

# **PRIVACY POLICY**

## **of KÁRÁSZY Commercial and Service Limited Liability Company**

### **Preamble**

*Kárászy Kft.* („Data Controller”) as the operator of *karsus.com*, declares that it processes personal data in accordance with the Fundamental Law of Hungary, Act 112 of 2011 on Informational Self-determination and Freedom of Information and Regulation (EU) no. 2016/679 of the European Parliament and of the Council of 27 April 2016 (“GDPR”).

The Data Controller respects the personal and confidential information of the visitors and registered users of the website. It shall treat and process all data and facts that come to its knowledge as confidential and such data is processed solely on the basis of performance of a contract, legal obligation, its own legal interest with respect to the data subject's interests and their consent based on prior information.

The data processing of *karsus.com* is carried out exclusively by *Kárászy Kft.* Personal data is disclosed to third parties only for the purpose of courier services, and only with the express consent of the data subject, which is deemed to be given by placing an order for the service. If a competent authority requests *Kárászy Kft.* to provide or disclose data, the company is obliged to release personal data, provided that all legal conditions for such disclosure are met.

### **Legality of data processing**

Its data processing principles are in accordance with the applicable data protection laws and regulations.

Processing shall be lawful only if and to the extent that at least one of the following applies:

- (i) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- (ii) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- (iii) processing is necessary for compliance with a legal obligation to which the controller is subject;
- (iv) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- (v) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- (vi) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

### **Principles of data processing**

The processing of personal data is carried out by the Data Controller by following the below principles at all times:

We carry out data processing lawfully, fairly, and in a transparent manner for the data subject.

During data processing, we adhere to the principle of data minimisation, meaning that the data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

Data processing must be accurate and, where necessary, kept up to date. In this regard, we take all reasonable measures to ensure that inaccurate data is promptly deleted or rectified.

Personal data is stored for a limited period, only as long as necessary for the purpose of processing.

During the processing of personal data, we ensure protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

We process personal data only for the purposes and in the manner specified in our Data Protection Policy, and for the exercise of rights and fulfilment of obligations defined therein. At every stage of the data processing, it must comply with these purposes.

We only process personal data that is essential for the realisation of the purpose of the data processing, suitable for achieving the purpose, and only to the extent and for the duration necessary for fulfilling the purpose.

In particular, we process personal data when it is necessary for the protection of the vital interests of the data subject, for the performance of a contract concluded between the data subject and the Data Controller, or for the legitimate interests pursued by the Data Controller or a third party.

### **Information provided to data subjects**

By the issuance of present Privacy Policy, we make adequate steps in order to ensure that the information addressed to the data subjects is handed over in a way that is concise, easily accessible and easy to understand in a clean and plain language.

By adopting our Data Protection Policy, publishing this statement, preparing a summary privacy notice and individual information sheets, as well as displaying informational signage, we fulfil our obligation to provide information to data subjects.

**Our employees, partners, and service providers are bound by the obligation of confidentiality towards us.**

### **Definitions:**

1. **Data security:** a comprehensive system of technical, personnel, and organizational measures and procedures implemented to protect the security criteria of data, such as confidentiality, integrity, and availability.
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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
3. **Data controller:** means 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;
4. **Processing:** the execution of the technical tasks relating to data processing, regardless of the used technique and instrument, or the place of processing, where the technical task is performed on personal data;
5. **Data processor:** a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
6. **Destruction of data:** the total physical destruction of the data medium on which the data are stored;
7. **Erasure of data:** making data unrecognizable in such a way that their recovery is no longer possible;
8. **Transfer of data:** making the data available to certain third parties;
9. **Data locking:** The marking of data with an identifier for the purpose of permanently or temporarily restricting its further processing;

10. **Personal data breach:** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
11. **Biometric data:** personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
12. **Confidentiality (Secrecy):** The characteristic of data that allows access only to a predefined group of users (authorized individuals), with all other access being illegal;
13. **Loss of Confidentiality:** The loss of confidentiality is referred to as disclosure, where confidential data becomes known and/or accessible to unauthorized individuals;
14. **Security Incident:** Any event that may negatively affect the confidentiality, integrity, or availability of IT equipment or the data stored on it;
15. **Data concerning health:** personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;
16. **GDPR:** General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016);
17. **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;
18. **Third party:** a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;
19. **Consent:** any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
20. **Info Act:** Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information.;
21. **Publicly Accessible Part of Private Property:** A part of private property that is freely accessible to the public, including parts of public areas under the possession of someone performing personal and property protection activities based on a civil law contract (e.g., lease), provided that:  
a) its use is directly related to and supports the activities taking place on the publicly accessible part of the protected private property, or  
b) it serves for the placement of movable property by either the data controller or the public using the publicly accessible part of the private area;
22. **Disclosure:** Making data accessible to anyone;
23. **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, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
24. **Integrity:** The criterion of the existence, authenticity, accuracy, and completeness of data, ensuring that data, information, or programs can only be altered by authorized individuals and cannot be changed unnoticed.
25. **Policy:** The data controller's data protection policy;
26. **Personal data:** any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to

