# Privacy Policy

## INTRODUCTION

Walking Sage Kft. (2030 Érd, Festő u. 86/1., Tax Number: 24247757-2-13, Company Registration Number: 13-09-161726), (hereinafter referred to as: Service Provider, Data Controller) adopts the following policy.

The following Privacy Policy is provided 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 – GDPR).

This Privacy Policy governs the data processing activities of the following website:

https://zulupack.shop

This Privacy Policy is available at:
https://zulupack.shop/shop_help.php?tab=privacy_policy

Changes to this Privacy Policy shall become effective upon publication on the above-mentioned website.

### DATA CONTROLLER AND CONTACT DETAILS

**Name:** Walking Sage Kft.
**Registered Office:** 2030 Érd, Festő u. 86/1., Hungary
**E-mail:** info@walkingsage.hu
**Telephone:** +36-70-507-4440

## Definitions

**1. "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 one or more factors such as a name, identification number, location data, online identifier, or factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

**2. "Data Processing"**: any operation or set of operations performed on personal data or data files, whether by automated means or not, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

**3. "Data Controller"**: any 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.

**4. "Data Processor"**: any natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

**5. "Recipient"**: any natural or legal person, public authority, agency, or other body to whom personal data are disclosed, regardless of whether they are a third party or not. Public authorities which may receive personal data within the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of such data by those public authorities shall comply with the applicable data protection rules according to the purposes of the processing.

**6. "Consent of the Data Subject"**: any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to them.

**7. "Data Breach"**: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed

## The principles of managing personal data

Personal data:

1. must be processed lawfully, fairly, and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency");
2. must be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) shall not be considered incompatible with the original purposes ("purpose limitation");
3. must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed ("data minimization");
4. must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data are erased or rectified without delay, having regard to the purposes for which they are processed ("accuracy");
5. must be 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 they are 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 the implementation of appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ("storage limitation");
6. must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures ("integrity and confidentiality").

The Data Controller shall be responsible for compliance with the above principles and must be able to demonstrate such compliance ("accountability").

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

## Data management in connection with the operation/use of the webshop

### 1. Fact of Data Collection, Scope of Managed Data, and Purpose of Data Processing

Personal Data Purpose of Data Processing Legal Basis

Article 6(1)(b) GDPR and Section

| | | |
|---|---|---|
| Username | Identification enabling registration. | 13/A(3) of the Hungarian Act on Electronic Commerce Services. |
| Password | Used for secure access to the user account. | |
| First name and surname | Necessary for purchasing and issuing a proper invoice, as well as for contacting the User. | |
| E-mail address | Necessary for communication. | |
| Telephone number | Necessary for communication and for more efficient coordination regarding billing or shipping issues. | |
| Billing name and address | Issuance of a proper invoice, conclusion, establishment, modification, performance of the contract, invoicing of resulting charges, and enforcement of related claims. | Article 6(1)(c) GDPR and Section 169(2) of Act C of 2000 on Accounting. |
| Delivery name and address | To enable home delivery. | Article 6(1)(b) GDPR and Section 13/A(3) of the Hungarian Act on Electronic Commerce Services. |
| Date of purchase/registration | Ensuring technical operation. | |
| IP address at the time of purchase/registration | Ensuring technical operation. | |

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

### 2. Scope of Data Subjects

All persons registering or purchasing on the website.

### 3. Duration of Data Processing, Deadline for Data Deletion

If any of the conditions set out in Article 17(1) GDPR are met, the data subject may request the deletion of their personal data. The Data Controller shall notify the data subject electronically of the deletion of the personal data provided by them pursuant to Article 19 GDPR. If the deletion request also concerns the e-mail address provided by the data subject, the Data Controller shall delete the e-mail address following notification.

Accounting documents must be retained for eight years pursuant to Section 169(2) of Act C of 2000 on Accounting.

