# Privacy Policy - IPMFlow.com

Last updated: 2026.09.28. Version 4; accepted on 2026.07.07.

## Introduction

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

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

This privacy policy regulates the data processing of the following websites/mobile applications: https://ipmflow.com/ The privacy policy is available at: Ipmflow.com/adatvedelem, Ipmflow.com/privacy Amendments to the policy shall enter into force upon their publication at the above address.

## The Data Controller and Contact Details

**Name:** Trapshop Kft. **Registered office:** 8797 Batyk, Fő utca 34, Hungary **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.

## Contacting us

1. Fact of data collection, scope of processed data and purpose of data processing:

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

*In the case of an e-mail address, it does not necessarily have to contain personal data.*

1. **Scope of data subjects:** All data subjects sending a message through the contact form.
2. **Duration of data processing, deadline for data erasure:** The Data Controller processes personal data until the purpose of the data processing is achieved, but for a maximum of 2 years. If any of the conditions laid down in Article 17(1) of the GDPR apply, data processing shall last until the data subject's erasure request.
3. **Description of the data subjects' rights in relation to 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.
4. **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 to: 8797 Batyk, Fő utca 34, Hungary,

- by e-mail to: hello@ipmflow.com,
- by phone at: +36 30 220 9884.

5. **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) provided during the contact in accordance with this policy.
6. **Please be informed that:**
   - this data processing is based on your consent, or is necessary for providing a quotation.
   - you are required to provide personal data in order to contact us.
   - failure to provide the data has the consequence that you will not be able to 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", "strictly necessary cookies", "functional cookies" does not require prior consent from the 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 data erasure:**

| Type of cookie | Legal basis for data processing | Duration of data processing |
|---|---|---|
| Session cookies or other cookies strictly necessary for the website's operation | No data processing occurs through the use of this cookie. | The period ending with the closing of the relevant visitor session; thus, it remains on the computer only until the browser is closed. |
| Statistical, marketing cookies | Article 6(1)(a) GDPR | 1 day - 2 years, according to the cookie information, or data processing lasts until the withdrawal of the data subject's consent. |

1. **Description of data subjects' rights related to data processing:** Data subjects have the opportunity to delete cookies in the Tools/Settings menu of browsers, usually under the Privacy settings.
2. Most browsers used by our users allow setting which cookies should be saved and allow for (specific) cookies to be deleted again. If you restrict the saving of cookies on specific websites or do not allow third-party cookies, this may, under certain circumstances, lead to our website no longer being fully usable. You can find information on how to customize cookie settings for standard browsers here:

- Google Chrome (https://support.google.com/chrome/answer/95647?hl=hu)
- Microsoft Edge (https://support.microsoft.com/en-us/microsoft-edge/delete-cookies-in-microsoft-edge-63947406-40ac-c3b8-57b9-2a946a29ae09)
- 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 uses Google's conversion tracking service within its framework. Google conversion tracking is an analytics service provided by Google Ireland Limited (1600 Amphitheatre Parkway, Mountain View, CA 94043, USA; "Google"). When a User accesses a website through a Google ad, a cookie required for conversion 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 clicked on the ad. Every Google Ads customer receives a different cookie, so they cannot be tracked across the websites of Ads customers. The information obtained with the help of conversion tracking cookies serves the purpose of creating conversion statistics for Ads customers who opt for conversion tracking. Customers thereby learn the number of users who clicked on their ad and were redirected to a page tagged with a conversion tracking tag. However, they do not

obtain information that could 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 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 to Google for advertising purposes regarding user data. ad_personalization controls whether data can be used for personalized advertising (e.g., remarketing). The Data Controller ensures the acquisition and withdrawal of appropriate consents on its cookie banner / panel. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Further information and Google's privacy policy are available at the following page: https://policies.google.com/privacy

## Use of Google Analytics

This website uses Google Analytics, a web analytics service provided by Google Ireland Limited ("Google"). Google Analytics uses so-called "cookies", text files stored on your computer, to help analyze how the User uses the visited website. The information generated by cookies regarding the website used by the User is usually transmitted to a Google server in the USA and stored there. With IP anonymization activated on the website, Google will shorten the User's IP address beforehand within Member States of the European Union or in other contracting states to the Agreement on the European Economic Area. Only in exceptional cases is the full IP address 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 the User's use of the website, compile reports on website activity for the website operator, and provide other services related to website activity and internet usage. The IP address transmitted by the User's browser as part of Google Analytics will not be merged with other Google data. The User can prevent the storage of cookies by setting their browser software accordingly; however, please note that if you do this, you may not be able to use all the functions of this website to their full extent. Furthermore, you can prevent Google's collection and processing of data generated by the cookie and related to the User's use of the website (including the IP address) by downloading and installing the browser plugin available at the following link: https://tools.google.com/dlpage/gaoptout?hl=en

