



INRIMAS Ltd. Privacy Notice for Job Applicants

Introduction

1.1. INRIMAS Ltd., acting as the Data Controller (hereinafter referred to as the "Company" or the "Data Controller"), hereby informs applicants for positions advertised by the Company (hereinafter referred to as the "Privacy Notice") about the manner in which it processes the personal data of individuals applying for vacancies.

1.2. In the course of collecting, recording, processing, storing and transferring the personal data of Data Subjects, the Data Controller acts in accordance with:

- Regulation (EU) 2016/679 of the European Parliament and of the Council 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 (hereinafter the "GDPR" or the General Data Protection Regulation);
- Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information (hereinafter the "Hungarian Data Protection Act"); and
- all other applicable data protection legislation and the recommendations of the competent supervisory authorities.

1.3. In order to comply with data security requirements, the Data Controller ensures the protection and security of the personal data of Data Subjects, particularly against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, personal data transmitted, stored or otherwise processed.

1.4. Personal data are processed on the basis of the Data Subject's consent, statutory authorization, where necessary for the performance of a contract, or for the purposes of pursuing the legitimate interests of the Data Controller. Through its internal organizational units, the Company implements all necessary technical, organizational, administrative and information security measures to ensure an appropriate level of protection for personal data. To this end, the Company's security, data protection and IT operation and development functions are organizationally separated and operate independently from one another.

1.5. This Privacy Notice also explains the purposes for which personal data are processed, the manner in which such data are used, and the measures implemented to ensure their confidentiality, integrity and secure retention.

Please read this Privacy Notice carefully before submitting your application in order to understand how we process your personal data and to become familiar with your rights relating to data processing.

Should you require any additional information beyond the contents of this Privacy Notice, or if you have any comments, objections or questions regarding the processing of your personal data, please contact INRIMAS Ltd. using the contact details below.



Registered Office: 1046 Budapest, Klauzál u. 10., Hungary
Telephone: +36 30 322 2905
E-mail: info@inrimas.hu

1. Definitions

Data Controller

Company name: INRIMAS Ltd.
Registered office: 1046 Budapest, Klauzál u. 10., Hungary
Company registration number: 01-09-417899
Website: www.inrimas.hu
Legal representative: József Kerékgyártó, Managing Director
Telephone: +36 30 322 2905
E-mail: info@inrimas.hu
Data Protection Contact: info@inrimas.hu

Definitions Related to Data Processing

For the purposes of this Privacy Notice, the following terms shall have the meanings set out below:

"Personal Data" means 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, identification number, location data, online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Processing" means any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means, including 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.

"Data Controller" means the Company as well as any 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.

"Data Processor" means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Data Controller.

"Recipient" means a natural or legal person, public authority, agency or other body to which Personal Data are disclosed, whether a third party or not. However, public authorities which may receive Personal Data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as Recipients. The Processing of such data by those public authorities shall comply with the applicable data protection rules according to the purposes of the Processing.

"Third Party" means any natural or legal person, public authority, agency or other body other than the Data Subject, the Data Controller, the Data Processor and persons who, under the direct authority of the Data Controller or Data Processor, are authorised to Process Personal Data.

"Consent of the Data Subject" means 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.

"Special Categories of Personal Data" means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data processed for the purpose of uniquely identifying a natural person, data concerning health, and data concerning a natural person's sex life or sexual orientation.

"Data Concerning Health" means Personal Data relating to the physical or mental health of a natural person, including the provision of healthcare services, which reveal information about that person's health status.

"Data Transfer" means making Personal Data available to a specified Recipient.

"Personal Data Breach" means 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.

Any additional definitions not expressly set out in this Privacy Notice shall have the meaning assigned to them in Article 4 of the GDPR.

Scope of Data Subjects



This Privacy Notice applies to all individuals who apply for a position advertised by the Data Controller or who submit an unsolicited application for a position not currently advertised by the Data Controller (hereinafter referred to as the "Applicant" or the "Data Subject"). By submitting an application to the Company, the Applicant acknowledges and accepts the provisions of this Privacy Notice and consents to the Processing of his or her Personal Data in accordance with its terms. Where an unsolicited application is submitted, the Data Controller shall promptly inform the Applicant of this Privacy Notice and request confirmation that the Applicant has read and understood its contents. The Data Controller reserves the right to amend this Privacy Notice unilaterally at any time.

The Data Controller shall make this Privacy Notice available to Applicants:

- a) prior to the provision of personal data, where possible; or
- b) taking into account the specific circumstances of the processing of personal data, within a reasonable period after obtaining the personal data, but no later than one month; or
- c) if the personal data are used for the purpose of communicating with the Applicant, at the time of the first contact with the Applicant; or
- d) if the personal data are to be disclosed to another Recipient, at the latest at the time of the first disclosure of the personal data to such Recipient.