Accounting records (including general ledger accounts, analytical and accounting records) directly and indirectly supporting the accounts must be retained in a readable format and retrievable by reference to the accounting records for at least eight years.

### 4. Persons Authorized to Process the Data and Access the Personal Data

Personal data may be processed by the sales and marketing staff of the Data Controller in compliance with the above principles.

### 5. Rights of Data Subjects

The data subject may request from the Data Controller:

- access to personal data concerning them;
- rectification, deletion, or restriction of processing of personal data;
- the right to data portability;
- withdrawal of consent at any time.

### 6. Methods for Initiating Access, Deletion, Modification, Restriction of Processing, Data Portability, and Objection to Data Processing

By post:
2030 Érd, Festő u. 86., Hungary

By e-mail:
info@walkingsage.hu

By telephone:
+36-70-507-4440

### 7. Legal Basis for Data Processing

7.1.

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

7.2.

Pursuant to Section 13/A(3) of Act CVIII of 2001 on Certain Issues of Electronic Commerce Services and Information Society Services (hereinafter: Electronic Commerce Act):

For the purpose of providing the service, the service provider may process those personal data that are technically indispensable for the provision of the service. The service provider shall, where other conditions are equal, choose and in all cases operate the tools used in providing information society services in such a way that personal data are processed only if this is strictly necessary for the provision of the service and only to the extent and for the duration necessary.

7.3.

Article 6(1)(c) GDPR in relation to invoicing obligations under accounting legislation.

7.4.

In the case of claims arising from the contract, Section 6:21 of Act V of 2013 on the Civil Code applies with a limitation period of five years.

**Section 6:22 [Limitation Period]**

1. Unless otherwise provided by law, claims shall become time-barred after five years.
2. The limitation period begins when the claim becomes due.
3. An agreement modifying the limitation period must be made in writing.
4. Agreements excluding limitation periods shall be null and void.

### 8. Please Note

- Data processing is necessary for the performance of the contract and for providing a quotation.
- Providing personal data is necessary in order for us to process your order.
- Failure to provide the required data will result in the inability to process your order.

## Newsletter, DM activity

1. Pursuant to Section 6 of Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities, the Customer may give prior consent to the Service Provider to send advertising and other communications to the contact details provided during registration.

2. Furthermore, the Customer may consent to the Service Provider processing their personal data for the purpose of sending advertising messages, taking into account the provisions of this Privacy Policy.

3. The Service Provider does not send unsolicited advertising, and the Customer may unsubscribe from advertising messages at any time, free of charge and without providing any reason. In such a case, the Service Provider shall delete all personal data necessary for sending the advertising messages from its records and shall cease sending further advertising offers. The Customer may unsubscribe from advertisements by clicking the unsubscribe link contained in the message.

4. Fact of Data Collection, Scope of Managed Data, and Purpose of Data Processing

| Personal Data | Purpose of Data Processing | Legal Basis |
|---|---|---|
| Name, e-mail address | Identification, subscription to the newsletter. | Consent of the data subject, Article 6(1)(a) GDPR, and Section 6(5) of Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities. |
| Date of subscription | Ensuring technical operation. | |
| IP address at the time of subscription | Ensuring technical operation. | |

5. Scope of Data Subjects

All data subjects subscribing to the newsletter.

6. Purpose of Data Collection

Sending electronic advertising messages (e-mail, SMS, push notifications) to the Customer containing information about current products, discounts, new features, and similar promotional content.

7. Duration of Data Processing and Deadline for Data Deletion

Until the withdrawal of consent, i.e. until unsubscribing from the newsletter.

8. Persons Authorized to Process the Data and Access the Personal Data

Personal data may be processed by the sales and marketing staff of the Data Controller in compliance with the above principles.

9. Rights of Data Subjects

The data subject may request from the Data Controller:

- access to personal data concerning them;
- rectification, deletion, or restriction of processing of personal data;
- objection to the processing of such personal data;
- the right to data portability;
- withdrawal of consent at any time.

