

Privacy Policy

Privacy Policy



1. DATA CONTROLLER INFORMATION

Data Controller Information:

- Name: **Török Levente EV**
- Address: **1114 Budapest, Ulászló utca 27., Hungary**
- Tax number: **91367358-1-43**

Contact Information:

- Postal address: **1114 Budapest, Ulászló utca 27., Hungary**
- E-mail: **hello@togetherhands.hu**
- Phone: **+36 20 459 7722**

1.1. Purpose and Scope of the Notice

This privacy policy (hereinafter referred to as the "Policy") aims to define the usage regulations of the records/databases maintained by the Data Controller.

- Ensures the enforcement of constitutional principles of data protection, the right to informational self-determination, and the requirements of data security.
- Ensures that within the framework of legal regulations, everyone can manage their personal data, know the circumstances of their processing, and prevent unauthorized access, alteration, and disclosure.
- Provides information to the data subjects about the Data Controller's data processing practices.

1.2. Governing Legislation

- Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation, GDPR) 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.
- Act CXXXIII of 2005 on the rules of personal and property protection and private investigative activities (Sztvtv.).
- Act CXII of 2011 on the right to informational self-determination and freedom of information (Infotv.).
- Act I of 2012 on the Labour Code.
- Act XXXIV of 2019 (GDPR Amendment Act).
- The National Authority for Data Protection and Freedom of Information's (NAIH) guidelines on the basic requirements of workplace data processing (NAIH Guidelines).
- The NAIH's recommendations on the data protection requirements of prior information (NAIH Recommendations).
- Act LXXVI of 1999 on copyright.

1.3. Data Controller

According to the interpretive provisions of Act CXII of 2011 on the right to informational self-determination and freedom of information, a data controller is a natural or legal person, or an organization without legal personality, who or which, alone or jointly with others, determines the purposes of data processing, makes and executes decisions regarding data processing (including the means used), or has them executed by the data processor.

Data Controller Information:

- Name: **Török Levente EV**
- Address: **1114 Budapest, Ulászló utca 27., Hungary**
- Tax number: **91367358-1-43**

Contact Information:

- Postal address: **1114 Budapest, Ulászló utca 27., Hungary**
- E-mail: **hello@togetherhands.hu**
- Phone: **+36 20 459 7722**

2. DATA PROCESSING

2.1. Data Processors

A data processor may only process personal data of the data subject for the purpose defined and specified in a contract by the Data Controller, following the instructions of the Data Controller. The data processor has no independent decision-making authority regarding data processing. The data processor has committed to confidentiality and contractual guarantees to preserve the personal data it encounters while performing its tasks.

- **Accounting:** Codexalba Kft., 1107 Budapest, Gém utca 6. I. lház. 6. em. 5., codexalba@gmail.com
- **Cash on Delivery Checker:** Utánvét Ellenőr Ltd., 8640 Fonyód, Szigligeti Street 10., hello@utanvet-ellenor.hu
- **Billing:** KBÖSS.hu Kft., 1031 Budapest, Záhony utca 7/D., info@szamlazz.hu
- **Debt Collection:** Legal Labs Kft., 1054 Budapest, Honvéd utca 8. 1. em. 2., hello@payee.tech
- **Hosting Service Provider:** UNAS Online Kft., 9400 Sopron, Major köz 2.1/15, unas@unas.hu
- **Various Extra Functions (e.g., Newsletter Distribution):** M.I. Solution Kft., 2030 Érd, Esztergályos utca 57.

Logistics Service Providers:

- Boxy Zrt., 1036 Budapest, Lajos utca 48-66. C. ép.
- GLS Hungary Kft., Alsónémedi, GLS Európa u. 2, 2351
- Packeta Hungary Kft., Budapest Ezred utca 2 B2/11, 1044
- FoxPost Zrt, Váci út 60-62, 1044
- Magyar Posta Zrt., 1138 Budapest, Dunavirág utca 2-6.
- DPD Hungary Kft., 1134 Budapest, Váci út 33./2

2.2. Purpose, Duration, and Legal Basis of Data Processing

The Data Controller processes personal data based on the voluntary consent of the data subjects or statutory authorization.

Data providers must provide all requested data accurately to the best of their knowledge.

If the data provider does not provide their personal data, it is their duty to obtain the consent of the data subject.

The duration of data processing is the minimum data processing time specified by law.

