

Privacy Policy

Summary

We collect and process personal data strictly in accordance with the law.

Data is stored as securely as possible.

Personal data is only shared with third parties with consent.

We provide information about stored personal data upon written request:
info@netadclick.com.

Requests for the deletion of personal data can be made at this address:
info@netadclick.com.

Introduction

The business group detailed below, including AD Solutions Kft. (1031 Budapest, Lilla u. 8., 01-09-930495, registered at the Budapest Court of Registration), hereinafter referred to as "Service Provider", adheres to the following policy.

According to Article 20(1) of Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information, before data processing begins, the affected individual (in this case, the website/blog user, hereinafter referred to as "User") must be informed whether data processing is based on consent or is mandatory.

Before the start of data processing, the affected individual must be clearly and thoroughly informed of all facts related to the processing of their data, particularly the purpose and legal basis of data processing, the person authorized to perform data processing and data management, and the duration of data processing.

The affected individual must also be informed, based on Section 6(1) of the Information Act, that personal data may be processed even if obtaining the individual's consent is impossible or would involve disproportionate effort, and the processing is necessary either to fulfill a legal obligation of the data controller or to protect the legitimate interests of the data controller or a third party, provided that such interests are proportionate to the limitation of the data subject's right to the protection of their personal data.

The affected individual must also be informed of their rights and legal remedies regarding data processing.

If providing personal information to the affected individual is impossible or would involve disproportionate effort, information may also be provided by publicizing the following:

- a) the fact of data collection,
- b) the scope of the affected individuals,

- c) the purpose of data collection,
- d) the duration of data processing,
- e) the potential data controllers authorized to access the data,
- f) a description of the affected individuals' rights and legal remedies related to data processing,
- g) if the data processing is subject to registration, the registration number of the data processing.

Scope

This privacy policy governs the data processing of the following websites:

- Main domain: <http://netadclick.com>
- Redirected domain: <http://netadclick.hu>

Amendments to this policy will become effective upon publication at the above address. Each chapter title of this policy also includes references to the relevant legal provisions.

Definitions

1. **Personal Data:** Any information relating to an identified or identifiable natural person ("Data Subject"); a natural person is identifiable if they can be identified, directly or indirectly, particularly by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more 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 which is performed on personal data or on sets of personal data, whether or not by automated means, 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. **Restriction of Data Processing:** The marking of stored personal data with the aim of limiting their processing in the future.
4. **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, particularly to analyze or predict aspects concerning that natural person's performance

at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

5. Pseudonymization: The processing of personal data in such a manner that the personal data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

6. Filing System: Any structured set of personal data which is accessible according to specific criteria, whether centralized, decentralized, or dispersed on a functional or geographical basis.

7. Data 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 Data Controller or the specific criteria for its nomination may be provided for by Union or Member State law.

8. Processor: A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the Data Controller.

9. 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.

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

11. 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.

12. 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.

13. Genetic Data: Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

14. **Biometric Data:** Personal data resulting from specific technical processing relating to the physical, physiological, or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

15. **Health Data:** Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about their health status.

16. **Main Establishment:**

a) Regarding a Data Controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the Controller in the Union, in which case the latter shall be considered to be the main establishment, provided that the establishment has the power to have such decisions implemented.

b) Regarding a Processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the Processor has no central administration in the Union, the establishment of the Processor in the Union where the main processing activities in the context of the activities of an establishment of the Processor take place to the extent that the Processor is subject to specific obligations under this Regulation.

17. **Representative:** A natural or legal person established in the Union who, designated by the Data Controller or Processor in writing pursuant to Article 27, represents the Controller or Processor regarding their respective obligations under this Regulation.

18. **Enterprise:** A natural or legal person engaged in economic activity, regardless of its legal form, including partnerships or associations regularly engaged in economic activity.

19. **Group of Undertakings:** A controlling undertaking and its controlled undertakings.

20. **Binding Corporate Rules:** Personal data protection policies adhered to by a Controller or Processor established on the territory of a Member State for transfers or a set of transfers of personal data to a Controller or Processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.

21. **Supervisory Authority:** An independent public authority which is established by a Member State pursuant to Article 51.

22. **Concerned Supervisory Authority:** A Supervisory Authority which is concerned by the processing of personal data because:

a) The Data Controller or Processor is established in the territory of the Member State of that Supervisory Authority;

b) Data Subjects residing in the Member State of that Supervisory Authority are substantially affected or likely to be substantially affected by the processing; or

c) A complaint has been lodged with that Supervisory Authority.

