

DATA PROCESSING NOTICE

Regarding the data processing related to the operations of iDOM HÁZÉPÍTŐ KFT.

iDOM Házépítő Kft. is a business entity engaged in construction industry services, and provides the following information regarding data processing related to its operations:

Data Controller Name: iDOM Házépítő Kft.
Data Controller Registration Number: Cg.01-09-202048
Data Controller Registered Office: 1037 Budapest, Bóbita utca 2. II. floor
Data Controller Electronic Contact: info@idomhazak.hu
Data Controller Representatives: Gergő Tikos, CEO

- **DATA PROCESSING**

- 1. Data processing related to the conclusion and maintenance of contracts for legal entities (B2B)**

Purpose of data processing: Conclusion and maintenance of contracts with business partners.

Legal basis for data processing: Your consent (Article 6(a) of regulation (EU) 2016/679).

Scope of processed data:

Processed data	Purpose of data processing
Full name of the contact person	contacting
Contact person's email address	contacting
Contact person's phone number	contacting

Data retention period: until the termination of the contractual relationship.

Possible consequences of failing to provide data: the contract will not be concluded.

- 2. Data processing related to the conclusion and maintenance of contracts for individuals**

Purpose of data processing: Conclusion and maintenance of contracts with individual business partners.

Legal basis for data processing: Performance of the contract (as per Article 6(1)(b) of Regulation (EU) 2016/679).

Data processed:

Processed data	Purpose of data processing
Full name	Contact, identification
Address	Contact, identification
Mother's name	identification
Place and date of birth	identification
Birth name	identification
Tax identification number	invoicing
Bank account number	payment

Data processing duration: Until the termination of the contractual relationship, for billing-related data, 8 years.

Consequences of failure to provide data: The contract will not be established.

3. Data Processing related to marketing communication (Newsletter)

Purpose of data processing: To create effective marketing communication and send personalized messages to the data subject based on their behavior on the Data Controller's platforms.

Legal basis for data processing: Your consent (according to Article 6(a) of EU Regulation 2016/679).

Scope of processed data:

Processed data	Purpose of data processing
Full name	User identification
E-mail	Personalized communication
Phone number	Contact
Permanent address	Contact, factors considered during personalized communication
Postal address	Contact

Data processing duration: until the withdrawal of consent.

Possible consequences of failure to provide data: the data subject will not receive personalized service and promotions from the Data controller.

4. data processing related to participation in events organized by the data controller or other organizers

Purpose of data processing: to effectively serve the data subjects at events, document the events, promote the events on the data controller's online platforms, and collect contacts during the events.

Legal basis for data processing: Your consent (according to article 6(a) of Regulation (EU) 2016/679), which also extends to the unlimited use of photographs and video recordings of the data subject by the data controller.

Scope of processed data:

Processed data	Purpose of data processing
Name of the event	ensuring entry on the appropriate event day
Full name	identifying the user
E-mail	personalized communication
Place of birth	aspect considered during personalized communication
Date of birth	aspect considered during personalized communication
Phone number	aspect considered during personalized communication
Other data provided during event registration	ensuring access on the appropriate event day
Photographs and video recordings	documentation and promotion of the event

Data processing duration: Until the withdrawal of consent.

Possible consequences of not providing data: The data subject will not receive efficient service, and the documentation and promotion of events will not be possible.

5. Data processing related to contact initiation

Purpose of data processing: Contact initiation through the website or other means, request for quotes

Legal basis for data processing: Your consent (according to Article 6(1)(a) of Regulation (EU) 2016/679).

Scope of processed data:

Processed data	Purpose of data processing
Full name	user identification
E-mail	user identification
Address	contact
Phone number	contact

Data processing duration: 30 days following the response to the query, or 8 days after the validity period of the offer in the case of an offer.

Possible consequences of failure to provide data: The data subject will not receive a response to their questions or will not be able to request an offer.

6. Data processing related to recruitment

Purpose of data processing: Filling vacant positions through job offers with employees and subcontractors.

Legal Basis for Data Processing: Your consent (according to Article 6(a) of Regulation (EU) 2016/679).

Scope of processed data:

Processed data	Purpose of data processing
Full name	user identification
E-mail	user identification
Address	contact
Phone number	contact

Any other personal data provided on the CV or cover letter	Application evaluation
Reference-related data	Evaluation of the application

Data processing duration: After the application evaluation, within 5 days of notifying the result; in case of a successful application, until the termination of the employment/subcontractor relationship; if the data subject separately consents for their CV and application materials to be stored by the data controller for up to 5 years after the evaluation, the consent is valid until withdrawal, but for a maximum of 5 years.

Possible consequences of failure to provide data: The data subject will not be able to apply.

Data Processing

The Data Controller is entitled to engage a data processor for certain technical operations or for the purpose of providing services in accordance with applicable laws. The data processor is authorized only to follow the instructions and decisions of the Data Controller.