10. Methods for Initiating Access, Deletion, Modification, Restriction of Processing, Data Portability, and Objection to Data Processing

By post:
2030 Érd, Festő u. 86., Hungary

By e-mail:
info@walkingsage.hu

By telephone:
+36-70-507-4440

11. Unsubscribing from the Newsletter

Users may unsubscribe from the newsletter at any time, free of charge.

12. Please Note

- Data processing is based on your consent.
- You are required to provide personal data so that we can respond to your message.
- Failure to provide the required data will result in the inability to process your request.
- Please note that you may withdraw your consent at any time by clicking the "Unsubscribe" link.
- Withdrawal of consent shall not affect the lawfulness of data processing carried out on the basis of consent prior to its withdrawal.

## Complaint handling

### 1. Fact of Data Collection, Scope of Managed Data, and Purpose of Data Processing

| Personal Data | Purpose of Data Processing | Legal Basis |
|---|---|---|
| First name and surname | Identification and contact. | Article 6(1)(c) GDPR and Section 17/A(7) of Act CLV of 1997 on Consumer Protection. |
| E-mail address | Maintaining contact. | |
| Telephone number | Maintaining contact. | |
| Billing name and address | Identification and handling of quality complaints, issues, and problems related to the ordered service. | |

### 2. Scope of Data Subjects

All persons purchasing on the website and submitting a legitimate complaint regarding quality.

### 3. Duration of Data Processing and Deadline for Data Deletion

Copies of the complaint record, report, and response thereto shall be retained for five years pursuant to Section 17/A(7) of Act CLV of 1997 on Consumer Protection.

### 4. Persons Authorized to Process the Data and Access the Personal Data

Personal data may be processed by the sales and marketing staff of the Data Controller in compliance with the above principles.

### 5. Rights of Data Subjects

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

### 6. Methods for Initiating Access, Deletion, Modification, Restriction of Processing, and Data Portability

- By post: 2030 Érd, Festő u. 86., Hungary
- By e-mail: info@walkingsage.hu
- By telephone: +36-70-507-4440

### 7. Please Note

- The provision of personal data is based on a legal obligation.
- The processing of personal data is a prerequisite for concluding a contract.
- You are required to provide personal data in order for us to process your complaint.
- Failure to provide the required data will result in the inability to process your complaint.

## Use of cookies

1. Webshop-specific cookies include so-called "password-protected session cookies," "shopping cart cookies," "security cookies," "necessary cookies," "functional cookies," and "cookies responsible for website statistics," which do not require the prior consent of users.

2. Fact of data processing and scope of processed data: unique identification number, timestamps, and data.

3. Scope of data subjects: all persons visiting the website.

4. Purpose of data processing: identification of users, registration of the "shopping cart," and tracking of visitors.

5. Duration of Data Processing and Deadline for Data Deletion

| Type of Cookie | Legal Basis for Data Processing | Duration of Data Processing | Processed Data |
|---|---|---|---|
| Session cookies | Pursuant to Section 13/A(3) of Act CVIII of 2001 on Certain Issues of Electronic Commerce Services and Information Society Services | Until the end of the relevant visitor session | connect.sid |
| Persistent or stored cookies | Pursuant to Section 13/A(3) of Act CVIII of 2001 on Certain Issues of Electronic Commerce Services and Information Society Services | Until deleted by the data subject | |
| Statistical cookies | Pursuant to Section 13/A(3) of Act CVIII of 2001 on Certain Issues of Electronic Commerce Services and Information Society Services | 1 month – 2 years | |

6. Potential Data Controllers Authorized to Access the Data

The Service Provider does not process personal data through the use of cookies.

7. Information on the Rights of Data Subjects in Relation to Data Processing

Users may delete cookies through the "Tools/Settings" menu of their browser, generally under the "Privacy" settings.

