Privacy Policy – IPMFlow.com

Last updated: 2025.06.12.

Trapshop Kft.

Privacy Policy

1. Introduction

Trapshop Kft. (registered office: 8797 Batyk, Fő utca 34, tax number: 32050547-2-20, company registration number/registration number: 2009078346) (hereinafter: Service Provider, data controller) subjects itself to the following policy.

We provide the following information in accordance with REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

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

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

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

2. The data controller and its contact details

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

3. Definitions

- **‘personal data’**: means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- **‘processing’**: means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- **‘data controller’**: means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- **‘data processor’**: means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- **‘recipient’**: means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;
- **‘consent’ of the data subject**: means any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
- **‘personal data breach’**: means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

- **‘profiling’**: means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

4. Principles relating to processing of personal data

Personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject (**‘lawfulness, fairness and transparency’**);
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (**‘purpose limitation’**);
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**‘data minimisation’**);
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (**‘accuracy’**);
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (**‘storage limitation’**);
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (**‘integrity and confidentiality’**).

The controller shall be responsible for, and be able to demonstrate compliance with, the ›ve (**‘accountability’**).

The data 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 the data processed and the **purpose** of the processing:

Personal Data	Purpose of Data Processing	Legal Basis
First name and surname	Necessary for contact, purchase, and issuing a lawful invoice.	Article 6(1)(b) of the GDPR
E-mail address	Contact. Sending messages, invoices.	Article 6(1)(b) of the GDPR
Phone number	Contact, more efficient coordination of questions related to invoicing.	Article 6(1)(b) of the GDPR
Billing name and address	Issuing a lawful invoice, as well as creating, determining the content of, modifying, monitoring the performance of the contract, invoicing the fees arising from it, and enforcing the related claims.	Article 6(1)(c) of the GDPR: 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 the order/purchase	Execution of a technical operation.	Article 6(1)(b) of the GDPR

2. Scope of data subjects: All data subjects making a purchase on the website.

3. Duration of data processing, deadline for erasure of data: If any of the conditions set out ırticle 17(1) of the GDPR are met, processing lasts until the data subject's request for

erasure. The data controller shall inform the data subject electronically of the erasure of any personal data provided by the data subject, in accordance with Article 19 of the GDPR. If the data subject's request for erasure also extends to the e-mail address provided by them, the data controller shall also erase the e-mail address after the notification. An exception is made for 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 erased 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 bookkeeping accounts (including general ledger accounts, analytical and detailed records) must be kept in a legible form for at least 8 years, retrievable by reference to the accounting records.

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

5. Description of the rights of data subjects in relation to data processing:

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

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

- by post at the address 8797 Batyk, Fő utca 34,
- by e-mail at the e-mail address 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: Elker tv.):
   The service provider may process personal data that are technically essential for the provision of the service. The service provider, provided that the other conditions are the same, must choose and in all cases operate the means used in the provision of the information society service in such a way that personal data are processed only if it is absolutely necessary for the provision of the service and for the fulfilment of other

purposes specified in this Act, but even in this case only to the extent and for the time necessary.

3. In the case of issuing an invoice in accordance with accounting legislation, Article 6(1)(c).
4. In the case of enforcing claims arising from the contract, 5 years according to Section 6:21 of Act V of 2013 on the Civil Code.
   § 6:22 [Limitation period]

   (1) Unless this Act provides otherwise, claims shall become statute-barred in five years.

   (2) The limitation period begins when the claim becomes due.

   (3) An agreement to change the limitation period must be in writing.

   (4) An agreement excluding the limitation period is 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 fulfil your order.
- failure to provide the data will result in us being **unable to process your order**.

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

Purpose of data processing: To ensure the operation of the IPMFlow intelligent pest control tools (e.g., Risk Assessment module), to process the data entered by the User, to generate analyses and reports, including the provision of AI (Google Gemini) based functions.

Scope of data processed: Data provided by the User within the framework of the Service, in particular (but not limited to):

- **Site data:** Facility name, description, environmental risk factors (water, green space, neighbours, waste), seasonal factors, general comments and measures.
- **Location data:** Location name, description, risk category, service intervals, list of potential pests, indicator system description, number of traps, structural/hygiene/entry point risks, location-specific comments and measures.

- **Assessment data:** Assessment date, identified pest, type and description of hazard, 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 entered will be processed by the Service Provider for the purpose of operating the service.

7. 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).