Data Processing Activities of the Data Controller:

Online Sales

- **Legal Basis:** Consent of the data subject
- **Data Processed:** Name, email address, phone number, billing and shipping information
- **Purpose:** Ensure the online sales procedure
- **Data Transfer:** None
- **Data Deletion Deadline:** Minimum data retention period specified by law
- **Consequence of Lack of Data:** Purchase failure

Newsletter Subscription

- **Legal Basis:** Consent of the data subject
- **Data Processed:** Name, email address
- **Purpose:** Send digital materials and offers via email
- **Data Transfer:** None
- **Data Deletion Deadline:** Until withdrawal
- **Consequence of Lack of Data:** Failure to receive updates

Contact

- **Legal Basis:** Consent of the data subject / Legitimate interest
- **Data Processed:** Sender's name, address, email address, phone number, contact date, attachments
- **Purpose:** Provide information, data disclosure, and proof of consent
- **Data Transfer:** In case of an incident, as defined by law
- **Data Deletion Deadline:** 3 years
- **Consequence of Lack of Data:** Inability to prove data disclosure/information/consent

Customer Satisfaction Measurement

- **Legal Basis:** Consent of the data subject
- **Data Processed:** Gender, age, education level, interests, purchase date, purchase method, service usage method
- **Purpose:** Measure satisfaction related to services/products to ensure further development
- **Data Transfer:** None
- **Data Deletion Deadline:** Data stored in an unidentifiable form until business interest is realized, up to 10 years
- **Consequence of Lack of Data:** Inaccurate needs assessment for further developments

If the Data Controller or data processors transfer data to third parties, they maintain a record of the data transfer. The data transfer record must include the recipient, method, time, and scope of the transferred data.

2.3. Handling Overdue Debts of Clients with Levente Török (Sole Proprietor) (Debt Collection)

During the debt collection process (via SMS, electronic and postal mail, telephone conversations), Levente Török (Sole Proprietor) processes the client's personal data, which were voluntarily provided by the client within the framework of the contractual relationship serving as the basis for the debt, or recorded according to legal provisions. As part of the debt collection procedure, Levente Török (Sole Proprietor) may transfer personal data to an external debt collection partner for the enforcement of overdue claims in accordance with Section 161 (1) (c) and Section 164 (q) of Act CCXXXVII of 2013. The appointed representative for debt collection of Levente Török (Sole Proprietor) is a notary public of MOKK.

The following data may be transferred to the representatives handling debt collection:

Personal Data of the Client:

- Name

- Mother's name
- Birth name
- Place and date of birth
- ID card number
- Address
- Notification address
- Phone number
- IP address used at the time of order

Debt Information:

- Currency
- Principal amount
- Overdue principal
- Overdue interest
- Other charges
- Breakdown of late fees
- Number of days overdue
- Date of default
- Contractual and default interest rates

The debt collection agents of Levente Török (Sole Proprietor) are notaries public of MOKK, who can be publicly queried in the register.

Legal Basis of Data Processing: The legal basis for data processing is provided by Article 6 (1) (b) of the GDPR.

The processed data originates from:

- Order details
- Client declarations
- Records of Levente Török (Sole Proprietor)

Duration of Data Processing:

The duration of data processing extends until the end of the debt collection, that is, until 8 years after the termination of the client relationship. If the debt still exists and has not expired, processing continues until the expiration of the statute of limitations.

2.4. Information on Extra Features

The website <http://www.enszobrom.hu> utilizes the M.I. system (M.I. Solution Kft., Hungary, 2030, Érd, Esztergályos utca 57., www.miclub.hu) to enhance customer experience and provide more effective information. This system employs text files stored on your computer (cookies). These cookies store activities (clicks) performed on our online store platform. Through the software and cookies used, we estimate which of our products or services may interest you, enabling us to send automated emails with informative content tailored to your interests.

If you do not wish to receive such emails or do not want us to track your activities for these purposes, please click on the "unsubscribe" link found in any email footer. This action will immediately stop the sending of automated emails and tracking of your activities on our website.

2.5. Information regarding the Cash on Delivery Checker

The Webshop sends the success of the product delivery (whether the order was received or not) and the hashed email address (using the SHA256 algorithm) of the Individual to the Cash on Delivery Checker service, where the Service Provider stores these data and sends them to other webshops that use the service for manual or automated querying.

How does the Cash on Delivery Checker work?

- It stores user habits (outcome of orders), hashed email addresses (hashed from email addresses using SHA256), phone numbers, and shipping addresses.
- It combines these with data received from other webshops in response to manual or automated queries.