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

27. **Objection:** A statement by the data subject objecting to the processing of their personal data and requesting the termination of data processing or the deletion of the data;
28. **Company:** The Data Controller, unless the context clearly indicates that the Company acts only as a data processor or does not perform data processing.
29. **Property Protection Security System:** An electronic alarm and video surveillance system installed on properties under the territorial scope of the Data Protection Policy for property protection purposes, including systems used solely for observation without recording, as well as systems enabling sound or image recording (surveillance), electronic access control systems, intrusion detection systems, remote monitoring systems, IT and data protection systems, and other electronic technical solutions enabling signal or image transmission, or light and sound signaling;
30. **Guest:** A natural person staying with permission on properties under the territorial scope of the Data Protection Policy, who is not an employee of the Data Controller.

### Data processing based on consent [GDPR Article 6 Section 1 paragraph a)

Through our website [karsus.com](https://karsus.com), we request the consent of visitors for the purpose of sending targeted promotional messages (newsletters).

By giving consent, the Data Subject agrees to the processing of their name and email address until the consent is withdrawn. After withdrawal of consent, the Data Subject's data will be deleted from our records.

In the case of targeted advertising (e.g., newsletter subscription), the legal basis for data processing is the Data Subject's consent, given based on prior information.

### Access, Use, and Transmission of Data

Personal data stored about Data Subjects may only be accessed by individuals whose duties require such access. The name of the person handling or otherwise authorized to access the personal data, as well as the reason and time of access, must be recorded in a log.

Use is defined as the situation where personal data is used as evidence in judicial or other official proceedings. A person whose rights or legitimate interests are affected by the recording of personal data may, within three (3) working days from the recording, request—by providing proof of such right or legitimate interest—that the data controller does not destroy or delete the data. Upon request from a court or other authority, the personal data must be forwarded without delay. If no such request is made within thirty (30) days from the request for data retention, any recorded image, audio, or other personal data must be destroyed or deleted.

Personal data may only be transferred to third parties with the prior written consent of the data subject. This does not apply to legally mandated data transfers, which may only occur in exceptional cases. Data subjects are informed that the employer uses data processors for the processing and storage of data handled within the human resources system. The Data Controller is obliged to inform data subjects about the identity of these data processors.

### Rights of data subjects and their assertions

Information about the Data Controller, the Data Processor, the processed data, the purpose of processing, the rights and the options for asserting of rights of data subjects, are provided for the data subjects in the Privacy Policy issued.

- a) **right of access** ~ during the data processing, the data subject is entitled to access all data stored about him/her, and to be informed about the purpose, legal basis, storage and the duration of storage of his/her

data. The right to information covers the rectification, erasure and restriction of processing concerning the processed data, and the option to file a complaint to the supervisory authority. Fulfilment of the request of the data subject to exercise his/her rights shall not be denied, unless it may be demonstrated that the data subject shall not be identified. For any further hard-copies requested by the data subject, we may charge a reasonable fee based on administrative costs.

- b) **right to rectification** ~ the data subject is entitled to ask from the Data Controller to have any of the data subject's data that may be incorrect or incomplete, rectified
- c) **right to erasure ("right to be forgotten")** ~ Erasing of the data by the Data Controller upon the request of the data subject, but this does not mean a general obligation for the Data Controller. The data subject is entitled to have his/her data to be erased (forgotten), where at least one of the following conditions applies:
  - (i). the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed;
  - (ii). the data subject has withdrawn his or her consent to the processing of personal data concerning him or her, and the data processing does not have other legal basis;
  - (iii). the data subject objects to the processing of personal data concerning him/her, and there is no other prioritized reason for the data processing;
  - (iv). the data processing was unlawful;
  - (v). the data needs to be erased under applicable legislative duties of the Data Controller.

Following the termination of the legal basis for the data processing, including the case in which the data subject withdraws his/her consent to the processing of personal data, any personal data processed by the data controller shall be erased within a short period of time.

- d) **right to blocking of data** ~ Instead of erasure, the Data Controller shall block the personal data upon the data subject's request, if based on the available evidence it can be assumed that the erasure would infringe the rightful interests of the data subject.

Personal data blocked this way shall only be processed until the purpose prohibiting the erasure of the data, stands.

