Valid as of 28th of July 2025

PRIVACY POLICY

OF PROCESSING THE PERSONAL DATA OF CANDIDATES

This Privacy Policy of processing the Personal Data of Candidates (hereinafter – **the Privacy Policy**) describes how **SIA INGAIN TECHNOLOGIES**, registration No. 50203431551, legal address: Latgales Street 322S, Riga, LV-1063, Latvia (hereinafter – **the Company**) processes the Personal Data of Candidates. As an employer, the Company needs to store and process information about Candidates for employment commencement and maintenance purposes and to enable it to run its business effectively, lawfully and appropriately. The Company is the controller of processed personal data.

1. DEFINITIONS

Candidate means any natural person who is applying/applied for a position at the Company.

Data Protection Legislation means the applicable EU and national data protection legislation that the Company is subject to, for example, 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 (General Data Protection Regulation), hereinafter – **GDPR**.

Personal Data means any information directly or indirectly related to a Candidate. The categories of Personal Data are set out in Section 3 of the Privacy Policy.

Data Controller means anyone who alone or jointly with others determines the purposes and means of the Processing of Personal Data. For the Processing of Personal Data described in the Privacy Policy, the Company is the Data Controller.

Data Processor means anyone who Processes Personal Data on behalf of the Data Controller.

Recipient means a natural or legal person, public authority or another body, to whom the Company is entitled to disclose Personal Data. The categories of Recipients are set out in Section 5 of the Privacy Policy.

Processing means any operation or set of operations performed regarding Personal Data (such as collection, recording, storing, erasure, sharing).

Regulatory Legislation means the applicable legal acts that the Company is subject to, for example, relating to anti-money laundering, commercial activity, data protection, taxes, bookkeeping etc.

The Company means **SIA INGAIN TECHNOLOGIES**, registration No. 50203431551, legal address: Latgales Street 322S, Riga, LV-1063, Latvia.

Third person means a person with whom the Candidate may be in close relations (such as relatives) that can lead to conflict of interests at the Company, as well providers of feedback (such as the Candidate's former colleagues, cooperation partners, managers).

2. GENERAL

2.1 This document describes how the Company Processes Personal Data of Candidates. Detailed information on the Processing of Candidates' Personal Data might be additionally described in job advertisement and other documents related to the advertisement and application, as well as on website of placement of the job advertisement.

2.2 Within the framework of Data Protection Legislation, the Company ensures the confidentiality of Personal Data. The Company has implemented appropriate technical and organisational measures to safeguard Personal Data from unauthorized access, unlawful disclosure, accidental loss, modification, destruction or any other unlawful Processing.

2.3 The Company engages Data Processors for Processing of Personal Data and takes necessary steps to ensure that Processing of Candidates' Personal Data by Data Processors takes place under a contract or Regulatory Legislation and according to documented instructions of the Company.

3. CATEGORIES OF PERSONAL DATA

Personal Data is collected directly from a Candidate, through the activities performed and systems used by the Candidate and from external sources such as public and private registers or other third parties and Third persons. Personal Data categories which the Company collects and processes are:

Identification data such as name, surname, personal identification number, date of birth, sex, data regarding identification document;

Contact details such as address, phone number, e-mail address, language of communication.

Data about relationships with legal entities, such as data submitted by the Candidate or obtained from public data bases or third-party service providers.

Professional data such as language skills, education, professional career and duration, job title, licenses, training certificates and any other information set out in CV, as well as references/recommendations.

Financial data such as solvency and salary information.

Data about trustworthiness, such as data about regarding possible conflicts of interest, incl. data about Candidate's business activities, data related to anti-money laundering, counter terrorist financing or financial sanctions or organized crime, damage caused to the Company or any third party.

Communication and device data such as the data contained in messages, emails, visual images, video and/or audio recordings, as well as other conversations and interactions, collected when the Candidate participates in job interview, from Candidate's application and/or activities in communication tools of the Company.

Demographic data such as country of residence, citizenship.

Data about habits, preferences and satisfaction, such as Candidate satisfaction.

Sensitive data such as Special categories of Personal Data (for example, data concerning health) and Data about criminal convictions and offences such as data about absence of a crime which is connected with terrorism or about convictions for breach of international or national sanctions or anti-money laundering and counter terrorist financing legislation.