## Newsletter, Direct Marketing Activity Based on Consent

1. Pursuant to Section 6 of Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities, unless otherwise provided by a specific act, an advertisement may only be communicated to a natural person – the User – as the recipient of the advertisement through direct contact (hereinafter: direct marketing), in particular by electronic mail or equivalent other means of individual communication, if the recipient of the advertisement has expressly and unambiguously consented thereto in advance.
2. Furthermore, keeping in mind the provisions of this policy, the User may consent to the Service Provider processing their personal data necessary for sending advertising offers.
3. The Service Provider does not send unsolicited commercial messages, and the User may unsubscribe from receiving offers free of charge, without limitation and without justification. In this case, the Service Provider will delete all personal data necessary for sending commercial 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.
4. **Fact of data collection, scope of processed data and purpose of data processing:**

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

1. The sending of newsletters is carried out in compliance with the provisions of Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities.
2. **Scope of data subjects:** All data subjects subscribing to the newsletter.
3. **Purpose of data processing:** sending electronic messages containing advertising (e-mail, sms, push messages) to the data subject, providing information on current information, products, promotions, new functions, etc.
4. **Duration of data processing, deadline for data erasure:** Data processing lasts until the withdrawal of consent

(unsubscribing, the data subject's erasure request) or until the discontinuation of the newsletter.

5. **Description of the data subjects' rights in relation to 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, erasure, modification, or restriction of processing of personal data, and data portability in the following ways:**
   - by post to: 8797 Batyk, Fő utca 34, Hungary,
   - by e-mail to: hello@ipmflow.com,
   - by phone at: +36 30 220 9884.
7. The data subject may unsubscribe from the newsletter at any time, free of charge.
8. **Please be informed that:**
   - data processing is based on your consent.
   - you are required to provide personal data if you wish to receive a newsletter from us.
   - failure to provide data will result in us not being able 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 shall not affect the lawfulness of processing based on consent before its withdrawal.

## Data Processors Used

### Hosting Provider

1. **Activity performed by Data Processor:** Hosting service
2. **Name and contact details of the Data Processor:** Data of the IT systems (hosting providers) servicing the service:

**Rackhost Zrt.** Activity: hosting service for ipmflow.com Registered office: 6722 Szeged, Tisza Lajos körút 41, Hungary. E-mail: info@rackhost.hu Phone: +36 1 445 1200 Website: www.rackhost.hu

**Vercel Inc.** Activity: Hosting the installable, offline-capable PWA associated with the software Registered office: 340 S Lemon Ave #4133, Walnut, CA 91789, USA Website: www.vercel.com

1. **Fact of data processing, scope of processed data:** All personal data provided by the data subject.
2. **Scope of data subjects:** All data subjects using the website/mobile application.
3. **Purpose of data processing:** Making the website/mobile application available, ensuring its proper operation.
4. **Duration of data processing, deadline for data erasure:** The data processing lasts until the termination of the agreement between the Data Controller and the hosting provider, or until the data subject's erasure request directed to the hosting provider.
5. **Legal basis for data processing:** Article 6(1)(c) and (f), and Section 13/A (3) of Act CVIII of 2001 on certain issues of electronic commerce services and information society services. Legitimate interest includes the proper operation of the website and protection against attacks and fraud.

### Other Data Processors (if any)

**1. Hosting and Infrastructure Providers**

| Name of Data Processor | Registered office / Contact | Description of activity | Privacy Policy |
|---|---|---|---|
| Rackhost Zrt. | 6722 Szeged, Tisza Lajos körút 41. E-mail: info@rackhost.hu Phone: +36 1 445 1200 | Hosting service, hosting of the main website (ipmflow.com) and static content. | https://www.rackhost.hu/privacy-policy |

**2. Analytics, Marketing and Artificial Intelligence (AI)**

| Name of Data Processor | Registered office / Contact | Description of activity | Privacy Policy |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Google Ireland Limited | Gordon House, Barrow Street, Dublin 4, Ireland | Google Analytics 4: Visitor statistics, web analytics. Google Ads: Ad serving, conversion tracking, remarketing. Google Workspace: Business email, document storage. | https://policies.google.com/privacy |