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

The Data Controller shall ensure the secure storage and handling of API keys and other authentication data with 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 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 only transmitted to the Google Gemini API for the purpose of performing the requested operation (e.g., report generation). The processing of data received by Google via the API, including its possible use for the development of Google’s own services or the training of its models, is subject to Google’s then-current privacy policies and terms of service, about which the User can find information 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 proper legal basis for their processing).

Contact

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

Personal Data	Purpose of Data Processing	Legal Basis
Name	Identification	Article 6(1)(a) of the GDPR
E-mail address	Contact, sending reply messages	
Phone number	Contact	
Message content, if it contains personal data	Necessary for replying	

It is not necessary for the e-mail address to contain personal data.

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

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

4. Identity of potential data controllers entitled to access the data, recipients of the personal data: Personal data may be processed by the authorised staff of the data controller.

5. Description of the rights of data subjects in relation to data processing:

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

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

- by post at the address 8797 Batyk, Fő utca 34,
- by e-mail at the e-mail address hello@ipmflow.com,

- by phone at +36 30 220 9884.

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

8. We inform you that

- this data processing is based on **your consent** or is necessary for making an offer.
- you **are obliged** to provide the personal data to be able to contact us.
- failure to provide the data will result in you being **unable to contact the data controller**.
- withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.

9. Cookie (suti) management

1. The use of so-called "password-protected session cookies", "shopping cart cookies", "security cookies", "essential cookies", "functional cookies", and "cookies responsible for managing website statistics" does not require prior consent from the data subjects.

2. The fact of data processing, the scope of the data processed: Unique identifier, 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 erasure of data:

Cookie Type	Legal Basis for Data Processing	Duration of Data Processing
Session cookies or other cookies essential for the operation of the website	No data processing occurs through the use of the cookie.	The period until the end of the relevant visitor session, i.e., it only remains on the computer until the browser is closed.

Cookie Type	Legal Basis for Data Processing	Duration of Data Processing
Statistical, marketing cookies	Article 6(1)(a) of the GDPR	1 day – 2 years, according to the cookie information notice, or until the data subject withdraws their consent.

6. Identity of potential data controllers entitled to access the data: The personal data may be accessed by the data controller.

7. Description of the rights of data subjects in relation to data processing: The data subject has the option to delete cookies in the Tools/Settings menu of browsers, usually under the Privacy settings.

8. Most browsers used by our users allow setting which cookies should be saved and allow (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 common browsers:

- **Google Chrome** (https://support.google.com/chrome/answer/95647?hl=hu)
- **Internet Explorer** (https://support.microsoft.com/en-us/help/17442/windows-internet-explorer-delete-manage-cookies)
- **Firefox** (https://support.mozilla.org/en-US/kb/enable-and-disable-cookies-website-preferences)
- **Safari** (https://support.apple.com/guide/safari/manage-cookies-and-website-data-sfri11471/mac)

10. Use of Google Ads conversion tracking

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

en a User reaches a website via a Google advertisement, a cookie required for nversion tracking is placed on their computer. These cookies have a limited validity and

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 has clicked on the advertisement.

Each Google Ads client receives a different cookie, so they cannot be tracked through the websites of Ads clients.

The information obtained with the help of conversion tracking cookies serves the purpose of creating conversion statistics for Ads clients who opt for conversion tracking. Clients are thus informed about the number of users who clicked on their ad and were redirected to a page with a conversion tracking tag. However, they do not receive information that could identify any user.

If you do not wish to participate in conversion tracking, you can refuse it by disabling the possibility of installing 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 cookie types: **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 sending user data to Google for advertising purposes. ad_personalization controls whether the data can be used for ad personalization (e.g., remarketing). The Data Controller ensures that the appropriate consents are obtained and can be withdrawn via 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 policy are available at:
https://policies.google.com/privacy

11. Application of Google Analytics

This website uses Google Analytics, a web analytics service provided by Google, Inc. ("Google"). Google Analytics uses "cookies", which are text files placed on your computer, to help the website analyze how users use the site.

e information generated by the cookie about your use of the website will generally be ..ansmitted to and stored by Google on servers in the United States. By activating IP

anonymization on the website, Google will truncate the User's IP address within Member States of the European Union or other parties to the Agreement on the European Economic Area beforehand.

Only in exceptional cases will the full IP address be sent to a Google server in the USA and shortened there. On behalf of the operator of this website, Google will use this information for the purpose of evaluating your use of the website, compiling reports on website activity for website operators, and providing other services relating to website activity and internet usage.