Special categories of Personal Data can also be processed based on legitimate interests of the Company, for example, to exercise a legal claim, or based on a legal obligation that the Company is subject to.

4. LEGAL BASIS AND PURPOSE OF PERSONAL DATA PROCESSING

The Company Processes Candidate's Personal Data primarily for the purposes described below:

4.1 Managing Candidate selection for vacancies

The Company Processes Candidate's Personal Data within the recruitment process in order to administer Candidate's identification, evaluation and selection for vacancies of the Company.

Legal basis for Personal Data Processing:

Pre-contractual agreement

4.2 Managing Candidate personal data to establish employment

The Company Processes Candidate's Personal Data within the recruitment process to conclude employment contract.

Legal basis for Personal Data Processing: Performance of agreement, legal obligation and/or legitimate interest of the Company.

4.3 Suitability assessment

The Company Processes Candidate's Personal Data in order to assess the suitability of a Candidate for a certain job position. Personal data of Third persons (such as name, job role, contact information or relationship type) can be processed for this purpose.

Legal basis for Personal Data Processing:

Performance of agreement and legal obligation.

4.4 Managing Candidate for future job opportunities

The Company Processes Candidate's Personal Data to save Candidate's personal data for future job opportunities.

Legal basis for Personal Data Processing: Candidate´s consent.

4.5 Candidate surveys

The Company Processes Candidate's Personal Data to evaluate Candidate's satisfaction about recruitment process.

Legal basis for Personal Data Processing: legitimate interest of the Company.

4.6 Managing compliance, internal audit and fulfilling statutory duties

The Company Processes Candidate's Personal Data to interpret, set compliance tests, monitor and check activities related to regulatory requirements, reporting and communication, as well as to conduct reviews and controls for providing opinion to the Company management concerning governance and internal control.

Legal basis for Personal Data Processing: legitimate interests or legal obligation of the Company.

4.7 Establishing, exercising and defending legal claims

The Company Processes Candidate's Personal Data to establish, exercise and defend legal claims, handle complaints and requests, as well as to retain information for this purpose.

Legal basis for Personal Data Processing: legitimate interest and legal obligation of the Company.

5. RECIPIENTS OF PERSONAL DATA

To be able to provide the recruitment process, the Company may share the Candidates' Personal Data with the Recipients. These Recipients are in general:

5.1 Authorities (such as law enforcement authorities, tax authorities, supervisory and control authorities, and financial investigation authorities).
5.2 Companies in the same group as the Company and the authorities of the country of residence of their shareholders/members, if so requested by such authorities.
5.3 Any accounting service provider, auditor, financial adviser, legal adviser, solicitor, notary public and/or bailiff and other Personal Data processors selected and approved by the Company (recruitment management systems, recruitment agencies).
5.4 Third parties maintaining registers (e.g. Insolvency Register and other registers which contain Personal Data or through which Personal Data is shared).
5.5 Judicial and extrajudicial dispute settlement institutions.
5.6 Other persons or entities related to provision of services to the Company, incl. archiving, postal and courier service providers, data storage providers selected by the Company; website and mobile application operators; video surveillance system providers; tele-marketing, marketing and survey service providers, email and SMS gateway service providers, online intermediaries and other third parties, ensuring that such parties will process the Candidate's personal data only to the extent and for the purposes (purposes) set out in this Privacy Policy.
5.7 Providers of feedback concerning the previous professional career of the Candidate and persons who, on behalf of the Company, carry out a statistical, market or public opinion study or survey, if the disclosure of personal data is necessary for the purpose of carrying out the study or survey in question.

The Company will not share Candidates' Personal Data more than necessary for the particular purpose of Processing.

Recipients may Process the Personal data as Data Processors and/or as Data Controllers.

When the Company receives and transfers your Personal Data to the Recipients (independent Data Controllers), the Recipients, as independent Data Controllers, are

responsible for providing information to data subjects on such Processing of Personal Data. In such case the Company advise the Candidate to contact this Recipient for information on the Processing of Personal Data by the Recipient.

When the Company receives and transfers your Personal Data to Data Processors who process Personal Data on behalf of the Company, the Company shall take all necessary measures to ensure that the Personal Data is processed by the Data Processors in accordance with the agreement or regulatory enactments and documented Company instructions.