23. Cross-Border Processing of Personal Data:

a) Processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a Data Controller or Processor in the Union where the Controller or Processor is established in more than one Member State; or

b) Processing of personal data which takes place in the context of the activities of a single establishment of a Controller or Processor in the Union but which substantially affects or is likely to substantially affect Data Subjects in more than one Member State.

24. Relevant and Reasoned Objection: An objection to a draft decision as

to whether there is an infringement of this Regulation or whether the envisaged action regarding the Controller or Processor complies with this Regulation, which clearly demonstrates the significance of the risks posed by the draft decision regarding the fundamental rights and freedoms of Data Subjects and, where applicable, the free flow of personal data within the Union.

25. Information Society Service: A service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council.

26. International Organization: An organization and its subordinate bodies governed by public international law or any other body set up by or based on an agreement between two or more countries.

Legal Basis for Data Processing

1. Personal data may be processed if:

- The Data Subject has given consent, or
- Processing is necessary for compliance with a legal obligation to which the Controller is subject or, under the authorization of the law, for a public interest purpose as specified therein.

2. Personal data may also be processed if obtaining consent from the Data Subject is impossible or would involve disproportionate effort, and the processing is necessary:

- a) For compliance with a legal obligation to which the Controller is subject; or
 - b) To protect the legitimate interests of the Controller or a third party, provided that such interests are proportionate to the limitation of the Data Subject's right to the protection of personal data.
3. If the Data Subject is unable to give consent due to incapacity or other compelling reasons, personal data may be processed to the extent necessary to protect vital interests, such as life, physical integrity, or property, while the obstacles to obtaining consent persist.
4. The validity of the consent of a minor who has reached the age of 16 does not require the consent or subsequent approval of their legal representative.
5. If the purpose of data processing based on consent is to execute a contract concluded in writing with the Data Controller, the contract must include all necessary information that the Data Subject must know, including the identification of the data to be processed, the duration of processing, the purpose of the use, the fact of data transfer, recipients, and the use of data processors. The contract must explicitly state that by signing it, the Data Subject consents to the processing of their data as specified in the contract.
6. If the collection of personal data is based on the Data Subject's consent, the Data Controller may process the collected data for the fulfillment of its legal obligations or for the protection of the legitimate interests of the Data Controller or a third party, provided that such interests are proportionate to the limitation of the Data Subject's right to the protection of personal data.

Principles for Processing Personal Data

Personal data shall be:

- a) Processed lawfully, fairly, and in a transparent manner in relation to the Data Subject ("lawfulness, fairness, and transparency");
- b) 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 shall not be considered incompatible with the original purposes ("purpose limitation");
- c) Adequate, relevant, and limited to what is necessary concerning the purposes for which they are processed ("data minimization");
- d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, concerning the purposes for which they are processed, are erased or rectified without delay ("accuracy");

e) Kept in a form that permits the 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, subject to the implementation of the appropriate technical and organizational measures required by this Regulation to safeguard the rights and freedoms of the Data Subject ("storage limitation");

f) 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").

2. The Data Controller shall be responsible for and be able to demonstrate compliance with paragraph 1 ("accountability").

Functional Data Processing

1. According to Article 20(1) of Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information, the following must be specified regarding the functionality of the website/blog:

a) The fact of data collection,

b) The scope of the affected individuals,

c) The purpose of data collection,

d) The duration of data processing,

e) The potential data controllers authorized to access the data,

f) A description of the affected individuals' rights and legal remedies related to data processing.

2. The fact of data collection, scope of processed data:

Registered partner:

- Email address

- Name

- Phone number

- Username

- Name of the represented organization

- Headquarters of the represented organization

- Tax number of the represented organization
- Bank account number of the represented organization
- Website(s) of the represented organization
- Name, email address, phone number of the representative/users' other provided contacts

Other requested data:

- IP addresses, browsing, ordering, purchase data, history

3. Scope of affected individuals: All users registered on the website.

4. Purpose of data collection:

For the website:

Email:

- Marketing
- Direct marketing
- Newsletter distribution
- Database building
- Non-official statistics
- Customer relationship
- Periodic promotions
- Sweepstakes
- Surveys
- Loyalty programs
- Discounts
- Satisfaction measurement
- Registration
- Recommendation of related services, including third-party promotions

Name (first name and/or last name, company name):

- Marketing
- Direct marketing

- Newsletter distribution
- Database building
- Non-official statistics
- Customer relationship
- Periodic promotions
- Sweepstakes
- Surveys
- Loyalty programs
- Discounts
- Satisfaction measurement
- Registration
- Recommendation of related services, including third-party promotions

