# Privacy Policy – IPMFlow.com - IPMflow

Last updated: 2026.03.09.

# Trapshop Kft.
# Privacy Policy

## Introduction

The data processing of **Trapshop Kft.** (8797 Batyk, Fő utca 34, tax number: 32050547-2-20, company registration number: 2009078346) (hereinafter: Service Provider, Data Controller) is carried out in accordance with the provisions of this privacy policy.

We provide the following information 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).

This privacy policy regulates the data processing of the following websites/mobile applications: **https://ipmflow.com/ ; app.ipmflow.com**

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

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

## The Data Controller and contact details

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

## 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;
- **"third party":** a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

## 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 Data Controller declares that its data processing is carried out in accordance with the principles set out in this section.

## Data processing related to sales / provision of services

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

| Personal data | Purpose of data processing | Legal basis |
|---|---|---|
| First and last name | Necessary for contact, purchase, and issuing a lawful invoice. | Article 6(1)(b) of the GDPR |
| E-mail address | Keeping contact. Sending messages and invoices. | Article 6(1)(b) of the GDPR |
| Phone number | Keeping contact, more efficient reconciliation of billing questions. | Article 6(1)(b) of the GDPR |
| Billing name and address | Issuing a lawful invoice, as well as concluding the contract, defining its content, amending it, monitoring its performance, invoicing the fees arising from it, and enforcing related claims. | Article 6(1)(c) of the GDPR:<br>Legal obligation: Section 169 (2) of Act C of 2000 on Accounting |
| Date of order / purchase | Execution of a technical operation. | Article 6(1)(b) of the GDPR |
| IP address of order / purchase | Execution of a technical operation. | 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 erasure of data:** It lasts until the data subject's request for erasure, if any of the conditions in Article 17(1) of the GDPR are met. Based on Article 19 of the GDPR, the Data Controller shall inform the data subject electronically of the erasure of any personal data provided by the data subject. If the data subject's request for erasure also covers the e-mail address they provided, the Data Controller will also erase the e-mail address following the notification. Except in the case of accounting documents, as under 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 documents directly and indirectly supporting the accounting records (including ledger accounts, analytical or detailed records) must be kept in a legible form, retrievable by reference to the accounting records, for at least 8 years.

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

**5. Description of data subjects' rights regarding data processing:**

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

**6. The data subject can initiate access to personal data, their erasure, modification, or restriction of processing, and the portability of 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 data processing:**

1. Article 6(1)(b) and (c) of the GDPR,
2. Section 13/A (3) of Act CVIII of 2001 on certain issues of electronic commerce services and information society services (hereinafter: E-commerce Act):
   The service provider may process personal data that are technically indispensable for providing the service. Should other conditions be identical, the service provider must select and continuously operate the equipment used in providing the information society service in a way that personal data is only processed if it is strictly necessary for providing the service and fulfilling other purposes defined in this Act, but even in this case, only to the extent and for the time strictly necessary.
3. In case of issuing an invoice compliant with accounting legislation, Article 6(1)(c).
4. In case of enforcing claims arising from the contract, 5 years according to Section 6:21 of Act V of 2013 on the Civil Code.
   *Section 6:22 [Limitation]*
   *(1) Unless otherwise provided in this Act, claims shall lapse in five years.*
   *(2) The limitation period begins when the claim becomes due.*
   *(3) An agreement to change the limitation period must be put in writing.*
   *(4) An agreement excluding limitation is null and void.*

**8. Please be informed that:**

- the data processing is necessary for the performance of a contract.
- you are required to provide personal data so that we can fulfill your order.
- failure to provide data has the consequence that we cannot process your order.

## Providing the Service (Using IPMFlow Tools)

**Purpose of data processing:** Ensuring the operation of IPMFlow smart 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, especially (but not limited to):

- **Site data:** Facility name, description, environmental risk factors (water, green area, neighbors, waste), seasonal factors, general comments and measures.
- **Location data:** Location name, description, risk category, service intervals, potential pests list, indicator system description, quantity of traps, structural/hygiene/entry point risks, location-specific comments and measures.
- **Assessment data:** Assessment date, identified pest, hazard type and description,

probability and severity values, calculated risk level, proposed/implemented measures, 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 Data Controller processes the entered data for the purpose of the operation of the service.

