KÁRÁSZY Ltd.
H-1033 Budapest,
Szőlőkert street 11.
HUNGARY
Phone: +36-1-349-8193, +36-1-349-9143, +36-1-350-6712
Mobile: +36-30-883-0965, *Fax:* +36-1-320-3836
e-mail: info@karsus.com
www.karsus.com

DATA PROTECTION INCIDENT POLICY

The Data Controller, **KÁRÁSZY Kereskedelmi és Szolgáltató Korlátolt Felelősségű Társaság** (hereinafter referred to as the "Data Controller"), in accordance with the provisions of the Fundamental Law of Hungary and the provisions of Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information and the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter referred to as the "GDPR"), in order to ensure the protection of personal data, hereby establishes the following rules for data protection incidents to ensure the protection of personal data breaches.

I. Definitions

Data breach: a breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed (a hereinafter "data breach")

In the absence of appropriate and timely action, a data breach may result in physical, material or non-property damage to the data subjects, including:

- the loss of control over their personal data or the restriction of their rights;
- discrimination;
- identity theft or identity fraud;
- financial loss;
- the unauthorised lifting of a pseudonymisation;
- damage to reputation;
- damage to the confidentiality of personal data protected by professional secrecy;
- any other significant economic or social disadvantage suffered by the natural persons in question.

II. Announcement

To report any data breach concerning the data processed by the Data Controller or the Data Processor, the Data Controller operates the following electronic contact address info@karsus.com.

As the Data Controller, we ensure that the contact details provided are kept under constant review.

The Processor shall notify the Data Controller electronically of a potential data breach **within 24 hours** of becoming aware of it.

III. Obligations of the Data Controller

1. Our Company, through its respective CEO, in accordance with the provisions of the GDPR **keeps records of data breaches**. GDPR. This register shall include the facts relating to each data breach, its effects and the measures taken to remedy it.

2. Our Company will **investigate** a notification of a data breach sent by a Data Processor or brought to its attention by a Data Processor or suspected breach detected in its internal systems **within 48 hours and decide** whether the potential breach poses a risk to the rights and freedoms of the data subject.

3. If the investigation shows that **no data protection breach has occurred**, we will inform the potential notifier and close the case.

4. In the event that our Company, as Data Controller, in accordance with the principle of accountability can demonstrate that the data breach is unlikely to result in risk to the rights and freedoms of natural persons, notification to the competent supervisory authority may be waived.

   This includes cases where appropriate measures, such as the use of encryption, do not ensure access to personal data by unauthorised persons, so that the personal data cannot be interpreted without the key used for encryption. However, even with appropriate encryption, the obligation to notify may still apply in cases where there is no adequate backup of the personal data affected by the personal data breach.

5. If the investigation **proves that an infringement has occurred,**

   a. **we will report it within 72 hours of becoming aware of it through our company director to the competent supervisory authority**.

      The notification to the competent supervisory authority includes:
      - the nature of the personal data breach, including, where possible, the identity of the data subjects the categories and approximate number of data concerned by the incident categories and approximate number of data subjects affected by the incident;
      - the identity of the DPO or other person providing further information
      - the likely consequences of the data breach;
      - the measures we have taken or plan to take to remedy the data breach, including, where appropriate, measures to mitigate any adverse consequences of the data breach.
      - in view of the particularities of the data breach, our Company reserves the right to include in the notification additional information relevant to the case.

   b. If the notification **cannot be made within 72 hours**, we will state the reason for the delay in the notification made and provide the required information **in detail** without further undue delay.

   c. If the investigation shows that there is a **high risk of infringement** of the rights and freedoms of natural person, at the latest within 72 hours of becoming aware of it, we will contact our company director **we will inform the data subject** of the data breach.

KÁRÁSZY Ltd.
H-1033 Budapest,
Szőlőkert street 11.
HUNGARY
Phone: +36-1-349-8193, +36-1-349-9143, +36-1-350-6712
Mobile: +36-30-883-0965, Fax: +36-1-320-3836
e-mail: info@karsus.com
www.karsus.com

d. The person responsible for the notification is the managing director, or in the case of more than one managing director, the managing directors jointly and severally, each with a duty to notify and with the right.

The information provided to the data subject will **clearly and plainly explain the nature of the data breach and the content of the mandatory notification to the supervisory authority and will provide information on the steps the data subject can take to protect himself or herself from the consequences of the breach.** In any case, the information will be provided to the data subject in the form of a separate message (by e-mail, or, failing that, by post, or, failing that, by SMS).

Please note that it is not necessary for the data subject to data protection breach if:

- we have implemented appropriate technical and organisational security measures, and these measures have been applied to the data affected by the data breach affected by the data breach;

- we have taken such additional measures following the data breach, to ensure that the high level of risk to the rights and freedoms of the data subject is minimized. risk to the data subject is no longer likely to materialise;

- would require a disproportionate effort to provide the information. In such cases, the publicly disclosed information (notice on our website or by issuing a press release), or by similar measure that ensures that the data subjects are informed in an equally effective manner.

IV. Final provisions

1. The provisions of the current Data Processing Regulation shall prevail, subject to the provisions of these Rules and the In the event of any discrepancy between these Rules and the Data shall prevail.

2. If you have any questions or queries regarding this Policy, please contact us at the following contact details:

   Kárászy Kft. – 1033 Budapest, Szőlőkert utca 11.
   Customer Service: info@karsus.com
   Website: https://karsus.com/

3. This Privacy Incident Management Policy is effective upon publication by our Company (from the date of posting on our website) and shall remain in effect indefinitely (until revoked or until a later amended Policy is published).

4. By accepting this Policy, you expressly agree that we, as Data Controller, are entitled to unilaterally amend this Policy at any time, provided that we will publish the amendment on our website no later than the date on which it becomes effective.

Closed and entered into force: 30st April 2025.