Phone number:

- Marketing
- Direct marketing
- Message distribution
- Database building
- Non-official statistics
- Customer relationship
- Periodic promotions
- Sweepstakes
- Surveys
- Loyalty programs
- Discounts
- Satisfaction measurement
- Registration
- Recommendation of related services

Username:

- Surveys
- Loyalty programs
- Customer relationship
- Satisfaction measurement
- Registration
- Recommendation of related services
- Newsletter distribution
- Database building
- Non-official statistics

Other personal data:

- Marketing
- Non-official statistics

5. Duration of data processing, deadline for data deletion: Immediately upon registration deletion. Except for accounting documents, which must be retained for 8 years under Section 169(2) of Act C of 2000 on Accounting. Accounting records directly and indirectly supporting the accounting records (including general ledger accounts, analytical or detailed records) must be retained in a legible form and retrievable by reference to the accounting records for at least 8 years.

6. Potential data controllers authorized to access the data: Personal data may be processed by the Data Controller's employees in compliance with the above principles.

7. Description of the affected individuals' rights and legal remedies related to data processing: The following data can be modified on the websites:

- Email address
- Name
- Phone number
- Username
- Other personal data

The Data Subject can initiate the deletion or modification of personal data through the following methods:

- By mail: 1052 Budapest, Vármegye u. 7. V. em. 3.
- By email: info@netadclick.com.

8. Legal basis for data processing: User consent, Section 5(1) of the Information Act, and Section 13/A(3) of Act CVIII of 2001 on Electronic Commerce and on Information Society Services (hereinafter: "E-Commerce Act"): The service provider may process personal data technically indispensable for the provision of the service. The service provider must select and operate the tools used for the provision of the information society service in such a way that personal data is only processed when it is essential for providing the service and for fulfilling other purposes set out in this Act, and even then, only to the necessary extent and for the necessary time.

Data Processing During Service Provision

1. Under Article 20(1) of Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information, the following must be specified regarding data processing during service provision on the website/blog:

- a) The fact of data collection,
- b) The scope of the affected individuals,
- c) The purpose of data collection,
- d) The duration of data processing,
- e) The potential data controllers authorized to access the data,
- f) A description of the affected individuals' rights and legal remedies related to data processing.

2. Fact of data processing, scope of processed data:

- a) Data transferred for delivery purposes: delivery name, delivery address, phone number, amount payable.
- b) Data transferred for online payment purposes: billing name, billing address, amount payable.

3. Scope of affected individuals: All individuals requesting home delivery/online purchase.

4. Purpose of data processing: The delivery of ordered products/handling online purchases.

5. Duration of data processing, deadline for data deletion: Until the completion of home delivery/online payment.

6. Potential data controllers authorized to access the data: Personal data may be processed by the following entities, in compliance with the above principles: Service Provider, Data Controller.

7. Description of the affected individuals' rights and legal remedies related to data processing: The Data Subject may request the prompt deletion of their personal data from the delivery service/online payment provider.

8. Legal basis for data processing: User consent, Section 5(1) of the Information Act, and Section 13/A(3) of the E-Commerce Act.

Use of Cookies

1. Under Article 20(1) of Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information, the following must be specified regarding the use of cookies on the website/blog:

- a) The fact of data collection,
- b) The scope of the affected individuals,
- c) The purpose of data collection,
- d) The duration of data processing,
- e) The potential data controllers authorized to access the data,
- f) A description of the affected individuals' rights and legal remedies related to data processing.

2. The typical cookies used on the website/blog include "password-protected session cookies," "shopping cart cookies," and "security cookies," which do not require prior consent from the affected individuals.

3. Fact of data processing, scope of processed data: unique identifiers, dates, times, browsing, and purchasing history.

4. Scope of affected individuals: All individuals visiting the website or partner websites (publishers, advertisers, other service users).

5. Purpose of data processing: User identification, tracking shopping cart content, and visitor tracking.

6. Duration of data processing, deadline for data deletion: Data processing lasts for the duration of session cookies as defined by the website/blog or until the user clears their browser.

7. Potential data controllers authorized to access the data: Personal data may be processed by the Data Controller's employees in compliance with the above principles.

8. Description of the affected individuals' rights and legal remedies related to data processing: The affected individuals can delete cookies through their browser's Tools/Settings menu, typically under the Privacy settings.

