www.huonker.hu

PRIVACY POLICY

The translation was made with an automatic google translator, in case of a dispute the Hungarian text shall prevail.

Tartalom

1. INTRODUCTION

Huonker Hungária Kft. (2060 Bicske, Tatai u. 35, tax number: 11114516-2-07, company registration number: 07-09-003668) (hereinafter: Service Provider, data controller) is subject to the following regulations:
REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL On the protection of natural persons with regard to the processing of personal data and on the free flow of such data and on the repeal of Regulation 95/46/EC (General Data Protection Regulation) (April 2016) 27.), we provide the following information.
This data protection policy regulates the data management of the following pages:
https://www.huonker.hu
The data protection policy is available from the following page: https://www.huonker.hu/adatvedelem
Amendments to the regulations will come into effect upon publication at the above address.

1.1. THE DATA MANAGER AND ITS CONTACTS:

Name: Huonker Hungária Kft.
Headquarters: 2060 Bicske, Tatai u. 35.
E-mail: adatvedelem@huonker.hu
Phone: +36 (20) 383 2307

2. TERM DEFINITIONS:

1. "personal data": any information relating to an identified or identifiable natural person ("data subject"); a natural person can be identified directly or indirectly, in particular on the basis of an identifier such as name, number, location data, online identifier or one or more factors relating to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person identifiable;

2. "data management": any operation or set of operations performed on personal data or data files in an automated or non-automated manner, such as the collection, recording, organization, segmentation, storage, transformation or change, query, insight, use, communication, transmission, distribution or by making it available in other ways, coordinating or connecting, limiting, deleting or destroying;

3. "data controller": the natural or legal person, public authority, agency or any other body that determines the purposes and means of processing personal data independently or together with others; if the purposes and means of data management are determined by EU or member state law, the data controller or the special aspects regarding the designation of the data controller may also be determined by EU or member state law;

4. "data processor": the natural or legal person, public authority, agency or any other body that processes personal data on behalf of the data controller;

5. "recipient": the natural or legal person, public authority, agency or any other body to whom or to which the personal data is communicated, regardless of whether it is a third party. Public authorities that have access to personal data in accordance with EU or Member State law in the context of an individual investigation are not considered recipients; the management of said data by these public authorities must comply with the applicable data protection rules in accordance with the purposes of data management;

6. "consent of the data subject": the voluntary, specific and well-informed and clear declaration of the will of the data subject, with which the data subject indicates by means of a statement or an unmistakable act of confirmation that he gives his consent to the processing of personal data concerning him;

7. "data protection incident": a breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure or unauthorized access to personal data transmitted, stored or otherwise handled.

3. PRINCIPLES REGARDING THE HANDLING OF PERSONAL DATA

Personal data:

a) it must be handled legally and fairly, as well as in a transparent manner for the data subject ("legality, fair procedure and transparency");

b) it is collected only for specific, clear and legitimate purposes, and they are not handled in a way that is incompatible with these purposes; in accordance with Article 89 (1), further data processing for the purpose of archiving in the public interest, for scientific and historical research purposes, or for statistical purposes is not considered incompatible with the original purpose ("purpose limitation");

c) they must be appropriate and relevant from the point of view of the purposes of data management, and must be limited to what is necessary ("data economy");

d) they must be accurate and, if necessary, up-to-date; all reasonable measures must be taken to promptly delete or correct personal data that is inaccurate for the purposes of data processing ("accuracy");

e) it must be stored in a form that allows the identification of the data subjects only for the time necessary to achieve the goals of personal data management; personal data may only be stored for a longer period of time if the personal data will be processed in accordance with Article 89 (1) for the purpose of archiving in the public interest, for scientific and historical research purposes or for statistical purposes, the rights of the data subjects and subject to the implementation of appropriate technical and organizational measures required to protect your freedoms ("restricted storage");

f) must be handled in such a way that adequate security of personal data is ensured through the application of appropriate technical or organizational measures, including protection against unauthorized or unlawful processing, accidental loss, destruction or damage of data ("integrity and confidentiality").

The data controller is responsible for compliance with the above, and must also be able to prove this compliance ("accountability").

The data controller declares that its data management is carried out in accordance with the basic principles contained in this point.