The IP address transmitted by the User's browser within the scope of Google Analytics will not be associated with any other data held by Google. The User may refuse the use 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. You can also prevent Google from collecting and processing the data generated by the cookie about your use of the website (including your IP address) by downloading and installing the browser plug-in available at the following link: https://tools.google.com/dlpage/gaoptout?hl=en

12. Newsletter, DM activity based on consent

1. In accordance with Section 6 of Act XLVIII of 2008 on the basic conditions and certain restrictions of economic advertising activities, the User may give prior and explicit consent for the Service Provider to contact them with advertising offers and other mailings at the contact details provided during registration.

2. Furthermore, the Customer, keeping in mind the provisions of this policy, 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 the sending of offers free of charge, without restriction and without giving any reason. In this case, the Service Provider will delete all of 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 on the link in the message.

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

Personal Data	Purpose of Data Processing	Legal Basis
Name, e-mail address.	Identification, enabling subscription to newsletters/promotional coupons.	The data subject's consent, Article 6(1)(a). Section 6(5) of Act XLVIII of 2008 on the basic conditions and certain restrictions of economic advertising activities.
Date of subscription	Execution of a technical operation.	The data subject's consent, Article 6(1)(a).
IP address at the time of subscription	Execution of a technical operation.	

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

6. 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.

7. Duration of data processing, deadline for erasure of data: The data processing lasts until the consent is withdrawn (unsubscription, data subject's request for erasure), or until the newsletter is discontinued.

8. Identity of potential data controllers entitled to access the data, recipients of the personal data: Personal data may be processed by the data controller and its sales and marketing staff, in compliance with the above principles.

9. Description of the rights of data subjects in relation to data processing:

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

10. The data subject can initiate access to, erasure, modification, or restriction of cessing of personal data, data portability, or object to processing in the following ways:

- by post at the address 8797 Batyk, Fő utca 34,
- by e-mail at the e-mail address 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 newsletters from us.
- failure to provide the data will result in us being **unable to send you a newsletter**.
- we inform you that you can withdraw your consent at any time by clicking on unsubscribe.
- the withdrawal of consent **does not affect the lawfulness of processing based on consent before its withdrawal.**

13. Complaint handling

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

Personal Data	Purpose of Data Processing	Legal Basis
First name and surname	Identification, contact.	Article 6(1)(c). (The relevant legal obligation: Section 17/A. (7) of Act CLV of 1997 on Consumer Protection)
E-mail address	Contact.	
Phone number	Contact.	
Billing name and address	Identification, handling of quality complaints, questions and problems	

Personal Data	Purpose of Data Processing	Legal Basis
	arising in connection with the ordered products/services.	

2. Scope of data subjects: All data subjects who make a purchase on the website and make a quality complaint or file a complaint.

3. Duration of data processing, deadline for erasure of data: Copies of the record of the complaint, the transcript and the reply thereto must be kept for 3 years in accordance with Section 17/A (7) of Act CLV of 1997 on Consumer Protection.

4. Identity of potential data controllers entitled to access the data, recipients of the personal data: Personal data may be processed by the data controller and its authorised staff, in compliance with the above principles.

5. Description of the rights of data subjects in relation to data processing:

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

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

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

7. We inform you that

- the provision of personal data is based on a **legal obligation**.
- the processing of personal data is a **prerequisite** for the conclusion of the contract.
- you **are obliged** to provide the personal data so that we can handle your complaint.
- failure to provide the data will result in us being **unable to handle your complaint**.

14. RECIPIENTS WITH WHOM PERSONAL DATA IS 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/hu/privacy)
3. **The fact of data processing, the scope of the data processed:** Billing data, name, e-mail address
4. **Scope of data subjects:** All data subjects choosing to pay on the website.
5. **Purpose of data processing:** To process the online payment, confirm transactions and for fraud-monitoring (checking for abuse) to protect users.
6. **Duration of data processing, deadline for erasure of data:** Lasts until the online payment is processed.
7. **Legal basis for data processing:** Article 6(1)(b) of the GDPR. The 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 from the controller confirmation as to whether or not personal data concerning you are being processed, and, where that is the case, access to 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.

15. Data processors used

Hosting provider

1. **Activity performed by data processor:** Hosting service

2. **Name and contact details of data processor:** Rackhost Zrt. (6722 Szeged, Tisza Lajos körút 41., 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 the data processed:** 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:** To make the website/mobile application available and to operate it properly.
6. **Duration of data processing, deadline for erasure of data:** The 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 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. Legitimate interest in the proper operation of the website, protection against attacks, fraud.