9. Legal basis for data processing: Consent is not required if the sole purpose of using cookies is to carry out communication through an electronic communications network or if the Service Provider requires the use of cookies to provide a service requested by the subscriber or user.

Data Transfer

1. Under Article 20(1) of Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information, the following must be specified regarding data transfer activities on the website/blog:

- a) The fact of data collection,
- b) The scope of the affected individuals,
- c) The purpose of data collection,
- d) The duration of data processing,
- e) The potential data controllers authorized to access the data,
- f) A description of the affected individuals' rights and legal remedies related to data processing.

2. Fact of data processing, scope of processed data:

- a) Data transferred for delivery purposes: delivery name, delivery address, phone number, amount payable.
- b) Data transferred for online payment purposes: billing name, billing address, amount payable.

3. Scope of affected individuals: All individuals requesting home delivery/online purchase.

4. Purpose of data processing: The delivery of ordered products/handling online purchases.

5. Duration of data processing, deadline for data deletion: Until the completion of home delivery/online payment.

6. Potential data controllers authorized to access the data: Personal data may be processed by the following entities, in compliance with the above principles: Service Provider, Data Controller.

7. Description of the affected individuals' rights and legal remedies related to data processing: The Data Subject may request the prompt deletion of their personal data from the delivery service/online payment provider.

8. Legal basis for data processing: User consent, Section 5(1) of the Information Act, and Section 13/A(3) of the E-Commerce Act.

Social Media

- We use Facebook: [Facebook Page](<https://www.facebook.com/Netadclickcom-175389209149370/>)

Facebook Privacy Policy: [Facebook Privacy](<https://www.facebook.com/privacy/explanation>)

1. Under Article 20(1) of Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information, the following must be specified regarding data transfer activities on the website/blog:

- a) The fact of data collection,
- b) The scope of the affected individuals,
- c) The purpose of data collection,
- d) The duration of data processing,
- e) The potential data controllers authorized to access the data,
- f) A description of the affected individuals' rights and legal remedies related to data processing.

2. Fact of data collection, scope of processed data: name registered on the above social media sites and the public profile picture of the user.

3. Scope of affected individuals: All individuals registered on Facebook who have liked the website.

4. Purpose of data processing: Sharing or liking certain content elements, products, promotions, or the website itself on the above social media sites.

5. Duration of data processing, potential data controllers authorized to access the data, and a description of the affected individuals' rights and legal remedies related to data processing: Information about the source of the data, the management of data, the manner of transfer, and the legal basis can be found at the addresses (addresses) of the above social media sites.

6. Data processing is carried out on the above social media sites, so their regulations apply to the duration of data processing, the method, and the possibilities for deletion and modification of data.

7. Legal basis for data processing: The voluntary consent of the affected individual to the processing of their personal data on the above social media sites.

External Online Billing Provider

- Name: Szamlazz.hu

Transferred data:

- Tax number

- Email address

- Shipping address

External CRM System

- Name: Clickup.com

Privacy Policy: [ClickUp Privacy Policy](<https://clickup.com/privacy>)

Transferred data: Access to all data

Purpose of data processing: Direct sales and contact management, solicitation with new business offers

Duration of data processing: Until the client requests the deletion of their data

Data Transfer to External Companies

- Google

- Google AdSense: Used as an advertiser

- Google Adwords: Used as an advertiser

The website/blog uses Google Adwords remarketing tracking codes.

Remarketing is a function that helps the website/blog display relevant ads to users who have previously visited the site while browsing other sites within the Google Display Network. The remarketing code uses cookies to tag visitors. Users who visit the online store can disable these cookies, and additional information on Google's data management can be found at the following addresses: [Google Ads Policies](<http://www.google.hu/policies/technologies/ads/>) and [Google Analytics Opt-out](<https://support.google.com/analytics/answer/2700409>).

If users disable remarketing cookies, they will not receive personalized offers from the website/blog.

- Google Analytics: The website/blog measures its visitor traffic data using the Google Analytics service. During the use of the service, data is transferred. The transferred data is not suitable for identifying the individual. More information about Google's privacy practices can be found here: [Google Privacy](<http://www.google.hu/policies/privacy/ads/>)

Email Marketing (EDM) Activity

1. According to Section 6 of Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities, the User may give prior and express consent for the Service Provider to contact them with promotional offers and other communications at the contact information provided during registration (e.g., email address or phone number).
2. Additionally, the Client, taking into account the provisions of this policy, may consent to the processing of their personal data necessary for sending promotional offers by the Service Provider.
3. The Service Provider does not send unsolicited promotional messages, and the User may unsubscribe from receiving offers without limitation, free of charge, and without providing any reason. In this case, the Service Provider will delete all personal data necessary for sending promotional messages from its records and will no longer contact the User with promotional offers. Users can unsubscribe by clicking the link in the message.
4. Under Article 20(1) of Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information, the following must be specified regarding data processing for newsletter distribution:
 - a) The fact of data collection,
 - b) The scope of the affected individuals,
 - c) The purpose of data collection,
 - d) The duration of data processing,
 - e) The potential data controllers authorized to access the data,
 - f) A description of the affected individuals' rights and legal remedies related to data processing.