**3. IT Security and External Service Providers** To maintain the security of the Website, ensure the continuous availability of the service, and to prevent malicious attacks (e.g., DDoS, hacking attempts, data theft), the Data Controller uses specialized external partners. Out of technical necessity, these services may record visitors' IP addresses, browsing data (User-Agent), and request metadata. The services may place security cookies on the user's device that are essential for operation, which do not serve marketing purposes. **Legal basis for data processing:** The legitimate interest of the Data Controller (Article 6(1)(f) GDPR), which is attached 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 service providers after the threat has been averted or following a specified technical period (usually 30 days).

| Name of Data Processor | Registered office / 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. Processed data: IP address, system configuration information, traffic data, necessary cookies. | Privacy Policy. The company participates in the EU-US Data Privacy Framework. |
| Defiant, Inc. (Wordfence) | 800 5th Ave Ste 4100, Seattle, WA 98104, USA | Activity: Endpoint-based website protection, intrusion detection system, malicious code filtering. Processed data: IP address, login attempt data, log of blocked requests, necessary cookies. | Privacy Policy. The data transfer is based on the Standard Contractual Clauses (SCC) approved by the European Commission. |

## Social Media Platforms

The Data Controller is also present on social media platforms in order to present its services and maintain contact with prospects and clients. **Scope of processed data:** The data publicly available on the data subject's social media profile, in particular: – name (username) – public profile picture – content published by the data subject, and interactions related to the Data Controller's page (e.g., comments, messages). **Scope of data subjects:** Natural persons who follow the Data Controller's social media page, interact with it, or send messages through it. **Purpose of data processing:** – presenting the Data Controller's activities and services, – marketing and communication on social media platforms, – maintaining contact with prospects and clients. **Legal basis for data processing:** The voluntary consent of the data subject to the processing of their personal data on social networking sites. **Duration of data processing:** The data processing lasts until the data subject's interaction exists, or until the content published by the data subject is deleted. The Data Controller retains messages and communication for a maximum of 2 years. **Further data controllers:** Social media platforms process user data as independent data controllers according to their own privacy policies.

## Facebook / Meta Joint Controllership

The Data Controller has a Facebook / Meta profile related to its activities. The data processing for statistical purposes realized on the Facebook social network constitutes joint controllership between the Data Controller and Facebook Ireland Ltd. (4 Grand Canal Square, Grand Canal Harbour, D2 Dublin Ireland). Detailed information on the details of the joint controllership agreement is provided by the Controller Addendum for Facebook Page Insights. 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 network if you contact us there. **1. Categories of data subjects**

- data subjects who registered on the social network and "liked" the Data Controller's profile page,
- data subjects who contact the Data Controller in a private message on the social network. **2. Purpose of data processing** The purpose of data processing is to share and promote the activities and services of the Data Controller on the Facebook social network. The Data Controller may use the data provided by the data subject in a private message to respond to the message; otherwise, the Data Controller does not collect data through social networks and does not 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 is the data subject's consent to the processing of their personal data on the Facebook social network. **4. Scope of processed data**
- registered name of the data subject,
- public profile picture of the data subject,

- other public data provided and shared by the data subject on the social network. **5. Source of processed personal data:** 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 you can delete your post or comment. Data processing takes place through social networking sites, which are operated by third parties. 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, erasure, modification, or restriction of processing of personal data, and data portability in the following ways:
- by post to: 8797 Batyk, Fő utca 34, Hungary,
- by e-mail to: hello@ipmflow.com,
- by phone at: +36 30 220 9884. **7. Duration of data processing**
- until the withdrawal of the data subject's consent,
- if an exchange of messages takes place, then 2 years. **8. Transfer and recipients of personal data, or categories of recipients:** For the definition of recipient see: Article 4(9) GDPR. The Data Controller only transfers the Data Subject's personal data to state bodies, authorities – in particular courts, prosecutors, investigating authorities, and the minor offence authority, 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 through the Facebook social network, or send a message to the Data Controller via Facebook Messenger. **10. Automated decision-making (including profiling):** During data processing, no automated decision-making, including profiling, takes place. **11. Joint Controller Agreement with Facebook Ireland Ltd.:** The Page Insights function 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 concerning the processing of insights data. The Page Insights Addendum defines the responsibilities of Facebook and the Data Controller concerning the processing of insights data. Facebook Ireland agrees to take primary responsibility under the GDPR for the processing of insights data and to comply with all applicable obligations under the GDPR concerning the processing of insights 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 insights data, identifies the controller of the page, and complies with any other applicable 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 may not act or respond on behalf of Facebook Ireland when fulfilling data protection requests.