Result of the Legitimate Interest Assessment

The Data Controller conducted a legitimate interest assessment, and the results indicated that the data processing restricts the legitimate interest of the Individuals in a proportionate manner. Processing the personal data of Individuals is essential for safeguarding the assets of the Webshop as the Data Controller and ensuring the related rights of the Individual. Currently, there are no alternative data processing solutions available that involve less personal data or different methods.

The Data Controller, as the Seller, uses certain personal data of Individuals who have entered into a contract with them (purchasing on the website) when using the Cash on Delivery Checker service, aiming to reduce damages caused by breach of contract. Therefore, as a customer of the Webshop, the Individual can expect the possibility of the application of the Cash on Delivery Checker service based on this information. The application of the Cash on Delivery Checker service by the Webshop does not involve more data collection or disclosure than what the Individual provided to the Webshop during their order (e.g., name, ordered goods).

The Data Controllers aim to protect their interests legally, socially, and economically recognized, and the personal data processing is purpose-bound. They handle personal data with consideration for the principle of data minimization. During data processing, they do not collect any special categories of data under any circumstances.

The Data Controllers provide all necessary and expected support for Individuals to exercise their rights.

In summary, the Data Controllers conduct data processing in a lawful, fair, and transparent manner.

The purpose of this information is to inform you about the processing of personal data when using the Cash on Delivery Checker.

The Joint Data Controllers jointly prepared the information for Individuals, defining the distribution of responsibilities for fulfilling obligations under the GDPR in the agreement reached between them.

2.6. Further Data Processing

Should the Data Controller wish to conduct additional data processing activities, prior information will be provided regarding the essential circumstances of the data processing:

- Legal background and basis of the data processing
- Purpose of the data processing
- Scope of the processed data
- Duration of the data processing

Please be informed that the Data Controller is obliged to comply with written data requests from authorities based on legal authorization. In accordance with Section 15 (2)-(3) of the Information Act (Infotv.), the Data Controller maintains a record of data transfers (to which authority, which personal data, based on what legal basis, and when the Data Controller transmitted the data), and upon request, provides information about the content of this record, except where prohibited by law.

3. DATA HANDLING, STORAGE METHODS, AND SECURITY

We handle data confidentially in accordance with legal requirements.

We only contact users for matters they have approved. Phone conversations are not recorded.

The Data Controller stores the data it manages, both in paper and electronic form, at the following location: HU-1114 Budapest, Ulászló utca 27.

The Data Controller uses an IT system for its operations that ensures data:

- Integrity can be verified (data integrity);
- Authenticity is ensured (authenticity of data processing);
- Is accessible to authorized persons (availability);
- Is protected against unauthorized access (data confidentiality).

The Data Controller and its data processors always provide protection against fraud, espionage, viruses, hacking, vandalism, and natural disasters targeting their IT systems. The Data Controller (or data processor) employs server-level and application-level security procedures.

Messages sent to the Data Controller over the internet – in any form – are particularly vulnerable to network threats that could lead to data modification, unauthorized access, or other illegal activities. The Data Controller takes all reasonably possible and expected measures to prevent such dangers.

Please provide the next part of the text for further translation.

4. ANALYTICS AND COOKIES

Cookies are small data packets stored by internet services in your browser. The TOGETHERHANDS.HU website uses cookies to optimize user experience. Users can delete these cookies from their computer or browser at any time. However, if the user does not accept cookies, we cannot guarantee the website will function properly. Detailed information on cookie usage is provided in our Cookie Policy.

Cookie Usage Information

- **About Cookies:** The Data Controller uses cookies during the visit to the website. A cookie is a package of information consisting of letters and numbers that our website sends to your browser to save certain settings, facilitate the use of our website, and assist in collecting some relevant statistical information about our visitors.
- **Legal Background and Basis of Cookies:** The background of data processing is provided by Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (Infotv.) and Act CVIII of 2001 on Certain Issues of Electronic Commerce Services and Information Society Services. The legal basis of data processing is your consent in accordance with Section 5 (1) (a) of Infotv.
- **Cookies Strictly Necessary for Operation:** These cookies are essential for the use of the website and allow for the basic functions of the website to be used. Without these, many features of the site will not be available to you. The lifespan of these types of cookies is limited to the duration of the session.
- **Cookies for Improving User Experience:** These cookies collect information about how users use the website, such as which pages they visit most often or what error messages they receive from the website. These cookies do not collect information that identifies the visitor; they work with completely general, anonymous information. The data obtained from these cookies is used to improve the performance of the website. The lifespan of these types of cookies is limited to the duration of the session.
- **RTB Personalized Retargeting Cookies:** These cookies may appear for previous visitors or users while browsing other websites on the Google Display Network or searching for terms related to your products or services.