4. CERTAIN DATA PROCESSES

4.1. CONTACT

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

Personal data	Purpose of data management	Legal basis
Name	Identification	6. article (1) paragraph a), b) and c) point
E-mail address	Keeping in touch, sending reply messages	6. article (1) paragraph a), b) and c) pont
Phone number	Keeping in touch	6. article (1) paragraph a), b) and c) point
Message content	Required to respond	6. article (1) paragraph a), b)and c) point

2. Scope of stakeholders: All stakeholders who send messages.

3. Duration of data management, deadline for data deletion: If one of the conditions set out in Article 17 (1) of the GDPR exists, it lasts until the data subject's request for deletion.

4. Person of possible data controllers entitled to access the data, recipients of personal data: Personal data can be handled by authorized employees of the data controller.

5. Description of the rights of data subjects related to data management:

• The data subject may request from the data controller access to personal data relating to him, their correction, deletion or restriction of processing, 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 personal data, its deletion, modification, or limitation of processing, data portability in the following ways:

- by post to 2060 Bicske, Tatai u. at address 35,
- by e-mail at the e-mail address adatvedelem@huonker.hu,
- by phone at +36 (20) 383 2307.

7. Legal basis for data management: the consent of the data subject, Article 6 (1) points a), b) and c). If you contact us, you agree that your personal data (name, phone number, e-mail address) provided to us during the contact process will be handled in accordance with these regulations.

8. We inform you that

- this data management is **<u>based on your consent</u>**, or is **<u>necessary for the submission of an offer</u>** or is based on a legal obligation (cooperation) in the case of a contractual relationship.
- you are **<u>required</u>** to provide personal data in order to contact us
- failure to provide data **<u>results</u>** in the inability to contact the Service Provider.
- withdrawal of consent does not affect the legality of data processing based on consent, prior to withdrawal.

4.2. CUSTOMER RELATIONSHIP

1. The fact of data collection, the scope of the managed data and the purpose of the data management

Personal data	Purpose of data management	Legal basis
Name, e-mail address, phone number.	Contact, identification, fulfillment of contracts, business purpose.	Article 6 paragraph (1) points (b) and (c), in case of enforcement of claims arising from the contract, Act V of 2013 on the Civil Code 6:21. §

2. Scope of stakeholders: All stakeholders who are in contact with the data controller by phone/e-mail/in person or who have a contractual legal relationship.

3. Duration of data management, deadline for data deletion: Letters containing inquiries last until the data subject's request for deletion, but a maximum of 2 years.

4. **The person of the possible data controllers entitled to access the data, the recipients of the personal data**: The personal data can be handled by the authorized employees of the data controller, in compliance with the above principles.

5. **Description of the rights of data subjects related to data management:**

• The data subject may request from the data controller access to personal data relating to him, their correction, deletion or restriction of processing, 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 personal data, its deletion, modification, or limitation of processing, data portability in the following ways:**

- by post to 2060 Bicske, Tatai u. at address 35,
- by e-mail at the e-mail address adatvedelem@huonker.hu,
- by phone at +36 (20) 383 2307.

7. **Legal basis for data management:**

8. We inform you that

• **data management is necessary to fulfill the contract and submit an offer.**
• is **obliged** to provide personal data so that we can fulfill the contract/fulfill your other requests.

- failure to provide data results in us **not being able** to fulfill the contract/process your request.

5. ADDRESSES WITH WHOM THE PERSONAL DATA IS COMMUNICATED

"recipient": the natural or legal person, public authority, agency or any other body to whom or to which the personal data is communicated, regardless of whether it is a third party.

5.1. DATA PROCESSORS (THOSE WHO PROCESS DATA ON BEHALF OF THE DATA PROCESSOR)

The data controller uses data processors in order to facilitate its own data management activities and to fulfill its contractual obligations with the data subject and the obligations imposed by legislation.

The data controller places great emphasis on using only data processors who provide adequate guarantees for the implementation of appropriate technical and organizational measures ensuring compliance with the requirements of the GDPR and the protection of the rights of the data subjects.

The data processor and any person acting under the control of the data processor who has access to personal data shall handle the personal data contained in these regulations exclusively in accordance with the instructions of the data controller.

The data controller is legally responsible for the activities of the data processor. The data processor is only liable for damages caused by data processing if it has not complied with the obligations specifically imposed on data processors specified in the GDPR, or if it has ignored or acted contrary to the legal instructions of the data controller.

The data processor has no meaningful decision-making regarding the management of the data.