2. Purposes, Legal Bases, Categories of Processed Data, Duration of Processing, and Data Security

2.1. Purposes of data processing:

- (I) recruitment;
- (II) communication;
- (III) legal enforcement / enforcement of legal claims.

For purposes (I) and (II), the legal basis of the processing is the Data Subject's voluntary consent pursuant to Article 6(1)(a) of the GDPR. Where the Data Subject provides Special Categories of Personal Data in their application materials, the legal basis for processing such data is the Data Subject's explicit, informed consent pursuant to Article 9(2)(a) of the GDPR. Where the Applicant provides information relating to reduced working capacity, health deterioration, or disability, such data shall also be processed by the Data Controller on the basis of explicit consent pursuant to Article 9(2)(a) of the GDPR.

The Data Controller processes the data collected via its website and other job advertisement platforms for the purposes of:

- maintaining a database of applicants,
- evaluating submitted applications,
- notifying applicants after the completion of the selection process for advertised positions,
- and, subject to separate consent, storing data in the internal database of INRIMAS Ltd.

For purpose (III), the processing of the Applicant's personal data is based on the legitimate interests of the Data Controller pursuant to Article 6(1)(f) of the GDPR.

The purpose of this processing is to enable the Company to fulfil its burden of proof in the event of any potential legal claim brought by the Applicant. In case of rejection of the application, the Company stores both electronic and paper-based applicant data for an additional period of 3 years following the rejection, in accordance with the rules applicable to potential legal remedies related to proceedings before the Equal Treatment Directorate of the Office of the Commissioner for Fundamental Rights. For this purpose of processing, no active data processing is carried out by the Company; only data storage takes place.

Legal basis of processing:

The processing of the Applicant's personal data is based on the legitimate interests of the Data Controller pursuant to Article 6(1)(f) of the GDPR.

2.2. Categories of processed data and duration of processing

For purposes (I) and (II) – recruitment and communication

The personal data processed by the Company regarding Applicants include all data provided by the Applicant in the application form and/or in their CV, in particular:

Identification data and identity document data, such as: name, date of birth, address, photograph, etc.

Data relating to education and professional experience, such as: certificates and diplomas proving highest level of education, language proficiency certificates, and any specific qualifications required for the position.



Additional information provided in the CV, such as: marital status, previous employment history, employment relationships with other employers, job positions held, photograph, contact details, skills, and hobbies, etc.

Data relating to personal interviews and tests completed by the Applicant.

Where the Applicant provides Special Categories of Personal Data, such as information relating to reduced working capacity, health deterioration, or disability, the processing shall also extend to such data categories.

Scope, limitations and duration of data processing

The Company processes Applicants' personal data only to the extent and for the duration necessary for the above-defined purposes. Only personal data that are strictly necessary and appropriate for achieving the purposes of processing may be processed. Applicants may request that their data be processed only in relation to a specific application. In such cases, the data will be stored by the Company for 30 days following the closure of the application process. Applicants may also request that their data be stored without reference to a specific application. In such cases, the Company shall store the data for 1 year from the date of consent. If the Applicant withdraws consent at any time, the data shall be deleted within 30 days. If the Applicant withdraws consent during the recruitment process, before its completion, the Company shall consider this as a withdrawal from the application process.

For purpose (III) – legal enforcement

The scope of personal data processed for this purpose is identical to the data processed during the recruitment process.

Scope, limitations and duration of processing

In the case of data processed for legal enforcement purposes, following the rejection of an application, the Company shall retain the data for a further 3 years, in relation to potential legal remedies connected to proceedings before the Equal Treatment Directorate of the Office of the Commissioner for Fundamental Rights.

For this purpose, no active data processing is carried out; only data storage is performed.

3. Recipients of personal data

Personal data of Applicants may be accessed within the Company by the following persons, strictly for the purposes and to the extent necessary for those purposes:



Employees of the Human Resources Department, for the following purposes:

- preparation and retention of employment-related documents and contracts.

Persons having access to personal data within the Company are subject to a confidentiality obligation regarding the personal data of Applicants. Accordingly, they are required to treat all personal data and information obtained during or in connection with their duties as strictly confidential and must not disclose them to third parties. This obligation shall remain in force without time limitation even after termination of employment.

Persons processing personal data are required to maintain the confidentiality of all personal data, and may not use, disclose, publish, or make such data accessible to any third party, except as provided in this Privacy Notice.