**AI (Google Gemini) based data processing:**

- Certain functions of the Service (e.g., report generation) operate with the help of artificial intelligence (Google Gemini, via the OpenRouter API).
- 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 Data 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 associated with the User's account in the Service system.
- The Data 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 their possible use to develop Google's own services or train its models, is governed by Google's currently effective privacy policies and terms of service, which the User can consult on Google's platforms.

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

## Contact

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

| Personal data | Purpose of data processing | Legal basis |
|---|---|---|
| Name | Identification | Article 6(1)(a) of the GDPR |
| E-mail address | Keeping contact, sending reply messages | Article 6(1)(a) of the GDPR |
| Phone number | Keeping contact | Article 6(1)(a) of the GDPR |
| Content of the message, if it contains personal data | Necessary for replying | Article 6(1)(a) of the GDPR |

*In the case of the e-mail address, it is not necessary that it contains personal data.*

**2. Scope of data subjects:** All data subjects sending messages via the contact form.

**3. Duration of data processing, deadline for erasure of data:** The Data Controller processes the personal data until the data processing purpose is achieved, but for a maximum of 2 years. If any of the conditions in Article 17(1) of the GDPR are met, the data processing lasts until

the data subject's request for erasure.

**4. Description of data subjects' rights regarding data processing:**

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

**5. The data subject can initiate access to personal data, their erasure, modification, or restriction of processing, and the portability of 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.

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

**7. Please be informed that:**

- this data processing is based on your consent and is necessary for providing an offer.
- you are required to provide personal data to be able to contact us.
- failure to provide data has the consequence that you cannot contact the Data Controller.
- the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

## 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. Fact of data processing, 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, providing customized operation.

**5. Duration of data processing, deadline for erasure of data:**

| Cookie type | Legal basis for data processing | Duration of data processing |
|---|---|---|
| Session cookies or other cookies essential for website operation | No data processing occurs with the use of the cookie. | Period lasting until the end of the relevant visitor session, meaning it only remains on the computer until the browser is closed. |
| Statistical, marketing cookies | Article 6(1)(a) of the GDPR | 1 day – 2 years, according to the cookie policy, or until the data subject's withdrawal of consent. |

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

**7.** Most browsers used by our users allow adjusting which cookies should be saved and enable the deletion of (specific) cookies again. If you restrict the saving of cookies on specific 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?hl=hu)
- 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/en-gb/guide/safari/sfri11471/mac)

## Use of Google Ads Conversion Tracking

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

When a User reaches a website via a Google ad, a cookie required 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 Data Controller can see that the User clicked on the ad.

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

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

If you do not wish to participate in conversion tracking, you can opt-out by disabling the installation of 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 to Google for advertising purposes regarding user data. ad_personalization controls whether data can be used to personalize ads (e.g., remarketing). The Data Controller ensures the collection and withdrawal of appropriate consents on its cookie banner / panel. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.
Further information and Google's privacy statement are available at: https://policies.google.com/privacy

## Application of Google Analytics

This website uses the Google Analytics application, a web analytics service provided by Google Inc. ("Google"). Google Analytics uses so-called "cookies", text files stored on your computer, to help analyze the User's use of the website.

The information generated by the cookies about the website used by the User is usually transmitted to and stored on a Google server in the USA. By activating IP anonymization on the website, Google will shorten the User's IP address beforehand within Member States of the European Union or in other contracting states of 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 shortened 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 related to website and internet usage.