- e) **right to restriction of processing** ~ if the accuracy, lawfulness, or necessity of processing concerning the personal data is contested by the data subject, or if the data subject objects to the processing of personal data, the data subject is entitled to obtain from the Data Controller restriction of processing, concerning his/her data.
- f) **right to obtain a copy of personal data** ~ the data subject is entitled to obtain from the data controller a digital copy (pdf, doc, excel, txt) of the personal data undergoing processing, in order for the data to be provided to another data controller.
- g) **right to object** ~ where personal data are processed for the exercise of rights of the controller or any third parties; and where personal data are processed or forwarded for direct marketing or statistical purposes, scientific or historical research, and in the cases and under the conditions provided for by law, the data subject is entitled to object at any time to the processing of personal data concerning him or her. The objection shall be without delay, and no later than 15 days
  - examined,
  - the objection's merits be decided, and
  - the objector be informed about the decision.

## Data Security

The data shall be protected by adequate means especially against unauthorised access, modification, transfer, disclosure, erasure or destruction and accidental destruction or damage, and against inaccessibility resulting from the change of the technology used for access.

We act in accordance with our prevailing IT security policies and regulations and require the same from our employees and contracted partners.

We have developed a Data Protection Incident Policy that outlines the procedure for reporting data breaches, identifies the persons responsible for addressing such breaches, and defines the applicable deadlines.

We maintain a register of all data protection incidents.

In the event of a violation of the Data Subject's rights, the individual may take the matter to court. The court shall handle such cases as a priority.

We are liable to compensate any damages caused to third parties due to unlawful processing of the Data Subject's personal data or a breach of data security requirements. If the unlawful data processing or breach of data security requirements violates the Data Subject's personal rights, the Data Subject may claim non-pecuniary compensation.

*Kársus Kft.* may use lawfully retained personal data and information about you in any discussions or disputes that may arise between the parties, for the purpose of avoiding or resolving legal disputes.

## Cookies – Description and Management

The content published on the website [karsus.com](https://karsus.com) is accessible to anyone without the need to provide personal data.

The website may use the following types of cookies:

- **Necessary cookies** – for basic functionality;
- **Functional cookies** – to remember user preferences;
- **Performance cookies** – to improve website performance and enhance the user experience;
- **Analytics cookies** – to track user behavior and measure website usability, including the rate of returning visitors;
- **Advertising cookies** – to display advertisements tailored to the interests of individual visitors.

The operation of [karsus.com](https://karsus.com) is supported by the following cookies:

- Necessary cookies
- Functional cookies
- Performance-enhancing cookies, including WooCommerce cookies – to support the shopping cart functionality and the identification of registered customers in the online store.

The independent measurement and auditing of website traffic and other analytics data is supported by external service providers (For more details, please visit: [google.com/analytics](https://google.com/analytics)).

We inform our users that the use of cookies on our website requires the user's prior, informed consent, in accordance with Section 155 (4) of Act C of 2003 on Electronic Communications ("Eht."). Therefore, upon the first visit, a notice appears at the bottom of the screen indicating that the website uses cookies, along with a link to this notice. Users can give consent to the use of cookies by clicking the "Allow" button.

During website use, third-party cookies may also be placed on your device to support social media sharing or the compilation of visitor statistics.

The sharing of content and the use of the “Like” button on Facebook are made possible through Facebook cookies.

The website may also contain links or icons that direct users to other websites – such as a Facebook Like button or a YouTube video link – which may also use cookies. You can find information about their cookie usage on the respective websites. Please note that we do not control third-party websites and are not responsible for their content.

The purpose of managing data stored in cookies is to enhance user experience and improve the website’s online services. Cookies used on our website do not store personally identifiable information.

If you prefer not to accept certain types of cookies, you can configure your browser to block unique identifiers or to alert you when a cookie is being placed.

For more information on these functions or to adjust your cookie preferences, please refer to your browser’s help section or user guide. You may also enable or disable interest-based advertising from individual service providers using the following link: <http://www.youronlinechoices.com/hu/ad-choices>

Please note that restricting cookies may cause certain website features (e.g., shopping cart, login) to become unavailable.

This website also uses Facebook Pixel, which allows Facebook to collect or receive data from the site using cookies, web beacons, and similar technologies, and to use that data for providing measurement services and displaying targeted advertisements.

Data Subjects may contact us through the “Contact” section of the website by providing their name and email address. Providing this data is voluntary, and sending the email constitutes consent to data processing for the above-mentioned purposes.

Emails containing ideas, opinions, or comments will be retained by the Data Controller for a maximum of 1 year, unless the purpose of data processing ceases earlier, in which case the email will be deleted.

Effective from: April 30, 2025.

*If you have any questions beyond what is outlined above regarding our data processing practices, or if you wish to establish an offline business relationship, please request our detailed Data Privacy Policy.*