8. Legal Basis for Data Processing

Consent is not required if the sole purpose of the use of cookies is to carry out the transmission of communications over an electronic communications network or to provide an information society service explicitly requested by the subscriber or user.

9. Cookie Settings in Browsers

Most browsers used by our users allow users to determine which cookies may be stored and to delete specific cookies again. Restricting or disabling third-party cookies on certain websites may result in the website not being fully usable.

Information on adjusting cookie settings in standard browsers can be found here:

- Google Chrome: https://support.google.com/chrome/answer/95647?hl=en
- Edge / Internet Explorer: https://support.microsoft.com/en-us/windows/delete-and-manage-cookies-168dab11-0753-043d-7c16-ede5947fc64d
- Firefox: https://support.mozilla.org/en-US/kb/clear-cookies-and-site-data-firefox
- Safari: https://support.apple.com/guide/safari/manage-cookies-sfri11471/mac

## USING GOOGLE ADS CONVERSION TRACKING

1. The Data Controller uses the online advertising program "Google Ads" and, within its framework, utilizes Google's conversion tracking service. Google Conversion Tracking is an analytics service provided by Google (1600 Amphitheatre Parkway, Mountain View, CA 94043, USA).
2. When a User accesses a website via a Google advertisement, a conversion tracking cookie is placed on the User's computer. These cookies have a limited validity period and do not contain personal data, therefore the User cannot be personally identified through them.
3. When the User visits certain pages of the website and the cookie has not yet expired, Google and the Data Controller may recognize that the User clicked on the advertisement.
4. Each Google Ads customer receives a different cookie, therefore they cannot be tracked across the websites of other Google Ads

customers.

5. The information obtained through conversion tracking cookies is used to compile conversion statistics for customers using Google Ads conversion tracking. Customers are informed about the number of users who clicked on their advertisement and were redirected to a page containing a conversion tracking tag. However, they do not receive any information that could personally identify users.
6. If you do not wish to participate in conversion tracking, you may disable it by blocking the installation of cookies in your browser settings. In this case, you will not be included in conversion tracking statistics.
7. Further information and Google's Privacy Policy are available at:
   Google Privacy Policy

## USE OF GOOGLE ANALYTICS

1. This website uses Google Analytics, a web analytics service provided by Google ("Google"). Google Analytics uses so-called "cookies," which are text files stored on the User's computer to help analyze how Users use the website.
2. The information generated by the cookies regarding the User's use of the website is generally transmitted to and stored on a Google server in the United States. If IP anonymization is activated on the website, Google will truncate the User's IP address within Member States of the European Union or in other states party to the Agreement on the European Economic Area before transmission.
3. Only in exceptional cases will the full IP address be transmitted to a Google server in the USA and truncated there. On behalf of the operator of this website, Google will use this information to evaluate the User's use of the website, compile reports on website activity for the website operator, and provide additional services related to website and internet usage.
4. Within the framework of Google Analytics, the IP address transmitted by the User's browser will not be merged with other Google data. The User may prevent the storage of cookies by selecting the appropriate settings in their browser; however, please note that in this case not all functions of the website may be fully available. Furthermore, the User may prevent Google from collecting and processing data generated by cookies related to their use of the website (including their IP address) by downloading and installing the browser plugin available at the following link:
   Google Analytics Opt-out Browser Add-on

## Data processors (who manages data on behalf of the data controller)

The Data Controller places great emphasis on using only data processors that provide sufficient guarantees for implementing data processing in compliance with the requirements of the GDPR and ensuring the application of appropriate technical and organizational measures to protect the rights of data subjects.

The Data Processor, and any person acting under the authority of the Data Controller or the Data Processor who has access to personal data, shall process the personal data covered by these rules only in accordance with the instructions of the Data Controller.