5. Fact of data collection, scope of processed data: name, email address, (phone number) date, time.
6. Scope of affected individuals: All individuals subscribing to the newsletter.
7. Purpose of data processing: Sending electronic messages containing advertisements (email, SMS, push messages) to the affected individuals, providing information about current news, products, promotions, new features, etc.
8. Duration of data processing, deadline for data deletion: Data processing continues until the withdrawal of the consent, i.e., until the User unsubscribes.
9. Potential data controllers authorized to access the data: Personal data may be processed by the Data Controller's employees in compliance with the above principles.
10. Description of the affected individuals' rights and legal remedies related to data processing: The affected individuals can unsubscribe from the newsletter at any time, free of charge.
11. Legal basis for data processing: The voluntary consent of the affected individual, Section 5(1) of the Information Act, and Section 6(5) of Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities: The advertiser, the advertising service provider, or the publisher of the advertisement may keep a record of the personal data of individuals who have given their consent, to the extent specified in the consent. The personal data recorded in this database may only be processed according to the terms set out in the consent and until the consent is withdrawn, and may only be disclosed to third parties with the prior consent of the individual.

Data Security

1. The Data Controller and the Processor, taking into account the state of the art, the cost of implementation, the nature, scope, context, and purposes of processing, as well as the varying likelihood and severity of the risks to the rights and freedoms of natural persons, shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including, inter alia, as appropriate:
 - a) The pseudonymization and encryption of personal data;
 - b) The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;
 - c) The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
 - d) A process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security, particular consideration shall be given to the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed.

3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1.

4. The Data Controller and the Processor shall take steps to ensure that any natural person acting under the authority of the Data Controller or the Processor who has access to personal data does not process them except on instructions from the Data Controller unless required to do so by Union or Member State law.

Rights of the Data Subject

1. The Data Subject may request the Service Provider to provide information about the processing of their personal data, request the correction of their personal data, and request the deletion or blocking of their personal data, except for mandatory data processing.

2. Upon request, the Data Controller shall inform the Data Subject about the data processed by it or by the Processor it has instructed, the source of such data, the purpose, legal basis, and duration of the processing, the name, address, and processing activities of the Processor, and, in the case of data transfer, the legal basis and recipient of the transfer.

3. For the purpose of verifying the lawfulness of data transfer and informing the Data Subject, the Data Controller shall maintain a data transfer record, which shall include the time of the transfer of personal data it processes, the legal basis and recipient of the transfer, the scope of the transferred personal data, and other data specified in the legislation requiring the processing.

4. The Data Controller shall provide the information in a clear form, free of charge, upon the Data Subject's request in writing, within the shortest possible time, but no later than 30 days from the submission of the request.

5. Upon the User's request, the Service Provider shall provide information about the data it processes, the source of the data, the purpose of the processing, the legal basis, the duration of the processing, the Processor's name, address, and processing activities, and in the case of data transfer, the legal basis and recipient of the transfer. The Service Provider shall provide the information in a clear form, free of charge, within the shortest possible time, but no later than 30 days from the submission of the request.

6. If personal data processed by the Service Provider do not correspond to reality and the correct personal data are available to the Data Controller, the Service Provider shall correct the personal data.

7. Instead of deletion, the Service Provider shall block the personal data if requested by the User or if, based on the available information, it can be assumed that deletion would harm the legitimate interests of the User. The blocked personal data may only be processed for as long as the purpose of the data processing that excluded the deletion of the personal data exists.

8. The Service Provider shall delete the personal data if the processing is unlawful, the User requests it, the processed data are incomplete or inaccurate—and this state cannot be lawfully remedied—unless the deletion is excluded by law, the purpose of the processing has ceased, or the storage of the data is not permitted by law, or the deletion has been ordered by a court or the National Authority for Data Protection and Freedom of Information.