The IP address transmitted by the User's browser within the framework of Google Analytics will not be merged with other Google data. The User may prevent the storage of cookies by adjusting their browser settings accordingly; however, please note that if you do this, you may not be able to fully use all functions of this website. You can also prevent Google from collecting and processing data generated by the cookies regarding the User's website usage (including IP address) by downloading and installing the browser plugin available at the following link: https://tools.google.com/dlpage/gaoptout?hl=en

## Newsletter, DM 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, unless otherwise provided by a separate act, advertising may only be communicated to a natural person – User – as the recipient of the advertisement by means of direct contact (hereinafter: direct marketing), in particular by electronic mail or equivalent individual communication devices, if the recipient of the advertisement has given prior, clear, and explicit consent.

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

**3.** The Service Provider does not send unsolicited commercial messages, and the User may unsubscribe from receiving offers free of charge, without restriction and without giving a reason. In this case, the Service Provider deletes all personal data from its register – necessary for sending promotional messages – and will not contact the User with further promotional 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 | Purpose of data processing | Legal basis |
|---|---|---|
| Name, e-mail address. | Identification, enabling subscription to the newsletter/discount coupons. | Consent of the data subject, Article 6(1)(a) of the GDPR. |
| Date of subscription | Execution of a technical operation. | Consent of the data subject, Article 6(1)(a) of the GDPR. |
| IP address at the time of subscription | Execution of a technical operation. | Consent of the data subject, Article 6(1)(a) of the GDPR. |

**5.** Newsletters are sent 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 erasure of data:** Data processing lasts until the withdrawal of consent (unsubscription, until the data subject's request for erasure), or until the discontinuation of the newsletter.

**9. Description of data subjects' rights regarding data processing:**

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

**10. The data subject can initiate access to personal data, their erasure, modification, or restriction of processing, and the portability of 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.

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

**12. Please be informed that:**

- the data processing is based on your consent.
- you are required to provide personal data if you wish to receive newsletters from us.
- failure to provide data has the consequence that we cannot send you newsletters.
- please be informed 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.

## Complaint Handling

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

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

| Personal data | Purpose of data processing | Legal basis |
|---|---|---|
| Billing name and address | | |

**2. Scope of data subjects:** All data subjects purchasing on the website and submitting a quality objection or complaint.

**3. Duration of data processing, deadline for erasure of data:** Copies of the record taken of the objection, the transcript and the reply given to it must be kept for 3 years under Section 17/A (7) of Act CLV of 1997 on Consumer Protection.

**4. Description of data subjects' rights regarding data processing:**

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

**5. The data subject can initiate access to personal data, their erasure, modification, or restriction of processing, and the portability of 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.

**6. Please be informed 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 required to provide personal data so that we can handle your complaint.
- failure to provide data has the consequence that we cannot handle the complaint you have submitted.

## 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:**
Barion Payment Zrt.
Registered seat: H-1117, Budapest, Infopark sétány 1.
License number: H-EN-I-1064/2013
Institution ID: 14859034
Phone: + 36 1 464 70 99

**3. Fact of data processing, 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 (fraud checks) performed to protect users.

**6. Duration of data processing, deadline for erasure of data:** Lasts until the execution of the online payment.

**7. Legal basis for data processing:** Article 6(1)(b) of the GDPR. Data processing is necessary to execute the online payment at the data subject's request.

**8. Rights of the data subject:**

- a. You can be informed about the circumstances of 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 data 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.

## Processors Used

### Hosting Provider

**1. Activity performed by Data Processor:** Hosting Service

**2. Name and contact details of Data Processor:**
Details of IT systems providing the service (hosting providers):

- **Rackhost Zrt.**
  Activity: Hosting service of the related informational website (ipmflow.com)
  Registered seat: 6722 Szeged, Tisza Lajos körút 41.
  E-mail: info@rackhost.hu
  Phone: +36 1 445 1200
  Website: www.rackhost.hu
- **Cloudways Ltd. (DigitalOcean)**
  Activity: Server and database hosting (Backend system and data storage)
  Registered seat: Junction Business Centre, 1st Floor Sqaq Lourdes, St Julians STJ3334, Malta
  E-mail: info@cloudways.com
  Website: www.cloudways.com
- **Vercel Inc.**
  Activity: Hosting and cloud-based execution of the software frontend web application (app.ipmflow.com)
  Registered seat: 340 S Lemon Ave #4133, Walnut, CA 91789, USA
  Website: www.vercel.com

**3. Fact of data processing, 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 operating it properly.

**6. Duration of data processing, deadline for erasure of data:** Data processing lasts until the termination of the agreement between the data controller and the hosting provider, or until the data subject's request for erasure submitted 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. Legitimate interest is the proper operation of the website, protection against attacks and fraud.