Rights of the Data Subject

The data subject has the right to request information about the processing of their personal data, to request correction of their personal data, to request deletion of their data via email at info@idomhazak.hu, to request the restriction of processing, and is entitled to data portability and legal remedies. In case of a complaint, the data subject can turn to the National Authority for Data Protection and Freedom of Information in Hungary or, at their choice, to a court. In legal proceedings, the court has jurisdiction.

- **Information and access to personal data**

The Data Subject has the right to know the personal data stored by the Data Controller and information related to its processing; to verify which data the Data Controller holds about them, and is entitled to access their personal data. The data subject must submit their request for access to personal data in writing (via email or postal mail) to the Data Controller. The Data Controller will provide the information in a widely used electronic format, unless the data subject requests it in writing, on paper. The Data Controller will not provide verbal information over the phone when exercising the right of access.

When exercising the right of access, the information provided will cover the following:

- definition of the scope of processed data, the purpose, duration, and legal basis for processing the data
- data transfers: to whom the data has been transferred or will be transferred in the future
- identification of the data source.

The Data Controller provides the first copy of the personal data (in person at the customer service desk) free of charge to the Data Subject. For any additional copies requested by the Data Subject, the Data Controller may charge a reasonable fee based on administrative costs. If the Data Subject requests the copy electronically, the information will be provided by the Data Controller via email in a commonly used electronic format.

Following the information, if the Data Subject disagrees with the processing of their personal data or its accuracy, they may request the correction, supplementation, deletion, or restriction of processing of their personal data, object to the processing of such personal data, or initiate the procedure defined in section V as described in points III. 1.-6.

- **The right to rectification or supplementation of processed personal data.**

Upon the Data Subject's written request, the data controller shall rectify the inaccurate personal data or supplement the incomplete data specified by the data subject in writing or in person at one of the data controller's premises, without undue delay. The data controller will inform any recipients of the corrected or supplemented data, except when it is impossible or requires disproportionate effort. The data subject will be informed of these recipients if they request this information in writing.

- **Right to restriction of processing**

The Data Subject may request the restriction of the processing of their data from the data controller in writing if:

- The data subject disputes the accuracy of the personal data; in this case, the restriction applies for the period that allows the data controller to verify the accuracy of the personal data.
- The processing is unlawful, and the data subject objects to the deletion of the data and instead requests the restriction of its use.
- The data controller no longer needs the personal data for the purposes of processing, but the data subject requires it for the establishment, exercise, or defense of legal claims.
- The data subject objects to the processing; in this case, the restriction applies for the period until it is determined whether the data controller's legitimate grounds override those of the data subject.

If the Data Subject's objection is well-founded, the data controller shall restrict the data, meaning that only storage as data processing may take place until

- the data subject gives consent to the processing of personal data;
- the processing of personal data is necessary for the establishment, exercise, or defense of legal claims;
- the processing of personal data is necessary for the protection of the rights of another natural or legal person;
- processing is required by law in the public interest.

If the Data Subject requested the restriction of processing, the data controller will inform the Data Subject in advance about the lifting of the restriction.

- **The right to erasure (right to be forgotten)**

At the request of the Data Subject, the Data Controller shall erase the personal data related to the Data Subject without undue delay if any of the following grounds apply:

- the personal data is no longer necessary for the purposes for which it was collected or otherwise processed by the Data Controller;
- The Data Subject withdraws their consent upon which the processing is based, and there is no other legal ground for processing;
- the Data Subject objects to the processing based on their particular situation, and there are no legitimate grounds for processing;
- the Data Subject objects to the processing of their personal data for direct marketing purposes, including profiling, to the extent that it is related to direct marketing;
- the personal data is being processed unlawfully by the Data Controller;
- the personal data was collected in connection with the offering of information society services directly to children.

The Data Subject may not exercise the right to erasure (right to be forgotten) if the processing is necessary:

- for the exercise of the right to freedom of expression and information;
- based on public interest in the area of public health;
- for purposes of public interest archiving, scientific and historical research, or statistical purposes, where the exercise of the right to erasure would make this processing impossible or seriously jeopardize it; or
- for the establishment, exercise, or defense of legal claims.

Right to data portability

Data portability allows the Data Subject to obtain and further use their "own" data provided to the Data Controller within the Data Controller's system, for their own purposes and through various service providers they choose. In all cases, the right is limited to the data provided by the Data Subject, and there is no possibility of portability for other data (e.g., statistics, etc.).

The Data Subject can request the following personal data related to them, available in the Data Controller's system (e.g., during newsletter subscription):

- receive the data in a structured, widely used, machine-readable format;
- have the right to transfer the data to another data controller;
- request the direct transfer of the data to another data controller – if technically feasible within the Data Controller's system.

The Data Controller will fulfill the data portability request solely based on a request submitted via email or postal mail. To fulfill the request, the Data Controller needs to ensure that the Data Subject, who is entitled to exercise this right, is indeed the one making the request. For this, the Data Subject must appear in person at the Data Controller's headquarters following the notification, so that the Data Controller can identify the requesting Data Subject using the data in its system. The Data Subject can request the portability of the data they provided to the Data Controller. The exercise of this right does not automatically result in the deletion of the data from the Data Controller's systems. Therefore, even after exercising this right, the Data Subject's data will remain recorded in the Data Controller's systems unless the Data Subject also requests its deletion.