The Data Controller is responsible for the lawfulness of data processing. The Data Processor shall only be liable for damages caused by data processing if it has failed to comply with obligations specifically imposed on data processors by the GDPR or if it has ignored or acted contrary to the lawful instructions of the Data Controller.

The Data Processor shall not make substantive decisions regarding the processing of data.

The Data Controller may use a hosting provider for ensuring the IT background infrastructure and a courier service for the delivery of ordered products as Data Processors.

### Specific Data Processors

| Data Processing Activity Name, Address, Contact Details | |
|---|---|
| Hosting Provider | UNAS Online Kft.<br>9400 Sopron, Kőszegi út 14., Hungary<br>E-mail: unas@unas.hu<br>Telephone: +36-99/200-200 |
| Data Processor Used in Data Management | Számlázz.hu<br>Company: KBOSS.hu Kft.<br>E-mail: info@szamlazz.hu<br>Telephone: +36 30 35 44 789 |

## Transfer of data to third parties

A "Third Party" means any natural or legal person, public authority, agency, or other body other than the data subject, the Data Controller, the Data Processor, or persons who, under the direct authority of the Data Controller or Data Processor, are authorized to process personal data.

Third-party Data Controllers process personal data in their own name and in accordance with their own privacy policies.

### Third-Party Data Controllers

| Data Processing Activity Name, Address, Contact Details | |
|---|---|
| Transport / Delivery Services | FoxPost Zrt.<br>3200 Gyöngyös, Batsányi János utca 9., Hungary<br>Telephone: +36-1-999-0369<br>Customer service address: 1097 Budapest, Táblás utca 36-38., Building D<br>E-mail: info@foxpost.hu |
| | GLS General Logistics Systems Hungary Parcel-Logistics Kft.<br>2351 Alsónémedi, Európa u. 2., Hungary<br>E-mail: info@gls-hungary.com<br>Telephone: +36-29-88-66-94 |
| Online Payment | SaltPay<br>1072 Budapest, Rákóczi út 42., EMKE Office Building, 2nd Floor, Hungary<br>E-mail: ugyfelszolgalat@saltpay.co<br>Telephone: +36-1-793-6776 |

## SOCIAL WEBSITES

1. Fact of data collection and scope of managed data: the name and publicly available profile picture of the Customer registered on Meta / X (formerly Twitter) / Pinterest / YouTube / Instagram and similar social networking platforms.
2. Scope of data subjects: all persons registered on Meta/X/Pinterest/YouTube/Instagram and similar social networking sites who "like" the Service Provider's social media page or contact the Data Controller through a social networking platform.
3. Purpose of data collection: sharing or "liking" specific content elements, products, promotions of the website, or the website itself on social networking platforms.
4. Duration of data processing, deadline for deletion of data, identity of possible Data Controllers entitled to access the data, and information regarding the rights of data subjects: information regarding the source of the data, the processing of the data, the method of transfer, and the legal basis for the data processing can be found on the relevant social networking platform. Data processing takes place on social networking sites; therefore, the duration of data processing and the options for deleting or modifying data are governed by the rules of the respective social networking platform.
5. Legal basis for data processing: the voluntary consent of the Customer for the processing of personal data on social networking platforms.

## CUSTOMER SERVICE AND OTHER DATA MANAGEMENT

1. If you have any questions or issues regarding the use of our data processing services, you may contact the Data Controller through the contact methods provided on the website (telephone, e-mail, social networking platforms, etc.).
2. The Data Controller shall delete all incoming e-mails, messages, telephone messages, or communications received through social networking platforms, etc., containing the Customer's name, e-mail address, or other personal data provided, after 2 years from the commencement of the service.
3. Data processing activities not specifically listed in this Privacy Policy shall be governed by the information provided at the time of data collection.
4. The Service Provider is obliged to provide information, data, documents, and records to the competent authorities in response to exceptional requests or requests from other bodies authorized by law.
5. In such cases, the Service Provider shall provide personal data to the requesting party only to the extent and in the scope necessary to fulfill the purpose of the request, provided that the exact purpose and scope of the requested data have been specified.