Cookies used on TOGETHERHANDS.hu:

- **Facebook pixel:** This cookie allows us to track visitor activities on Facebook and display targeted ads.
- **TikTok pixel:** Similar to the Facebook pixel, it tracks visitor activities on the TikTok platform.
- **Google Analytics:** This cookie collects statistical data about website traffic and usage to better understand user behavior and optimize website performance.

- **Hotjar cookie:** The Hotjar cookie helps us analyze user behavior on the website to better understand how visitors navigate the site, enabling potential improvements in user experience.
- **RTB personalized cookies:** These cookies gather information for online advertising platforms to display personalized ads to users based on their activities on Énszobrom.hu.
- **PREFIBOX personalized cookies:** These are cookies from the Prefibox platform, enabling personalized advertising to users on the site.

These cookies help us tailor content and ads on Énszobrom.hu more effectively. Please note that typically your consent is required for the use of these cookies, and you can usually manage them by clicking on "cookie settings" or similar button in the footer of the website.

If you do not accept the use of cookies, certain features will not be available to you. For more information on deleting cookies, please visit the following links:

- [Internet Explorer](#)
- [Firefox](#)
- [Chrome](#)

5. EMBEDDED CONTENT FROM OTHER WEBSITES

The TOGETHERHANDS.HU website may include embedded content from external sources (e.g., videos, images). These embedded contents behave exactly as if you had visited the other website.

These external websites may collect data about visitors, use cookies, or employ third-party tracking codes. The Data Controller is not responsible for the data and information protection practices or policies of these external sites.

If the Data Controller becomes aware that an external site is violating applicable laws or engaging in harmful behavior, it will immediately remove the links to such sites from its page.

6. RIGHTS OF DATA SUBJECTS AND LEGAL REMEDIES

Data subjects can request information in writing from the Data Controller at any time regarding how their personal data is processed, request deletion or modification of their data, and withdraw their previously given consent.

Data subjects cannot exercise their right to deletion in cases where data processing is mandatory by law.

a) Right to Information: Upon request, the Data Controller will provide data subjects with concise, understandable information about the processing of their personal data, as specified in Articles 13 and 14, and notifications according to Articles 15-22 and 34 of the GDPR.

b) Right of Access: Data subjects can request confirmation from the Data Controller regarding whether their personal data is being processed. If such processing is taking place, the data subject has the right to access the following information:

- Their personal data
- The purpose(s) of data processing
- The categories of personal data concerned
- The recipients to whom the data has been or will be disclosed
- The period for which the data will be stored
- The right to request rectification, erasure, or restriction of processing
- The right to lodge a complaint with a supervisory authority
- The source of the data
- Any automated decision-making, including profiling, and its significance and consequences
- The transfer of data to a third country or international organization

The Data Controller will provide a copy of the requested data. Additional copies will incur an administrative fee of 500 HUF per page. The data will be provided within 30 days of receiving the request.

c) Right to Rectification: Data subjects can request the correction of inaccurate personal data processed by the Data Controller.

d) Right to Erasure: Data subjects can request the deletion of their personal data if any of the following conditions are met:

- The data was processed unlawfully
- The data is no longer necessary for the original purpose
- The data subject withdraws their consent, and there is no other legal basis for processing
- The data was collected in connection with information society services
- The data must be erased to comply with a legal obligation

The Data Controller cannot delete data if processing is necessary for:

- Compliance with legal obligations
- Exercising the right to freedom of expression and information
- Reasons of public interest
- Archiving, research, or statistical purposes
- Establishment, exercise, or defense of legal claims

e) Right to Restriction of Processing: Data subjects can request restriction of processing if:

- They contest the accuracy of the data, for a period enabling verification
- The processing is unlawful, but they oppose erasure and request restriction instead
- The Data Controller no longer needs the data, but they require it for legal claims

During the restriction period, the Data Controller will only process the data with the data subject's consent or for legal claims.

f) Right to Withdraw Consent: Data subjects can withdraw their consent at any time in writing. The Data Controller will promptly and permanently delete all data related to the data subject unless required by law or necessary for legal claims. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal.

g) Right to Data Portability: Data subjects can request the transfer of their data in a commonly used, machine-readable format to another data controller. This request will be fulfilled within 30 days.

h) Right to Object to Automated Decision-Making and Profiling: Data subjects have the right not to be subject to decisions based solely on automated processing, including profiling, if it affects them legally or significantly. This right does not apply if:

- Processing is necessary for a contract between the data subject and the Data Controller
- The data subject has given explicit consent
- Processing is authorized by law
- Processing is necessary for legal claims

7. PROCEDURAL RULES

If the Data Controller receives a request under Articles 15-22 of the GDPR, the Data Controller will inform the data subject in writing about the measures taken based on the request as soon as possible, but no later than 30 days.