- **Objection to the processing of personal data**

The Data Subject may object to the processing of their personal data by submitting a statement to the Data Controller if the legal basis for the processing is:

- Public interest according to Article 6(1)(e) of the GDPR; or
- Legitimate interest according to Article 6(1)(f) of the GDPR.

If the Data Subject exercises the right to object, the Data Controller may not continue processing the personal data unless the Data Controller demonstrates that there are compelling legitimate grounds for the processing that override the interests, rights, and freedoms of the Data Subject, or that the processing is necessary for the establishment, exercise, or defense of legal claims. The decision on whether the processing is justified by compelling legitimate grounds will be made by the Data Controller's managing director. The Data Controller will inform the Data Subject of this decision in writing.

The Data Subject may object in writing (via email or postal mail).

REQUEST FULFILLMENT DEADLINE, PROCEDURAL RULES

The Data Controller will inform the Data Subject about the actions taken without undue delay, but in any case, within one month from the receipt of any request specified in points III. 1-6. If necessary, considering the complexity of the request and the number of requests, this deadline may be extended by a further two months. However, in such cases, the Data Controller will inform the Data Subject within one month of receiving the request, indicating the reasons for the delay, and also informing the Data Subject that they have the right to lodge a complaint with the supervisory authority and seek judicial remedy.

If the request of the Data Subject is clearly unfounded or excessive (especially with regard to its repetitive nature), the Data Controller may charge a reasonable fee for fulfilling the request or refuse to take action on the request. The burden of proving this lies with the Data Controller.

If the Data Subject submitted the request electronically, the Data Controller will provide the information electronically unless the Data Subject requests otherwise.

The Data Controller will inform all recipients with whom the personal data has been shared about any corrections, deletions, or restrictions on processing, unless this proves impossible or requires disproportionate effort. Upon the request of the Data Subject, the Data Controller will inform them of these recipients.

LEGAL REMEDIES

The Data Subject may exercise their rights by submitting a written request via email or postal mail to the Data Controller.

The Data Subject cannot exercise their rights if the Data Controller proves that it is unable to identify the Data Subject. If there is doubt regarding the identity of the individual submitting the request, the Data Controller may request additional information necessary to confirm the identity of the applicant.

The Data Subject has the right to enforce their rights under the Info Act, the Regulation, and the Civil Code (Act V of 2013).

- They may turn to the National Authority for Data Protection and Freedom of Information (1055 Budapest, Falk Miksa Street 9-11; www.naih.hu); or
- They may enforce their rights before a court.

COMPENSATION AND DAMAGES

Any person who has suffered material or non-material damage as a result of a violation of the Regulation is entitled to compensation for the damage from the Data Controller or the data processor. The data processor is only liable for the damage caused by the data processing if it has not complied with the obligations specifically imposed on data processors by law, or if it disregarded or acted contrary to the lawful instructions of the Data Controller. The Data Controller or the data processor is exempt from liability if it proves that it is not responsible for the event causing the damage in any way.

HANDLING DATA PROTECTION INCIDENTS

A data protection incident is a security breach that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or unauthorized access to personal data that is transmitted, stored, or otherwise processed. The Data Controller keeps a record for monitoring actions related to the data protection incident, notifying the supervisory authority, and informing the Data Subject, which includes the scope of personal data affected by the incident, the scope and number of data subjects, the time, circumstances, impacts, and measures taken to address the incident. In the event of an incident, the Data Controller must inform the Data Subject and the supervisory authority of the data protection incident without undue delay, and within 72 hours at the latest, unless the incident does not pose a risk to the rights and freedoms of natural persons.

SECURITY BACKUP HANDLING PROCEDURES

The Data Controller, as part of its IT security duties, ensures the implementation of measures that allow for the restoration of data, including regular backups and the secure handling of copies (backup) in a separate and secure manner.

Accordingly, the Data Processor – in order to prevent the loss of electronically stored data – regularly creates backups of the personal data contained in its database three times a day on a separate storage medium.

Retention period of backups: 5 years

Deletion procedure for backups: Individual deletions are trackable in an anonymized register, while automatic deletions occur according to settings.

Access to backups: Access to backups is restricted, and only individuals with specified permissions can access them. Data access is granted only after appropriate identification (at least username and password).

OTHER PROVISIONS

The Data Controller reserves the right to unilaterally modify this Privacy Notice. The modifications will come into effect on the date specified in the notification, unless the Data Subject objects in writing to the changes.

If the Data Subject has provided third-party data for the use of the service and caused damage, the Data Controller is entitled to enforce compensation against the Data Subject.

The Data Controller does not verify the personal data provided to it. The person who provided the data is solely responsible for the accuracy of the information. By providing the data, the Applicant assumes responsibility for ensuring that they have the proper legal grounds for providing the personal data of the contact person and that they have informed the employee of the required notification under the Regulation before transmitting the data to the Data Controller.

Effective date of this Privacy Notice: August 25, 2021.