4. Source of personal data

The Data Controller obtains the Applicants' personal data either directly from the Applicants themselves or through recruitment agencies / employment intermediaries. The Applicant may withdraw their consent to data processing at any time; however, such withdrawal shall not affect the lawfulness of processing carried out prior to the withdrawal of consent.

If the Applicant fails to provide personal data, or provides incomplete data, depending on the nature of the missing information, communication with the Applicant may become impossible, or the Data Controller may not have sufficient information to assess the Applicant's suitability for the relevant position. As a result, the Applicant's suitability for the position cannot be evaluated, and therefore no employment contract can be concluded.

5. Location of data processing, nature of applied technology, and data security

The Data Controller applies the principle of "privacy by design" and "privacy by default" throughout the entire design and operation of its data processing activities, with particular regard to data security requirements. The objective of the Data Controller is to minimize the processing of personal data in order to reduce data protection risks.

All persons who have access to personal data within the Company are bound by a confidentiality obligation with respect to Applicants' personal data. Accordingly, they are required to treat all personal data and any related information obtained in the course



of their employment or otherwise as strictly confidential and must not disclose such information to third parties. This confidentiality obligation shall remain in force without limitation in time, even after termination of employment.

Persons involved in data processing are required to ensure the confidentiality of personal data and may not use, disclose, publish, or make such data accessible to any unauthorized party, except in cases specified in this Privacy Notice.

The Data Controller further implements all necessary technical, organizational, and administrative measures and complies with all relevant procedures required to ensure data protection and data security.

The Applicant acknowledges that the Data Controller excludes any liability for damages or disadvantages arising from failures or malfunction of IT systems or electronic communication.

The Applicant acknowledges that any files attached by the Applicant may be subject to virus scanning and other IT security screening processes. The IT systems used for data processing are located on the Data Controller's servers. The Data Controller ensures the security of data processing through technical, organizational, and operational measures that provide an appropriate level of protection in relation to the risks associated with processing personal data.

The IT systems and infrastructure are selected and operated in such a way that the processed data:

- a) are accessible to authorized persons only (availability);
- b) their authenticity and authentication are ensured (authenticity of processing);
- c) their integrity and immutability can be verified (data integrity);
- d) are protected against unauthorized access and remain confidential (confidentiality).

6. Data Protection Incidents

The Controller's employees are obliged to immediately report any data protection or data security incident to the Data Protection Officer and/or the Managing Director upon detection or notification of such incident.

If the data protection incident is likely to result in a high risk to the rights and freedoms of the Applicant, the Controller shall inform the Applicant without undue delay about the incident, including in particular:



- the name and contact details of the data protection contact person,
- the likely consequences of the incident,
- the measures taken or planned to address and remedy the incident.

The Controller shall keep a record of all data protection incidents, including their known effects and the measures taken in response.

7. Data Processors

The Controller does not use any data processors.

8. Data Transfers

In certain cases defined by law, the Controller may be entitled and obliged to transfer the personal data of Applicants to third parties, such as courts, authorities, the police, public prosecutors, local municipalities, or national security services, without limitation. The Applicant has the right to be informed about the transfer of their data to third parties, except where providing such information would jeopardize the purpose of the transfer.

The Controller maintains a record of data transfers, which includes:

- the date of the data transfer,
- the legal basis of the transfer,
- the recipient of the data,
- the scope of the personal data transferred.

The Controller declares that it does not transfer personal data of Applicants to third countries (i.e. countries outside the European Union), nor does it make such data available to data controllers operating in third countries.

The Controller ensures that all data transfers comply with legal requirements (purpose and legal basis) and do not infringe the rights of the Applicant.

9. Rights of the Applicant regarding data processing

The Company draws the attention of Data Subjects to the fact that in case of complaints or comments, it is recommended to first contact the Company as the Data Controller using the contact details provided in this Notice.



In accordance with applicable data protection laws, the Data Subject has the following rights:

- a) the right to request information about the processing of their personal data, including the right to request a copy of the data (right of access);
- b) the right to request the rectification of inaccurate personal data and to challenge the accuracy of the data (right to rectification);
- c) the right to request the deletion of their personal data (right to erasure / right to be forgotten);
- d) the right to withdraw consent at any time where processing is based on consent. The withdrawal does not affect the lawfulness of processing carried out prior to withdrawal;
- e) the right to request restriction of processing;
- f) the right to data portability (to receive the personal data provided to the Controller in a structured, commonly used, machine-readable format and to transmit those data to another controller, where the conditions set out in the GDPR are met);
- g) the right to object to the processing of personal data where the legal basis is the legitimate interest of the Controller or a third party, including profiling. In such cases, the data shall no longer be processed unless the Controller demonstrates compelling legitimate grounds which override the interests, rights and freedoms of the Applicant, or which relate to the establishment, exercise or defence of legal claims;
- h) the right to lodge a complaint and to seek legal remedies in relation to the processing of personal data or the exercise of rights under the GDPR.