If the complexity of the request or other objective circumstances justify it, the above deadline can be extended once by a maximum of 60 days. The Data Controller will inform the data subject in writing of the extension, along with a justification for the extension.

The Data Controller provides the information free of charge, except in the following cases:

- The data subject repeatedly requests information/actions on essentially unchanged content.
- The request is clearly unfounded.
- The request is excessive.

If the requester asks for the data to be provided on paper or electronic media (CD or DVD), the Data Controller will provide one copy of the data free of charge in the requested format (unless the chosen platform would cause a disproportionate technical difficulty). For any additional copies, an administrative fee of 500 HUF per page/CD/DVD will be charged.

The Data Controller will respond to the request in electronic form unless:

- The data subject explicitly requests a different method, and it does not cause an unreasonably high additional cost for the Data Controller.
- The Data Controller does not know the data subject's electronic contact details.

8. LEGAL REMEDIES

If you notice any objectionable issue related to data processing, please report it immediately via one of the contact methods provided in section 4.

If the data subject believes that their rights have been violated by the Data Controller and/or the data processors, they have the right to go to the competent court.

If the data subject wishes to file a complaint regarding data processing, they can do so with the National Authority for Data Protection and Freedom of Information at the following contact details:

- Address: 1125 Budapest, Szilágyi Erzsébet fasor 22/C.
- Mailing address: 1530 Budapest, Pf.: 5.
- Phone: +36-1/391-1400; fax: +36-1/391-1410
- Email: ugyfelszolgalat@naih.hu
- Website: www.naih.hu

9. COOPERATION WITH AUTHORITIES

If the Data Controller receives an official request from authorized authorities, it is obliged to hand over the specified personal data.

The Data Controller will only transfer data that is absolutely necessary to achieve the goal specified by the requesting authority.

Please provide the next part of the text for further translation or let me know if you need any other assistance.

10. PRINCIPLES OF COLLECTING AND DISPLAYING CUSTOMER REVIEWS

Impartial Reviews: Reviews are collected from consumers without offering any form of consideration (such as purchase discounts or coupons).

Indication of Actual Purchase Quality: For reviews originating from consumers who have actually purchased the product, this fact is clearly marked alongside the review.

Not Just Product Reviews: Reviews may pertain not only to the product itself but also to our online store. This distinction is particularly relevant in cases of reviews provided solely with star ratings, without accompanying text.

Diversity of Reviews: We do not selectively publish only positive reviews; a range of reviews, both positive and critical, are displayed.

Searchability of Reviews: We enable consumers to search through reviews based on various parameters (chronological order, best/worst ratings).

Prohibition of Fake Reviews: It is strictly prohibited to submit fake consumer reviews or endorsements into our system for the

promotion of our products, nor can third parties be commissioned to do so.

Criteria for Deleting Reviews: We delete consumer reviews that violate any of the following prohibitions:

- Advertising products/services is prohibited.
- Displaying information related to third-party intellectual property rights (such as brand names, trade names) is prohibited.
- Using hate speech, xenophobic, obscene, offensive, aggressive, threatening, fear-inducing, or hate-provoking discriminatory language is prohibited.
- Displaying personal data (such as names, email addresses, phone numbers) in consumer reviews is prohibited.

Note to Consumers Writing Reviews:

We kindly request consumers writing reviews to consider the following recommendations:

- Ensure the review contains accurate information and assists other consumers in making informed purchasing decisions.
- Describe both the advantages and disadvantages of the reviewed product (technical quality, aesthetic appearance, etc.).
- Include personal usage experiences and any suggestions or ideas for product improvement.
- Focus the review exclusively on the product itself, rather than on associated services (delivery, product availability, etc.) or sellers.

How We Collect Consumer Reviews

Our online store gathers consumer reviews through the following method(s):

- **Direct Email Requests from Actual Buyers:** Following the purchase, our online store contacts consumers via email after 1, 2, and 7 days to invite them to review the purchased product. Submitting a review is voluntary, and consumers do not gain any financial or other benefits from submitting reviews.
- **Google Reviews**
- **Facebook Reviews**
- **Trustindex**
- **Árukereső**
- **OnlinePénztárca**

This Privacy Policy is valid until revoked.