Other data processors

Data Processor	Activity	Privacy Policy/Contact
Stripe Payments Europe, Ltd.	Secure processing of online payment transactions.	https://stripe.com/hu/privacy
Bithuszárok Bt. (Listamester)	Sending newsletters to subscribers.	https://listamester.hu/felhasznalasi-feltetelek.php
Kutyavilág Kft. and Animadó Kft.	Accounting. Fulfilling the accounting and tax obligations of the Data Controller.	N/A
Google (Google Gemini ice via the	Generating text content (e.g., reports) based on the data entered by the User.	Google: https://policies.google.com/privacy OpenRouter: https://openrouter.ai/privacy

Data Processor	Activity	Privacy Policy/Contact
OpenRouter platform)		
KBOSS.hu Kft. (szamlazz.hu)	Billing service. The Data Controller operates a website (hereinafter: Website) for the purpose of ordering a billing service on the www.szamlazz.hu website, during which it processes the personal data of visitors to the Website and those who register on the Website. The data of natural person users (hereinafter: Users) are considered personal data. The User can access the privacy policy on the Website by clicking on the www.szamlazz.hu/adatvedelem/ link, in which the Data Controller has summarized its data processing principles and practices.	Name: KBOSS.hu Kereskedelmi és Szolgáltató Korlátolt Felelősségű Társaság (KBOSS.hu Kft.) Registered office: 1031 Budapest, Záhony utca 7. Representative's name: Balázs Ángyán, managing director Company registration number: 01-09-303201 Tax number: 13421739-2-41 E-mail: info@szamlazz.hu Data Protection Officer: dr. Éva Istvánovics, lawyer Contact: dpo@kboss.hu

16. Social media sites

The fact of data collection, the scope of the data processed: The registered name on social media sites such as Twitter/Pinterest/Youtube/Instagram/TikTok/Linkedin, etc., 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 have "liked" the Service Provider's social media page, or have contacted the data controller via social media site.

Purpose of data collection: To share, or “like”, follow, and promote certain content elements, products, promotions of the website or the website itself on social media sites.

Duration of data processing, deadline for erasure of data, identity of potential data controllers entitled to access the data and description of the rights of data subjects in relation to data processing: The data subject can find information about the source of the data, its processing, the method and legal basis of transfer on the given social media site. The data processing takes place on the social media sites, so the duration, manner of data processing, and the possibilities for 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 the social media sites.

17. Facebook / Meta joint controllership

The Data Controller has a Facebook / Meta profile for its activities. The data processing for statistical purposes on the Facebook social media site is a joint processing of the Data Controller and Facebook Ireland Ltd. (4 Grand Canal Square, Grand Canal Harbour, D2 Dublin, Ireland). The details of the joint processing agreement are provided in the Facebook Page Insights Controller Addendum. The addendum is available at the following link: https://www.facebook.com/legal/terms/page_controller_addendum

The Data Controller will only communicate via private message on the social media site if you contact us there.

1. **Categories of data subjects**
    - any data subject who has registered on the social media site and “liked” the Data Controller’s profile page,
    - any data subject who contacts the Data Controller via private message on the social media site.
2. **Purpose of data processing**
   The purpose of the data processing is to share and promote the Data Controller’s activities and services on the Facebook social media site. 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 data through the social media sites, nor does it extract data from there.

3. **Legal basis for data processing**

The data processing is based on Article 6(1)(a) of the GDPR; the legal basis for the data processing is the data subject's consent to the processing of their personal data on the Facebook social media site.

4. **Scope of data processed**
    - the data subject's registered name,
    - the data subject's public profile picture,
    - other public data provided and shared by the data subject on the social media site.
5. **Source of personal data processed:** The source of the processed data is the data subject.
6. **Withdrawal of consent:** You may withdraw your consent to data processing at any time, and delete your post or comment. The data processing takes place via 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 does not affect the lawfulness of processing based on consent before its withdrawal.
   You can initiate access to, erasure, modification, or restriction of processing of personal data, and data portability in the following ways:

    - by post at the address 8797 Batyk, Fő utca 34,
    - by e-mail at the e-mail address 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 a message exchange occurs, then for 2 years.
8. **Transfer of personal data, recipients, and categories of recipients:** For the definition of recipient, see GDPR Article 4(9). The Data Controller will only transfer the personal data of the Data Subject to state bodies, authorities – in particular courts, prosecution offices, investigating authorities and misdemeanor authorities, the National Authority for Data Protection and Freedom of Information – in exceptional cases and on the basis of a legal obligation.
9. **Possible consequences of failure to provide data**
   If the data is not provided, the data subject cannot be informed about the Data Controller's activities and services via the Facebook social media site, nor can they send a message to the Data Controller via Facebook Messenger.