No automated decision-making, including profiling, takes place in connection with this data processing.

10. Procedure in case of requests from the Applicant

The Applicant may contact the representative of the Company specified at the beginning of this Notice with any request based on the above rights, or with any other questions or requests concerning their personal data, using any of the contact details provided therein.

The Controller shall decide on the written request within 30 days from the date of receipt. If necessary, taking into account the complexity of the request and the number of pending requests, the Company may extend this deadline. The Applicant shall be

informed in advance of any such extension and the reasons for it. If the Applicant's request is well-founded, the Controller shall implement the requested measure within the applicable deadline and shall provide written confirmation of its execution. If the Controller rejects the Applicant's request, it shall issue a written decision. The decision must include the facts underlying the decision, the reasoning with reference to the relevant legal provisions and case law, and information on the available legal remedies against the decision.

The Applicant may be required to bear the costs related to the exercise of their rights only if, within 8 days of receiving the request, the Controller has informed the Applicant in writing that the request is excessive and has simultaneously informed them of the amount of administrative costs, and the Applicant nevertheless maintains their request. A request is considered maintained if the Applicant does not withdraw it within 5 working days despite the Controller's notice or until the end of the administrative deadline.

The Applicant shall pay the applicable costs within 8 days of receiving the payment request issued by the Controller. If the Applicant disagrees with the Controller's decision, or if the Controller fails to comply with the above procedural deadlines, the Applicant may обратиться to the supervisory authority or to a court.

Supervisory Authority

If the Applicant considers that the processing of their personal data by the Controller infringes applicable data protection laws, in particular the GDPR, they have the right to lodge a complaint with the National Authority for Data Protection and Freedom of Information (NAIH).

Contact details of the authority:

Website: <http://naih.hu/>

Address: 1055 Budapest, Falk Miksa utca 9–11.

Postal address: 1363 Budapest, P.O. Box 9

Phone: +36 1 391 1400

Fax: +36 1 391 1410

E-mail: ugyfelszolgalat@naih.hu

The Applicant also has the right to lodge a complaint with a supervisory authority established in another EU Member State, in particular in the Member State of their habitual residence, place of work, or the place of the alleged infringement.

Right to judicial remedy

Regardless of the right to lodge a complaint, the Applicant may bring an action before a court if their rights under the GDPR have been infringed during the processing of their personal data.

Legal proceedings may be initiated in Hungary against the Controller as a Hungarian data controller before Hungarian courts. Information on the competent courts in Hungary is available at: <http://birosag.hu/torvenyszekek>

11. Miscellaneous provisions

The Controller reserves the right to unilaterally amend this Notice at any time in compliance with applicable legislation.

Appendices:

- Annex No. 1 – Declaration of the Applicant on the acknowledgement of this Notice

Budapest, 3 July 2026

INRIMAS Ltd.
Data Controller



Annex No. 1 to the Notice

DECLARATION

I, the undersigned (name) (mother's name:, address:), as an applicant for a position advertised by INRIMAS Ltd. (registered office: 1046 Budapest, Klauzál u. 10.; hereinafter referred to as the "Company"), hereby declare that

I have read and understood the information regarding the processing of my personal data contained in the document titled "Privacy Notice regarding Job Applications" issued by INRIMAS Ltd. as Data Controller, which is valid as of the date indicated below, and I acknowledge and accept the provisions set out therein.

I further declare under penalty of perjury that the data provided by me are true and correct, and that I am entitled to provide and transmit the personal data submitted to the Data Controller.

In the case of consent-based data processing, I expressly consent to the processing of the personal data provided below by the Data Controller in accordance with the provisions of the aforementioned Privacy Notice regarding Job Applications. I will not provide any data for which I do not grant consent for processing.

I also declare that, in the event I provide personal data relating to other persons, I have the necessary authorisation from the relevant data subjects to disclose such data to the Data Controller.

I acknowledge that, in accordance with applicable data protection laws, I am entitled to exercise my rights, including the right of access, data portability, rectification, restriction of processing, erasure, and objection, by postal mail, in person via my direct supervisor and/or at the Company's central office address, as well as via the Company's email address, and that I may also exercise legal remedies.

Date:

.....
Applicant's signature