**Other Data Processors (if any)**

**1. Hosting and Infrastructure Providers**

| Name of Data Processor | Registered seat / Contact | Description of activity | Privacy Policy |
|---|---|---|---|
| Rackhost Zrt. | 6722 Szeged, Tisza Lajos körút 41.<br>E-mail: info@rackhost.hu<br>Phone: +36 1 445 1200 | Hosting service, hosting of the main website (ipmflow.com) and static content. | https://www.rackhost.hu/privacy-policy |
| Cloudways Ltd. (DigitalOcean) | Junction Business Centre, 1st Floor Sqaq Lourdes, St Julians STJ3334, Malta<br>Website: www.cloudways.com<br>E-mail: info@cloudways.com | Server and database hosting (api.ipmflow.com), secure storage of the backend system and user data (Frankfurt server center). | https://www.cloudways.com/en/privacy.php |
| Vercel Inc. | 340 S Lemon Ave #4133, Walnut, CA 91789, USA | Cloud-based execution, serving and optimization of the Frontend web application (app.ipmflow.com). | Vercel GDPR Compliance<br>Cookie Policy |

**2. General administration, billing, and communication**

| Name of Data Processor | Registered seat / Contact | Description of activity | Privacy Policy |
|---|---|---|---|
| Billingo Technologies Zrt. | 1133 Budapest, Árbóc utca 6. III. floor<br>E-mail: hello@billingo.hu | Billing service, issuing and storing electronic invoices. | https://www.billingo.hu/adatkezelesi-tajekoztato |
| Kutyavilág Kft. and Animadó Kft. | Based on a contract with the Data Controller. | Accounting. Fulfilling the accounting and tax obligations of the Data Controller. | Regulated in contract. |
| Bithuszárok Bt. (Listamester) | 2053 Herceghalom, Liget utca 3.<br>E-mail: info@listamester.hu | Sending newsletters to subscribers, e-mail marketing. | https://listamester.hu/adatkezelesi-tajekoztato.php |
| Resend Labs Inc. | 2261 Market Street #4816, San Francisco, CA 94114, USA | Technical transmission of transactional e-mails (e.g., order confirmation) (SMTP provider). | https://resend.com/legal/privacy-policy |

### 3. Online Payment Service Providers

| Name of Data Processor | Registered seat / Contact | Description of activity | Privacy Policy |
|---|---|---|---|
| Barion Payment Zrt. | 1117 Budapest, Infopark sétány 1. I. building 5. floor 5.<br>License number: H-EN-I-1064/2013 | Execution of online bank card payments, fraud prevention. | https://www.barion.com/hu/adatvedelmi-tajekoztato/ |

### 4. Analytics, marketing, and Artificial Intelligence (AI)

| Name of Data Processor | Registered seat / Contact | Description of activity | Privacy Policy |
|---|---|---|---|
| Google Ireland Limited | Gordon House, Barrow Street, Dublin 4, Ireland | Google Analytics 4: Visitor statistics, web analytics.<br>Google Ads: Serving ads, conversion tracking, remarketing.<br>Google Workspace: Business email, document storage. | https://policies.google.com/privacy |
| Google LLC (Gemini) and OpenRouter Inc. | Google: 1600 Amphitheatre Pkwy, Mountain View, CA 94043, USA<br>OpenRouter: San Francisco, CA, USA | Generating textual content (e.g., reports) based on the data entered by the User through the integration of the Google Gemini service and the OpenRouter platform. | Google: https://policies.google.com/privacy<br>OpenRouter: https://openrouter.ai/privacy |

### 5. IT Security and External Providers

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

Out of 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 Data Controller (Article 6(1)(f) of the GDPR), which attaches to the protection of the integrity, confidentiality, and availability of the system, as well as business continuity.