10. **Automated decision-making (including profiling):** No automated decision-making, including profiling, takes place during the data processing.
11. **Joint controller agreement with Facebook Ireland Ltd.:**

The Page Insights feature displays aggregated data that helps to understand how data subjects use the Facebook page. Facebook Ireland Limited (“Facebook Ireland”) and the Data Controller are joint controllers with respect to the processing of insights data. The Page Insights Addendum defines the responsibilities of Facebook and the Data Controller in relation to the processing of insights data. Facebook Ireland assumes primary responsibility under the GDPR for the processing of insights data and for complying with all applicable obligations under the GDPR in relation to the processing of insights data. Facebook Ireland also makes the substance 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 the insights data, identifies the controller of the page, and complies with all other applicable legal obligations. Facebook Ireland is solely responsible for the processing of personal data in connection with the Page Insights feature, except for data within the scope of the Page Insights Addendum. The Page Insights Addendum does not give 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 may not act on behalf of Facebook Ireland or provide a response when fulfilling data protection requests.

18. Customer relations and other data processing

If a question arises or the data subject has a problem while using the data controller’s services, they can contact the data controller in the ways specified on the website (phone, e-mail, social media sites, etc.).

The data controller will delete the received e-mails, messages, data provided by phone, on Meta, etc., along with the name and e-mail address of the inquirer and any other voluntarily provided personal data, no later than 2 years from the date of data provision.

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

Upon exceptional official request, or in case of a request from other bodies based on the authorization of law, the Service Provider is obliged to provide information, disclose data, transfer data, or make documents available.

In these cases, the Service Provider shall only disclose personal data to the requester – provided that the requester has specified the precise purpose and scope of the data – to the extent and in the amount that is absolutely necessary to achieve the purpose of the request.

19. Rights of the data subject

1. **The 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. **The 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. **The 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 certain grounds apply.

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

   - You contest the accuracy of the personal data, 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 which case, the restriction applies for the period until it is verified whether the legitimate grounds of the controller override your legitimate grounds.

6. **The 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. **The right to object**
   In the case of data processing based on legitimate interest or public authority, you have the right to object at any time to processing of personal data concerning you (…) for reasons relating to your particular situation, including profiling based on those provisions.

8. **Objection to 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.

20. Time limit for action

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

If necessary, this period may be extended by **2 months**. 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

The controller and the processor shall, 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, implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

a. the pseudonymisation and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
d. 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 them. For paper-based data carriers, by establishing a system for physical storage and filing; for data processed electronically, by using a central authorization management system.

The method of storing data using IT methods must be chosen so that their deletion – also ing into account any different deletion deadlines – can be carried out at the expiry 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 engaging an external organization specializing in document destruction. In the case of electronic data carriers, physical destruction must be ensured according to the rules for the disposal of electronic data carriers, and, if necessary, the data must be securely and irreversibly deleted beforehand.

The data controller takes 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):

- Store the documents in a secure, well-lockable dry room.
- If paper-based personal data is digitized, the rules applicable to digitally stored documents must be applied.
- The employee of the Service Provider performing data processing may only leave the room where data processing is taking place by locking away the data carriers entrusted to them or by locking the room.
- Personal data may only be accessed by authorized persons; third parties cannot access them.
- The building and premises of the Service Provider are equipped with fire and property protection equipment.

IT protection

- The 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 appropriate permissions can access the central server machine.
- The 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 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
sible, 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 case of mandatory data processing

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

The controller shall **document** the circumstances and results of this review, **retain 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: the Authority) upon the Authority's request.

25. Right to lodge a complaint

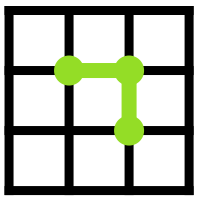
A complaint against a possible infringement by the data controller can be lodged with the National Authority for Data Protection and Freedom of Information:

Nemzeti Adatvédelmi és Információszabadság Hatóság
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

26. Final word

During the preparation of this policy, we have taken into account the following legislation:

- 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 CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (hereinafter: Infotv.);
- 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 conditions and certain restrictions of economic advertising activities (especially Section 6);
- Act XC of 2005 on Freedom of Information by Electronic Means;
- Act C of 2003 on Electronic Communications (specifically Section 155);
- Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising;
- The recommendation of the National Authority for Data Protection and Freedom of Information on the data protection requirements of prior information.



IPMFlow.com

Email: hello@ipmflow.com

Company: Trapshop Kft.

Address: H-8797 Batyk, Fő utca 34.

Informations

Home

Help Center

Contact
Cookie Policy
Privacy Policy
Terms and conditions

Payment Methods