5.2. CERTAIN DATA PROCESSORS

DATA PROCESSING ACTIVITY	NAME	ADDRESS, CONTACT
Hosting service	EV2 Internet Kft.	1149 Budapest, Róna út 120-122., Tel: +36-1-460-0104, +36-70-338-4091, email: info@cpanel.hu

6. MANAGEMENT OF COOKIES

1. This website only uses cookies that are necessary for the general operation of the site. The website itself does not store cookies.

2. Server log files ensure the safety and usability of the site, which were created by the service provider. The IP address is stored in these log files for the duration of the site visit. The site does not contain a contact form or similar, so it is not possible to associate the IP address of the site visitor with his or her person. In addition, the following data are recorded for the above-mentioned purpose:

    - browser type and browser version
    - used operating system
    - referrer URL
    - host name of the accessing computer
    - server query time

    It is also not possible to infer the identity of the site visitor from these data.

3. Most browsers allow you to set which cookies should be saved and to delete (specific) cookies. If the saving of cookies is restricted on specific websites or third-party cookies are prohibited, this may lead to the fact that the website can no longer be used in its entirety under certain circumstances. Here is information on how to customize cookie settings for standard browsers:

    Google Chrome (https://support.google.com/chrome/answer/95647?hl=hu)

    Internet Explorer (https://support.microsoft.com/hu-hu/help/17442/windows-internet-explorer-delete-manage-cookies)

    Firefox (https://support.mozilla.org/hu/kb/sutik-engedelyezese-es-tiltasa-amit-weboldak-haszn

    Safari (https://support.apple.com/kb/PH21411?locale=hu_HU)

    Microsoft Edge (https://support.microsoft.com/hu-hu/microsoft-edge/cookie-k-t%C3%B6rl%C3%A9se-a-microsoft-edge-ben-63947406-40ac-c3b8-57b9-2a946a29ae09)

7. USE OF COMMUNITY SERVICES

7.1 COMMUNITY WEBPAGES

1. The fact of the data collection, the scope of the processed data: Meta/Google+/Twitter/Pinterest/Youtube/Instagram, etc. the name registered on social networking sites and the user's public profile picture.

2. Scope of stakeholders: All stakeholders who have registered on Meta/Google+/Twitter/Pinterest/Youtube/Instagram, etc. on social media sites and "liked" the Service Provider's social media site, or contacted the data controller via the social media site.

3. Purpose of data collection: Sharing, "liking", following and promoting certain content elements, products, promotions or the website itself on social networks.

4. The duration of data management, the deadline for deleting data, the identity of possible data controllers entitled to access the data and the description of the rights of the data subjects in relation to data management: The data subject can find out about the source of the data, its management, the method of transfer and its legal basis on the given social site. Data management takes place on social media sites, so the duration and method of data management, as well as the options for deleting and modifying data, are governed by the regulations of the given social media site.

5. The legal basis for data management: the voluntary consent of the concerned person to the management of his personal data on social networking sites.

8. CUSTOMER RELATIONS AND OTHER DATA MANAGEMENT

1. If a question arises during the use of our data controller services, or if the data subject has a problem, he can contact the data controller using the methods provided on the website (telephone, e-mail, social media sites, etc.).

2. The data controller processes received e-mails, messages, on the phone, on Facebook, etc. data provided, together with the name and e-mail address of the interested party, as well as other voluntarily provided personal data, will be deleted after a maximum of 2 years from the date of data communication.

3. We provide information on data management not listed in this information when the data is collected.

4. The Service Provider is obliged to provide information, communicate and transfer data, or make documents available in the case of an exceptional official request or other bodies based on the authorization of the law.

5. In these cases, the Service Provider only discloses personal data to the requester - if he has indicated the exact purpose and the scope of the data - to the extent and to the extent that is absolutely necessary to achieve the purpose of the request.

9. RIGHTS OF THE DATA SUBJECTS

1. Right of access

You are entitled to receive feedback from the data controller as to whether your personal data is being processed, and if such data processing is underway, you are entitled to access your personal data and the information listed in the regulation.

2. Right to rectification

You have the right to request that the data controller correct inaccurate personal data concerning you without undue delay. Taking into account the purpose of data management, you are entitled to request the completion of incomplete personal data, including by means of a supplementary statement.

3. Right to erasure

You have the right to request that the data manager delete your personal data without undue delay, and the data manager is obliged to delete your personal data without undue delay under certain conditions.

