

DATA PROCESSING NOTICE

for Recruitment and Employment Placement Activities

R-Toth Office Private Limited Liability Company

Effective date: 13 September 2026

Version: 1.0

1. Details of the Data Controller

Name of Data Controller: R-Toth Office Private Limited Liability Company

Short name: R-Toth Office Kft.

Registered office: 1223 Budapest, Kápolna utca 9–11. Building A, Ground Floor, Door 4

Company registration number: 01-09-422248

Tax number: 27869284-2-43

Contact e-mail: robert@rtoth.hu

2. Purpose and Scope of this Notice

This Notice applies to the processing of personal data carried out by R-Toth Office Kft. in connection with recruitment, employment placement and activities supporting the preparation of employment. In particular, the Company processes data relating to the recruitment of third-country nationals and, where necessary, to the preparation of selection, immigration and employment-related procedures for prospective employers.

The purpose of this Notice is to provide data subjects with clear information about which of their personal data the Company processes, for what purposes, on what legal basis, for how long, and to which recipients the data may be disclosed.

3. Main Purposes of Data Processing

- identification of applicants and potential employees and communication with them;
- pre-selection and candidate presentation for a specific, currently open position;
- assessment of candidates' professional suitability against the requirements of the position;
- disclosure of candidate data to the prospective employer/client for the relevant open position;
- supporting the preparation of employment, immigration or related administrative procedures for third-country nationals where required by a separate mandate or statutory obligation;
- communication with the applicant and the client;
- assertion, enforcement and defence of legal claims, and compliance with statutory obligations.

4. Categories of Personal Data Processed

The personal data processed will depend on the actual requirements of the relevant position and assignment. In particular, the Company may process the following data:

- identification and personal identification data (name, date and place of birth, nationality, place of residence/stay);
- contact details (telephone number, e-mail address);
- CV, professional experience, education, qualifications, language skills and other professional information related to the position;
- photograph, where provided by the applicant as part of the selection process or where its processing is justified in the relevant process;
- passport data and, only where necessary, a copy of the passport;
- additional data and documents required for employment or immigration-related administration;
- communications with the data subject and information generated during the selection process.

A Társaság nem kér és nem kezel szükségtelen személyes adatokat. Különleges adatok kezelése csak akkor történhet, ha annak jogalapja és szükségessége egyértelműen fennáll.

5. Legal Bases for Processing

The legal basis for each processing activity shall be determined according to the relevant purpose and circumstances. In particular, the Company may rely on the following legal bases under Article 6 of the GDPR:

- the data subject's consent;
- processing is necessary for steps taken at the request of the data subject prior to entering into a contract, or for the performance of a contract to which the data subject is a party;
- compliance with a legal obligation;
- the legitimate interests of the data controller or a third party, provided that the interests or fundamental rights and freedoms of the data subject do not override those interests.

Where processing is based on consent, the data subject has the right to withdraw consent at any time; withdrawal does not affect the lawfulness of processing carried out before the withdrawal.

6. Disclosure to the Prospective Employer

The Company does not process applicants' personal data for the purpose of general database sales or unrestricted disclosure. Personal data is disclosed in connection with a specific, currently open position to the relevant prospective employer/client where this is necessary for the selection of the candidate and the further conduct of the process, and where there is an appropriate legal basis for the processing.

The Company does not sell personal data to third parties or disclose it for marketing purposes. Where the prospective employer acts as an independent data controller, it is independently responsible for its own processing of personal data and is required to provide the data subject with appropriate information about such processing.

If a partner processes personal data on behalf of the Company and in accordance with its instructions, the data processing relationship must be governed by an appropriate agreement.

7. Processing of Passport Data and Copies of Identity Documents

Passport data or a copy of a passport may only be processed and disclosed where this is genuinely necessary for a specific recruitment, employment, immigration or other lawful administrative purpose. The Company seeks to ensure that no data beyond what is necessary for the relevant purpose is processed or disclosed.

Passport copies and the data contained therein shall be subject to enhanced access controls and may only be accessed by authorised persons.

8. Data Retention Period

The Company processes personal data only for as long as necessary to achieve the relevant purpose. In the event of an unsuccessful application for a specific position, the data shall be deleted or anonymised after the selection process has ended, unless there is an appropriate legal basis for further retention.

Data required for the assertion, enforcement or defence of legal claims, or for compliance with accounting or other statutory obligations, may be retained for the period required for the relevant obligation or for the enforceability of the relevant claim.

If an applicant expressly consents to the inclusion of their data in the candidate database for the purpose of being considered for future positions, the data may be processed on the basis of that consent until it is withdrawn or until the specified retention period expires.

9. Data Security

The Company implements appropriate technical and organisational measures to protect personal data against unauthorised access, loss, destruction, alteration or unauthorised disclosure. Such measures may include, in particular, restricting access rights, using strong passwords, keeping IT systems up to date, maintaining backups, and handling electronic data transfers with due care.

When transmitting passport copies, identity documents or other higher-risk documents, the Company shall, where possible, use an appropriate security measure, such as secure file transfer or an encrypted document.

10. Personal Data Breach

In the event of a personal data breach, the Company shall promptly investigate and document the incident, assess the risk to the data subjects and, where necessary, fulfil its notification and information obligations towards the supervisory authority and the affected data subjects.

11. Rights of Data Subjects

- the right to information and access;
- the right to rectification;
- the right to erasure;
- the right to restriction of processing;
- the right to data portability, where the applicable conditions are met;
- the right to object, where the applicable conditions are met;
- the right to withdraw consent where processing is based on consent;
- the right to lodge a complaint with the supervisory authority.

Data subjects may submit their requests to robert@rtoth.hu. The Company shall handle such requests within the time limits specified by the GDPR.

12. Supervisory Authority

Nemzeti	Adatvédelmi	és	Információszabadság	Hatóság	(NAIH)
1055	Budapest,	Falk	Miksa	utca	9–11.
Postai	cím:	1363	Budapest,	Pf.	9.
E-mail:				ugyfelszolgalat@naih.hu	
Web: www.naih.hu					

13. Transfers Outside the EU/EEA

Where personal data is transferred to a recipient outside the European Union or the European Economic Area, the Company shall comply with the GDPR requirements applicable to such transfers and shall only make the transfer where an appropriate legal basis and appropriate safeguards are in place.

14. Internal Data Processing Requirements

- Personal data may only be accessed to the extent necessary for work purposes and by authorised persons.
- Applicants' data must not be stored in private e-mail accounts, private cloud storage or on unauthorised devices.
- Passport and other document copies must not be downloaded unnecessarily or stored permanently on local devices.
- Any e-mail sent to an incorrect recipient, lost device, unauthorised access or other data security incident must be reported immediately to the Company's data protection contact.
- Employees and contractors are subject to confidentiality obligations covering applicants' personal data.

15. Final Provisions

R-Toth Office Kft. shall apply this Data Processing Notice in accordance with its actual data processing activities and shall review it regularly. The document shall be reviewed and amended as necessary in the event of a change in legislation, a new processing purpose, the appointment of a new processor, or a material change to the data processing activities.

This document forms one element of the Company's data protection framework; on its own, it does not replace the records of processing activities, data processing agreements, information security rules, or, where required, consent declarations from data subjects.

Dated: Budapest, 13 September 2026

TÓTH RÓBERT
2026-09-13 (UTC)
Elektronikusan aláírva

FlintSign
Powered by
InfoCert

Róbert Tóth
R-Toth Office Kft.
Owner