing the order of physical storage and filing, and in the case of data processed in electronic form, by using a central access management system.

The method of storing data by IT means must be chosen so that their deletion—also taking into account a potentially different deletion deadline—can be performed upon the expiration of the data deletion deadline, or if it is necessary for other reasons. The deletion must be irreversible.

Paper-based data carriers must be stripped of personal data using a document shredder or by employing an external organization specialized in document destruction. In the case of electronic data carriers, physical destruction must be ensured according to the rules for scrapping electronic data carriers, and if necessary, the data must be securely and irreversibly deleted beforehand.

The controller implements the following specific data security measures:

To ensure the security of personal data processed on paper, the Service Provider applies the following measures (physical protection):

- Documents are placed in a secure, lockable dry room.
- If the personal data processed on paper are digitized, the rules governing digitally stored documents must be applied.
- During work, the Service Provider’s employee performing data processing may only leave the room where data processing takes place by locking away the data carriers entrusted to them or locking the given room.
- Personal data may only be accessed by authorized persons; third parties may not access them.
- The Service Provider’s building and premises are equipped with fire and property protection equipment.

IT protection

- Computers and mobile devices (other data carriers) used during data processing are the property of the Service Provider.
- The computer system containing personal data used by the Service Provider is equipped with antivirus protection.
- To ensure the security of digitally stored data, the Service Provider uses data backups and archiving.
- The central server machine can only be accessed with appropriate authorization and only by designated persons.
- Data on the computers can only be accessed with a username and password.

22. Communication of a personal data breach to the data subject

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

The communication to the data subject shall describe in clear and plain language the nature of the personal data breach and contain at least the name and contact details of the data protection officer or other contact point where more information can be obtained; describe the likely consequences of the personal data breach; describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The communication to the data subject shall not be required if any of the following conditions are met:

- the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
- the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;
- it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so.

23. Notification of a personal data breach to the supervisory authority

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

24. Review in the case of mandatory processing

If the duration or the necessity of periodic review of the mandatory processing is not determined by law, local government decree, or a mandatory legal act of the European Union, the controller shall review at least every three years from the commencement of the processing whether the processing of personal data by the controller, or by a processor acting on its behalf or under its instruction, is necessary for the realization of the purpose of the processing.

The controller shall document the circumstances and result of this review, keep this documentation for ten years following the performance of the review, and make it available to the National Authority for Data Protection and Freedom of Information (hereinafter: Authority) upon the Authority’s request.

25. Right to lodge a complaint

A complaint against possible infringement by the controller can be filed with the National Authority for Data Protection and Freedom of Information (Nemzeti Adatvédelmi és Információszabadság Hatóság):

National Authority for Data Protection and Freedom of Information

1055 Budapest, Falk Miksa utca 9-11., Hungary

Postal address: 1363 Budapest, Pf. 9., Hungary

Phone: +36 -1-391-1400

Fax: +36-1-391-1410

E-mail: ugyfelszolgalat@naih.hu

26. Closing remarks

During the preparation of this policy, we took into account the following legislation and recommendations:

- 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) (GDPR);
- Act CVIII of 2001 on certain issues of electronic commerce services and information society services (especially Section 13/A);
- Act XLVII of 2008 on the Prohibition of Unfair Commercial Practices against Consumers;
- Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities (especially Section 6);
- Act XC of 2005 on Electronic Freedom of Information;
- Act C of 2003 on Electronic Communications (specifically Section 155);
- EASA/IAB Recommendation on best practice for online behavioural advertising (Opinion 16/2011);
- Recommendation of the National Authority for Data Protection and Freedom of Information on the data protection requirements of preliminary information.

- Privacy Policy – IPMFlow.com – 2025.06.12.
- Privacy Policy – IPMFlow.com – 2025.06.16.
- Privacy Policy – IPMFlow.com – 2025.11.19.
- Privacy Policy – IPMFlow.com – 2025.11.23.