4. The right to be forgotten

If the data controller has disclosed the personal data and is required to delete it, it will take reasonable steps, including technical measures, taking into account available technology and implementation costs, to inform the data controllers that you have requested the personal data in question the deletion of links or duplicates of these personal data.

5. The right to restrict data processing

You have the right to have the data controller restrict data processing at your request if one of the following conditions is met:

- You dispute the accuracy of the personal data, in which case the limitation applies to the period that allows the data controller to check the accuracy of the personal data;
- the data processing is illegal and you object to the deletion of the data and instead request the restriction of its use;
- the data controller no longer needs the personal data for the purpose of data management, but you require them to present, assert or defend legal claims;
- You objected to data processing; in this case, the limitation applies to the period until it is determined whether the legitimate reasons of the data controller take precedence over your legitimate reasons.

6. The right to data portability

You have the right to receive the personal data you have provided to a data controller in a segmented, widely used, machine-readable format, and you have the right to transmit this data to another data controller without hindrance from the data controller whose provided personal data to (...)

7. The right to protest

In the case of data processing based on legitimate interest or public authority as legal grounds, you have the right to object at any time to the processing of your personal data for reasons related to your own situation, including profiling based on the aforementioned provisions.

8. Protest in the event of direct business acquisition

If personal data is processed for direct business acquisition, you have the right to object at any time to the processing of your personal data for this purpose, including profiling, if it is related to direct business acquisition. If you object to the processing of personal data for the purpose of direct business acquisition, then the personal data may no longer be processed for this purpose.

9. Automated decision-making in individual cases, including profiling

You have the right not to be subject to the scope of a decision based solely on automated data management, including profiling, which would have legal effects on you or would similarly significantly affect you.
The previous paragraph does not apply if the decision:

- Necessary to conclude or fulfill the contract between you and the data controller;
- it is made possible by EU or member state law applicable to the data controller, which also establishes appropriate measures for the protection of your rights and freedoms, as well as your legitimate interests; obsession
- Based on your express consent.

10. ACTION DEADLINE

The data controller will inform you of the measures taken following the above requests without undue delay, but in any case within **1 month** from the receipt of the request.

If necessary, this can be extended by **2 months**. The data controller will inform you of the extension of the deadline, indicating the reasons for the delay, within **1 month** of receiving the request.

If the data controller does not take measures following your request, **it will inform you of the lack of action without delay, but at the latest within one month from the receipt of the request**

reasons, and that you can file a complaint with a supervisory authority and exercise your right to judicial redress.

11. SECURITY OF DATA MANAGEMENT

The data controller and the data processor implement appropriate technical and organizational measures, taking into account the state of science and technology and the costs of implementation, as well as the nature, scope, circumstances and purposes of data management, as well as the variable probability and severity of the risk to the rights and freedoms of natural persons. , to guarantee a level of data security appropriate to the degree of risk, including, among others, where appropriate:

a) pseudonymization and encryption of personal data;

b) ensuring the continuous confidentiality, integrity, availability and resilience of the systems and services used to manage personal data;

c) in the event of a physical or technical incident, the ability to restore access to personal data and the availability of data in a timely manner;

d) a procedure for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures taken to guarantee the security of data management.

e) The 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 filing, and in the case of data handled in electronic form, by using a central authorization management system.

f) The method of storing the data using IT methods must be chosen in such a way that their deletion can be carried out - taking into account the possibly different deletion deadline - at the end of the data deletion deadline, or if necessary for other reasons. The deletion must be irreversible.

g) Paper-based data carriers must be stripped of personal data using a document shredder or an external organization specialized in document destruction. In the case of electronic data carriers, physical destruction must be ensured in accordance with the rules for the disposal of electronic data carriers, and, if necessary, the data must be securely and irretrievably deleted in advance.

h) The data controller takes the following specific data security measures:

a.

a. In order to ensure the security of personal data handled on a paper basis, the Service Provider applies the following measures *(physical protection):*

   i. Place the documents in a safe, well-sealed dry room.
   ii. The Service Provider's building and premises are equipped with fire protection and property protection equipment.
   iii. Personal data can only be accessed by authorized persons, third parties cannot access it.
   iv. During the course of his work, the Service Provider's employee performing data management may only leave the room where data management is taking place by blocking the data carriers entrusted to him or by closing the given room.
   v. If personal data managed on paper is digitized, the rules governing digitally stored documents must be applied.

b. IT protection

   i. Computers and mobile devices (other data carriers) used during data management are the property of the Service Provider.
   ii. Data on computers can only be accessed with a username and password.
   iii. The central server machine can only be accessed by persons with appropriate authorization and only those designated for it.
   iv. In order to ensure the security of digitally stored data, the Service Provider uses data backups and archives.
   v. The computer system containing personal data used by the Service Provider is equipped with virus protection.
   vi. The service provider also uses SSL/TLS encryption procedures on its website.