## CUSTOMER RIGHTS

### 1. Right of Access

You have the right to obtain confirmation from the Data Controller as to whether or not your personal data are being processed, and where such processing is taking place, you have the right to access your personal data and the information specified in the Regulation.

### 2. Right to Rectification

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

### 3. Right to Erasure

You have the right to request that the Data Controller erase personal data concerning you without undue delay, and the Data Controller shall be obliged to erase such personal data without undue delay under certain conditions.

### 4. Right to be Forgotten

Where the Data Controller has made the personal data public and is obliged to erase them, the Data Controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform other data controllers processing the personal data that you have requested the erasure of any links to, or copies or replications of, those personal data.

### 5. Right to Restriction of Processing

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

- you contest the accuracy of the personal data, for a period enabling the Data 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 Data Controller no longer needs the personal data for the purposes of processing, but you require them for the establishment, exercise, or defense of legal claims;
- you have objected to the processing; in this case, the restriction shall apply for the period pending the verification whether the legitimate grounds of the Data Controller override your legitimate grounds.

### 6. Right to Data Portability

You have the right to receive the personal data concerning you, which you have provided to a Data Controller, in a structured, commonly used, and machine-readable format, and you have the right to transmit those data to another Data Controller without hindrance from the Data Controller to whom the personal data were provided.

### 7. Right to Object

You have the right to object, on grounds relating to your particular situation, at any time to the processing of your personal data, including profiling based on those provisions.

### 8. Right to Object to Direct Marketing

Where personal data are processed for direct marketing purposes, you have the right to object at any time to the processing of personal data concerning you for such marketing purposes, including profiling insofar as it is related to direct marketing. If you object to the processing of personal data for direct marketing purposes, your 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 the performance of, a contract between you and the Data Controller;
- is authorized by European Union or Member State law applicable to the Data Controller, which also lays down suitable measures to safeguard your rights, freedoms, and legitimate interests;
- is based on your explicit consent.

## Deadline for measures

The Data Controller shall inform you without undue delay, and in any event within one month of receipt of the request, of any measures taken in response to these requests.

Where necessary, this period may be extended by a further two months. The Data Controller shall inform you of any such extension within one month of receipt of the request, together with the reasons for the delay.

If the Data Controller does not take action on your request, it 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 of your right to lodge a complaint with a supervisory authority and seek a judicial remedy.

## DATA MANAGEMENT SECURITY

The Data Controller and the Data Processor shall implement appropriate technical and organizational measures, taking into account the state of the art, the costs of implementation, the nature, scope, context, and purposes of the data processing, as well as the varying likelihood and severity of risks to the rights and freedoms of natural persons, in order to ensure a level of data security appropriate to the risk, including, where appropriate:

1. the pseudonymization and encryption of personal data;
2. ensuring the ongoing confidentiality, integrity, availability, and resilience of processing systems and services used for processing personal data;
3. the ability to restore access to personal data and the availability of data in a timely manner in the event of a physical or technical incident;
4. a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of data processing.
5. Processed data must be stored in a manner that prevents unauthorized access. In the case of paper-based data carriers, this shall be ensured by establishing rules for physical storage, archiving, and handling; in the case of electronically processed data, by implementing a centralized access authorization system.
6. The method of data storage using IT systems shall be selected in such a way that deletion may be carried out after the deletion deadline expires or when otherwise required, subject to any different statutory deletion periods. Deletion must be irreversible.
7. Paper-based data carriers shall be destroyed using a document shredder or by an external organization specializing in document destruction. In the case of electronic data carriers, physical destruction must be carried out in accordance with the rules governing the disposal of electronic media, including the prior secure and irreversible deletion of the data where necessary.
8. The Data Controller shall implement the following specific data security measures:

### Protection of Paper-Based Personal Data

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

1. Documents shall be stored in a secure, lockable, and dry room.
2. The buildings and premises of the Service Provider are equipped with fire protection and property protection systems.
3. Personal data may only be accessed by authorized persons and shall not be accessible to third parties.
4. Employees of the Service Provider may leave the room where data processing takes place during the course of their work only after locking the entrusted data carriers or securing the room itself.
5. Where digitization of paper-based personal data takes place, the rules applicable to digitally stored documents shall apply.