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

| Name of Data Processor | Registered seat / Contact | Description of activity and Processed data | Privacy Policy / Data Transfer |
|---|---|---|---|
| Cloudflare, Inc. | 101 Townsend St, San Francisco, CA 94107, USA | Activity: Content Delivery Network (CDN), Web Application Firewall (WAF), DDoS protection.<br>Processed data: IP address, | Privacy Policy<br>The company participates in the EU-US Data Privacy Framework. |

| Name of Data Processor | Registered seat / Contact | Description of activity and Processed data | Privacy Policy / Data Transfer |
|---|---|---|---|
| | | system configuration info, traffic data, necessary cookies. | |
| Defiant, Inc. (Wordfence) | 800 5th Ave Ste 4100, Seattle, WA 98104, USA | Activity: Endpoint-based website protection, intrusion detection system, filtering malicious codes.<br>Processed data: IP address, login attempt data, blocked requests log, necessary cookies. | Privacy Policy<br>Data transfer takes place based on Standard Contractual Clauses (SCC) approved by the European Commission. |

## Social Media

**The fact of data collection, the scope of processed data:** Registered name on Twitter/ Pinterest/Youtube/Instagram/TikTok/Linkedin etc. social media sites, 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 sites, and "liked" the Service Provider's social media page, or contacted the data controller through the social media site.

**Purpose of data collection:** Sharing, "liking", following, or promoting certain content elements of the website, its products, promotions, or the website itself on social media sites.

**Duration of data processing, deadline for erasure of data, persons of potential data controllers entitled to access the data, and description of data subjects' rights regarding data processing:** The data subject can find information about the source of the data, their processing, the method of transfer, and its legal basis on the given social media site. Data processing takes place on the social media sites, so the duration and method of data processing, as well as the possibilities of deleting and modifying data, are governed by the regulations of the respective social media site.

**Legal basis for data processing:** the data subject's voluntary consent to the processing of their personal data on social media sites.

### Facebook / Meta joint controllership

The Data Controller maintains a Facebook / Meta profile for its activity. Data processing for statistical purposes carried out on the Facebook social media site is joint data processing between the Data Controller and Facebook Ireland Ltd. (4 Grand Canal Square, Grand Canal Harbour, D2 Dublin Ireland). The Controller Addendum for Facebook Page Insights provides detailed information about the details of the joint controllership agreement. The addendum is available at the following link: https://www.facebook.com/legal/terms/page_controller_addendum

The Data Controller only communicates in private messages on the social media site if you contact us there.

**1. Categories of data subjects:**

- data subjects who have registered on the social media site and “liked” the Data Controller’s profile page,
- data subjects who contact the Data Controller in a private message on the social media site.

**2. Purpose of data processing:** The purpose of data processing on the Facebook social media site is sharing or promoting the activity and services of the data controller. The Data Controller may use the data provided by the data subject in a private message to reply to the message; otherwise, the Data Controller does not collect or extract data through social media sites.

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

**4. Scope of processed data:**

- registered name of the data subject,
- public profile picture of the data subject user,
- other public data provided and shared by the data subject on the social media site.

**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, delete your post or comment. Data processing takes place through social media sites operated by a third party. If you withdraw your consent, the Data Controller will delete the conversation with you. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

The data subject can initiate access to personal data, their erasure, modification, or restriction of processing, and the portability of 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. Duration of data processing:**

- until the data subject’s withdrawal of consent,
- if a message exchange occurs, then 2 years.