9. The Data Controller shall mark the personal data it processes if the Data Subject disputes its correctness or accuracy, but the incorrectness or inaccuracy of the disputed personal data cannot be clearly determined.

10. The Data Subject and all those to whom the data were previously transferred for processing shall be notified of the correction, blocking, marking, and deletion. Notification may be omitted if this does not violate the Data Subject's legitimate interest regarding the purpose of processing.

11. If the Data Controller does not fulfill the Data Subject's request for correction, blocking, or deletion, the Data Controller shall provide the factual and legal reasons for the rejection in writing within 30 days of receiving the request. If the Data Subject's request for correction, deletion, or blocking is rejected, the Data Controller shall inform the Data Subject about the possibility of judicial remedy or a complaint to the Authority.

Legal Remedies

1. The User may object to the processing of their personal data if:

a) The processing or transfer of personal data is necessary solely for the fulfillment of the Service Provider's legal obligation or for the enforcement of the legitimate interests of the Service Provider, the data recipient, or a third party, unless processing is required by law;

b) The personal data is used or transferred for direct marketing, public opinion polling, or scientific research purposes;

c) In other cases specified by law.

2. The Service Provider shall examine the objection within the shortest possible time, but no later than 15 days, decide whether it is justified, and notify the applicant in writing of its decision. If the Service Provider establishes the validity of the objection, the processing, including further data collection and data transfer, shall be terminated, the data shall be blocked, and all those to whom the data were previously transferred shall be notified of the objection and the measures taken based on the objection, who shall then take steps to enforce the right to object.

3. If the User does not agree with the decision of the Service Provider, they may take the matter to court within 30 days of notification. The court shall act promptly.

4. Any violation of the law by the Data Controller may be subject to a complaint to the National Authority for Data Protection and Freedom of Information:

National Authority for Data Protection and Freedom of Information

1125 Budapest, Szilágyi Erzsébet fasor 22/C.

Mailing address: 1530 Budapest, P.O. Box: 5

Phone: +36-1-391-1400

Fax: +36-1-391-1410

Email: ugyfelszolgalat@naih.hu

Judicial Enforcement

1. The Data Controller must prove that data processing complies with the legal requirements. The recipient of the data must prove the lawfulness of data transfer.

2. The case falls within the jurisdiction of the court. The lawsuit, at the choice of the Data Subject, may also be brought before the court with jurisdiction over the Data Subject's place of residence or temporary residence.

3. The party may also be someone who otherwise lacks legal capacity in court proceedings. The Authority may intervene in the lawsuit to support the Data Subject's claim.

4. If the court upholds the claim, the Data Controller is required to provide information, correct, block, or delete the data, cancel the automated decision-making based on data processing, respect the Data Subject's right to object, and provide the data requested by the recipient.

5. If the court rejects the recipient's claim, the Data Controller must delete the Data Subject's personal data within three days of the notification of the judgment. The Data Controller must delete the data if the recipient does not take the matter to court within the specified period.

6. The court may order the publication of its judgment, including the Data

Controller's identification data, if this is required by data protection interests and the protected rights of a large number of affected individuals.

Compensation and Damages

1. If the Data Controller unlawfully processes the Data Subject's data or violates the data security requirements, it must compensate for any damage caused.

2. If the Data Controller unlawfully processes the Data Subject's data or violates the data security requirements, the Data Subject may claim damages from the Data Controller.

3. The Data Controller is liable for the damage caused by the Processor and must pay the damages owed for the violation of personality rights caused by the Processor. The Data Controller is exempt from liability for the damage and the obligation to pay damages if it proves that the damage or the violation of personality rights was caused by an unavoidable external factor.

4. No compensation is required, and no damages can be claimed if the damage was caused by or resulted from the intentional or grossly negligent conduct of the Data Subject.

Final Provisions

The preparation of this policy took into account the following legislation:

- Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (hereinafter: Information Act)
- Act CVIII of 2001 on Electronic Commerce and on Information Society Services (especially Section 13/A)
- Act XLVII of 2008 on the Prohibition of Unfair Commercial Practices against Consumers
- Act XLVIII of 2008 on the Basic Requirements and Certain Restrictions of Commercial Advertising Activities (especially Section 6)
- Act XC of 2005 on the Freedom of Electronic Information
- Act C of 2003 on Electronic Communications (specifically Section 155)
- Opinion No. 16/2011 on the EASA/IAB Best Practice Recommendation on Online Behavioral Advertising
- Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation) on the protection of natural persons regarding the processing of personal data and the free movement of such data, repealing Directive 95/46/EC.