12. NOTIFICATION OF THE DATA PROTECTION INCIDENT

If the data protection incident likely involves a high risk for the rights and freedoms of natural persons, the data controller shall inform the data subject of the data protection incident without undue delay.

In the information provided to the data subject, the nature of the data protection incident must be **clearly and comprehensibly** described, and the name and contact information of the data protection officer or other contact person providing additional information must be provided; the likely consequences of the data protection incident must be described; the measures taken or planned by the data controller to remedy the data protection incident must be described, including, where appropriate, measures aimed at mitigating any adverse consequences resulting from the data protection incident.

The data subject does 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 these measures have been applied to the data affected by the data protection incident, in particular those measures - such as the use of encryption - that make them **unintelligible to persons not authorized to access personal data the data;**
- after the data protection incident, the data controller has taken additional measures to **ensure that the high risk to the rights and freedoms of the data subject is unlikely to materialize in the future;**
- providing information would **require a disproportionate effort**. In such cases, the data subjects must be informed through publicly published information, or a similar measure must be taken that ensures similarly effective information to the data subjects.

If the data controller has not yet notified the data subject of the data protection incident, the supervisory authority, after considering whether the data protection incident is likely to involve a high risk, may order the data subject to be informed.

13. REPORTING A DATA PROTECTION INCIDENT TO THE AUTHORITY

The data controller shall report the data protection incident to the competent supervisory authority pursuant to Article 55 without undue delay and, if possible, no later than 72 hours after becoming aware of the data protection incident, unless the data protection incident is likely to pose no risk to the rights of natural persons and freedoms. If the notification is not made within 72 hours, the reasons justifying the delay must also be attached.

14. REVIEW IN CASE OF MANDATORY DATA MANAGEMENT

If the duration of the mandatory data management, or the periodic review of its necessity, is not determined by law, a local government regulation, or a mandatory legal act of the European Union, the data controller **shall review at least every three years from the start** of the data management that the personal data managed by him or by the data processor acting on his behalf or on the basis of his order whether data management is necessary to achieve the purpose of data management.

The data controller documents the circumstances and results of this review, **keeps this documentation for ten years after the review has been completed** and makes it available to the Authority at the request of the National Data Protection and Freedom of Information Authority (hereinafter: the Authority).

15. OPPORTUNITY TO COMPLAINT

You can file a complaint with the National Data Protection and Freedom of Information Authority against possible violations of the data controller:

National Data Protection and Freedom of Information Authority
1055 Budapest, Falk Miksa utca 9-11.
Mailing address: 1374 Budapest, Pf.: 603.
Telephone: +36 -1-391-1400
Fax: +36-1-391-1410
E-mail: ugyfelszolgalat@naih.hu

16. CLOSING WORD

During the preparation of the information, we paid attention to the following legislation:

- REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (GDPR) on the protection of natural persons with regard to the processing of personal data and on the free flow of such data and on the repeal of Regulation 95/46/EC (General Data Protection Regulation) (April 27, 2016)
- CXII of 2011. Act - on the right to self-determination of information and freedom of information (hereinafter: Infotv.)
- CVIII of 2001 Act - on certain issues of electronic commercial services and services related to the information society (mainly § 13/A)
- XLVII of 2008 law - on the prohibition of unfair trade practices towards consumers;
- XLVIII of 2008 Act - on the basic conditions and certain limitations of economic advertising (especially § 6.a)
- 2005 XC. Act on Electronic Freedom of Information
- Act C of 2003 on electronic communication (specifically § 155.a)
- 16/2011. s. Opinion on the EASA/IAB Recommendation on Best Practices for Behavioral Online Advertising
- The recommendation of the National Data Protection and Freedom of Information Authority on the data protection requirements of prior information

March 2022