### IT Protection

1. Computers and mobile devices (and other data carriers) used for data processing are the property of the Service Provider.
2. The computer systems used by the Service Provider containing personal data are protected against viruses.
3. The Service Provider uses backups and archives to ensure the security of digitally stored data.
4. Access to the central server machine is granted only to authorized persons.
5. Access to data stored on computers is possible only through the use of a username and password.

## INFORMATION FOR THE DATA BREACHED PERSON ABOUT THE DATA BREACHE

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

The information provided to the data subject shall be clear and easy to understand and shall include the nature of the data breach, as well as the name and contact details of the Data Protection Officer or another contact person able to provide further information. The likely consequences of the personal data breach shall also be described, together with the measures taken or proposed to be taken by the Data Controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

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

- the Data Controller has implemented appropriate technical and organizational protection measures and those measures were applied to the data affected by the data breach, in particular measures such as encryption that render the personal data unintelligible to any person who is not authorized to access it;

- following the data breach, the Data Controller has taken subsequent measures ensuring that the high risk to the rights and freedoms of the data subject is no longer likely to materialize;
- informing the data subject would involve disproportionate effort. In such cases, a public communication or similar measure shall be used whereby the data subjects are informed in an equally effective manner.

If the Data Controller has not already communicated the data breach to the data subject, the supervisory authority may require it to do so after considering whether the breach is likely to result in a high risk.

### NOTIFICATION OF A PERSONAL DATA BREACH TO THE AUTHORITY

The personal data breach shall be notified to the supervisory authority referred to in Article 55 without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

Where the notification is not made within 72 hours, it shall be accompanied by reasons for the delay.

## REVIEW FOR MANDATORY DATA MANAGEMENT

If the duration of mandatory data processing or the periodic review of its necessity is not determined by law, local government decree, or a binding act of the European Union, the Data Controller shall review, at least every three years from the commencement of the data processing, whether the personal data processed by the Data Controller or by a Data Processor acting on its behalf or under its instructions are still necessary for the purpose of the data processing.

The circumstances and results of such review shall be documented by the Data Controller and retained for a period of ten years following the review, and shall be made available upon request to the Hungarian National Authority for Data Protection and Freedom of Information (NAIH) (hereinafter referred to as the "Authority")._)

## Complaint procedure

A complaint regarding a possible violation of the law by the Data Controller may be submitted to the Hungarian National Authority for Data Protection and Freedom of Information (NAIH):

Hungarian National Authority for Data Protection and Freedom of Information
1055 Budapest, Falk Miksa utca 9-11., Hungary

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

Telephone:
+36-1-391-1400

Fax:
+36-1-391-1410

E-mail:
ugyfelszolgalat@naih.hu

## CONCLUDING REMARKS

The following legislation and recommendations were taken into account when preparing this Privacy Policy:

- 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 Informational Self-Determination and Freedom of Information (hereinafter: "Infotv.")
- Act CVIII of 2001 on Electronic Commerce Services and Certain Issues of Information Society Services (in particular 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 (in particular Section 6)
- Act XC of 2005 on the Freedom of Electronic Information
- Act C of 2003 on Electronic Communications (in particular Section 155)
- Opinion No. 16/2011 concerning the EASA/IAB Recommendation on Best Practice in Online Behavioral Advertising
- Recommendation of the Hungarian National Authority for Data Protection and Freedom of Information on the data protection requirements of prior information notices