**8. Transfer of personal data, recipients, or categories of recipients:** For the definition of recipient, see Article 4(9) of the GDPR. The Data Controller only transfers the Data Subject’s personal data to state bodies, authorities – in particular courts, prosecution offices, investigating authorities, offense 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 Data Controller’s activities and services via the Facebook social media site, nor send a message to the Data 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 function displays aggregated data that helps understand how data subjects use

the Facebook page. Facebook Ireland Limited (“Facebook Ireland”) and the Data Controller are joint controllers regarding the processing of analytics data. The Page Insights Addendum defines the responsibility of Facebook and the responsibility of the Data Controller regarding the processing of analytics data. Facebook Ireland assumes primary responsibility under the GDPR for the processing of analytics data, and to comply with all relevant obligations prescribed in the GDPR regarding the processing of analytics data. Facebook Ireland also makes the essence of the Page Insights Addendum available to all data subjects. The Data Controller ensures that it has an appropriate legal basis under the GDPR for processing analytics data, identifies the controller of the page, and complies with all other relevant legal obligations. It is the sole responsibility of Facebook Ireland to process personal data in connection with the Page Insights function, except for data falling within the scope of the Page Insights Addendum. The Page Insights Addendum does not grant the Data Controller the right to request the personal data of Facebook users processed by Facebook Ireland in connection with Facebook, including page insights data. The Data Controller cannot act or respond on behalf of Facebook Ireland when fulfilling data protection requests.

## Customer Relations and Other Data Processing

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

The Data Controller deletes incoming e-mails, messages, data provided by phone, on Meta, etc., together with the inquirer’s name, e-mail address, and other voluntarily provided personal data, after a maximum of 2 years from data disclosure.

We provide information on data processing not listed in this policy at the time of data collection.

Upon exceptional official request, or based on the authorization of law upon request by other bodies, the Service Provider is obliged to provide information, disclose data, hand over data, or make documents available.

In these cases, the Service Provider only releases personal data to the requesting party – provided they have specified the exact purpose and the scope of data – to the extent and degree that is strictly necessary to achieve the purpose of the request.

## Rights of the 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 upon request. 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 without undue delay where specific grounds 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 the data subject has 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; 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 processing based on legitimate interests or public authority mandate 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 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. If 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.

**Deadline for taking action**
The controller shall provide information on action taken on a request under the above rights 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.

## 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.

Processed data must be stored in a way that unauthorized persons cannot access them. 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 applying a central access management system.

The method of storing data using IT methods must be chosen in such a way that their deletion – with regard to potentially different deletion deadlines – can be performed when the data deletion deadline expires, or if necessary for other reasons. Deletion must be irreversible.

Paper-based data carriers must be stripped of personal data using a paper 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 regarding the disposal of electronic data carriers, or, if necessary, the safe and irreversible deletion of data must be carried out in advance.

The Data Controller takes the following specific data security measures:

In order to secure personal data processed on paper, the Service Provider applies the following measures (physical protection):

- Documents are placed in a secure, well-lockable dry room.
- If paper-based personal data are digitized, the rules governing digitally stored documents must be applied.
- The Service Provider’s employee performing data processing may only leave the room where data processing is taking place during work by locking up 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 virus protection.
- To ensure the security of digitally stored data, the Service Provider uses data backups and archiving.
- Only authorized persons with proper authorization can access the central server machine.
- Data on computers can only be accessed with a username and password.

## 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.

## 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.

## Review in Case of Mandatory Data Processing

If the duration or the necessity of periodic review of mandatory data processing is not determined by law, local government decree, or mandatory legal act of the European Union, the controller shall review at least every three years from the start of data 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 data processing.

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

## Possibility to File a Complaint

In case of a potential legal violation by the data controller, a complaint can be filed with the National Authority for Data Protection and Freedom of Information:
**National Authority for Data Protection and Freedom of Information (NAIH)**
1055 Budapest, Falk Miksa utca 9-11.
Mailing address: 1363 Budapest, Pf. 9.
Phone: +36 -1-391-1400
Fax: +36-1-391-1410
E-mail: ugyfelszolgalat@naih.hu

## Closing Remarks

When drafting this policy, we took the following legislation and recommendations into account:

- 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);
- Opinion 16/2011 on the EASA/IAB Best Practice Recommendation on Online Behavioural Advertising;
- Recommendation of the National Authority for Data Protection and Freedom of Information on the data protection requirements for prior 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.
- Privacy Policy – IPMFlow.com – 2026.02.24.