## Customer Relations and Other Data Processing

Should any questions or problems arise while using the Data Controller's services, the data subject may contact the Data Controller using the methods specified on the website (phone, e-mail, social media pages, etc.). The Data Controller deletes received e-mails, messages, data provided over the phone, on Meta, etc., together with the inquirer's name and e-mail address, as well as any other voluntarily provided personal data, at the latest 2 years after the data was provided. We provide information on data processing not listed in this policy at the time the data is collected. Upon an exceptional official request from an authority, or in the case of a request from other bodies authorized by law, the Service Provider is obliged to provide information, disclose data, transfer data, or make documents available. In these cases, the Service Provider will disclose personal data to the requester – provided that the exact purpose and the scope of data have been indicated – only to the extent and in a measure that is strictly necessary for fulfilling the purpose of the request.

## Rights of the Data Subjects

**1. Right of access** You have the right to obtain confirmation from the controller as to whether or not personal data concerning you are being processed, and, where that is the case, access to the personal data and the information listed in the regulation. **2. Right to rectification** You have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning you. Taking into account the purposes of the processing, you have the right to have incomplete personal data completed, including by means of providing a supplementary statement. **3. Right to erasure** You have the right to obtain from the controller the erasure of personal data concerning you without undue delay and the controller shall have the obligation to erase personal data 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 you have requested the erasure by such controllers of any links to, or copy or replication of, those personal data. **5. Right to restriction of processing** You have the right to obtain from the controller restriction of processing where one of the following applies:

- the accuracy of the personal data is contested by you, for a period enabling the controller to verify the accuracy of the personal data;
- the processing is unlawful and you oppose the erasure of the personal data and request the restriction of their use instead;
- the controller no longer needs the personal data for the purposes of the processing, but they are required by you for the establishment, exercise or defence of legal claims;
- you have objected to processing; in this case, the restriction is pending the verification whether the legitimate grounds of the controller override yours. **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 interest or a task carried out in the exercise of official authority 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 previous 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.

## Time Limit for Action

The controller shall provide you with information on action taken on a request under the above rights 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 such a way that unauthorized persons cannot access them. In the case of paper-based data carriers, by establishing the order of physical storage and archiving, and in the case of data processed in electronic form, by applying a central access management system.

The method of storing data by IT means must be chosen so that their deletion – taking into account any possibly different deletion deadlines – can be carried out at the expiry of the data deletion deadline, or if it is necessary for other reasons. Deletion must be irreversible. Paper-based data carriers must be stripped of personal data using a document shredder or by employing an external organization specialized in document destruction. In the case of electronic data carriers, physical destruction must be ensured according to the rules for scrapping electronic data carriers, and, if necessary, the data must be securely and irreversibly deleted beforehand. The Data Controller takes the following specific data security measures: In order to ensure the security of personal data processed on paper, the Service Provider applies the following measures (physical protection):

- Documents are placed in a secure, well-lockable dry room.
- If personal data processed on paper are digitized, the rules applicable to 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 by locking away the data carriers entrusted to them or by locking the given room.
- Personal data may only be accessed by authorized persons; third parties cannot 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 used by the Service Provider containing personal data is equipped with virus protection.
- In order to ensure the security of digitally stored data, the Service Provider applies data backups and archiving.
- Only designated persons with appropriate 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 a 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 it, or by the processor acting on its behalf or according to its instructions, is necessary for the realization of the purpose of data processing. The circumstances and results of this review shall be documented by the controller; this documentation shall be retained for ten years following the review and made available to the National Authority for Data Protection and Freedom of Information (hereinafter: Authority) upon its request.

## Right to Lodge a Complaint

In case of possible infringement by the Data Controller, a complaint can be lodged 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

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

- REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR);
- Act CVIII of 2001 on certain issues of electronic commerce services and information society services (especially Section 13/A);
- Act XLVII of 2008 on the Prohibition of Unfair Commercial Practices against Consumers;
- Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities (especially Section 6);
- Act C of 2003 on Electronic Communications (specifically Section 155);
- Opinion 16/2011 on 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 of prior information.