Analytics (Sub-contractor)

We may use third-party service providers to monitor and analyze the use of our service.

- Google Analytics

Google Analytics is a web analytics service offered by Google that tracks and reports website traffic. Google uses the data collected to track and monitor the use of our service. This data is shared with other Google services. Google may use the collected data to contextualize and personalize the ads of its own advertising network.

You can opt-out of having made your activity on the service available to Google Analytics by installing the Google Analytics opt-out browser add-on. The add-on prevents the Google Analytics JavaScript (ga.js, analytics.js, and dc.js) from sharing information with Google Analytics about visits activity.

For more information on the privacy practices of Google, please visit the Google Privacy Terms web page

Behavioral Remarketing (Sub-contractor)

The Company uses remarketing services to advertise on third party websites to you after you visited our service. We and our third-party vendors use Cookies to inform, optimize and serve ads based on your past visits to our service.

- Google Ads

Google Ads remarketing service is provided by Google Inc. You can opt-out of Google Analytics for Display Advertising and customize the Google Display Network ads by visiting the Google Ads Settings page.

Google also recommends installing the Google Analytics Opt-out Browser Add-on for your web browser. Google Analytics Opt-out Browser Add-on provides visitors with the ability to prevent their data from being collected and used by Google Analytics.

Links to Other Sites

Our services may contain links to other sites that are not operated by us. If you click on a third party link, you will be directed to that third party's site. We strongly advise you to review the Privacy Policy of every site you visit. We have no control over and assume no responsibility for the content, privacy policies or practices of any third party sites or services.

6. CHILDREN'S PRIVACY

Services provided by the Company does not address anyone under the age of 13 ("Children"). The Company doesn't knowingly collect personally identifiable information from anyone under the age of 13. If you are a parent or guardian and you are aware that your Children has provided us with Personal Data, please contact us. If we become aware that we have collected Personal Data from children without verification of parental consent, we take steps to remove that information from our servers.

7. SECURITY OF DATA

The Company has established necessary legal, organizational, physical and technical security measures to protect your Personal Data against unauthorised access, accidental or unlawful alteration, disclosure, loss, destruction, erasure, including measures against threats caused by physical exposure and measures implemented by means of software. Some examples of the measures we use:

Physical measures - paper-based documents containing Personal Data are stored in locked rooms and cabinets to which only certain employees have access for fulfilling their job duties; data processing rooms and IT-systems are sufficiently protected against fire, overheating, water, current instability and power outages.

Technical measures - all employee work computers are protected with password protected screensavers when the employee leaves; it is ensured that the IT- system does not accept new login attempts and locks the username if certain number of access attempts has been exceeded; it is ensured that especially vulnerable systems (e.g. laptops, smartphones) are sufficiently protected (using encryption or other means).

Organizational means - all IT system Users are assigned roles and profiles; it is ensured that access rights are deleted when an employee leaves the Company; it is ensured that

there is no access from publicly used rooms to rooms where Personal Data is being processed.

In case we use external companies for providing services, which include data processing, we conclude data protection agreements with such service providers obligating them to: a) take appropriate measures to ensure confidentiality and security of the Personal Data and ii) process Personal Data in accordance with the applicable legal requirements.

8. **TERRITORY OF PROCESSING OF PERSONAL DATA AND TRANSFER OF PERSONAL DATA**

Personal data is processed in the European Union / European Economic Area (EU / EEA) and in the countries outside the EU where the European Commission has determined, that these countries outside the EU offer an adequate level of data protection: Personal Data is stored in US on the basis of the adequacy decision of the European Commission (Article 45 of the GDPR), and such data transfer shall not require any specific authorisation.

However, if the Personal Data is transferred outside the EU / EEA, the Company undertakes to take all necessary security measures to ensure the same level of security of Personal Data as in the EU / EEA, and appropriate guarantees in accordance with the provisions of Article 46 of the GDPR. The Company shall transfer Personal Data to a third country or to an international organisation only if there is a legitimate basis for it and appropriate safeguards have been put in place:

(a) the European Commission has decided in accordance with Article 45 of the GDPR that the third country or organisation concerned ensures an adequate level of protection; or

(b) the controller or processor has provided adequate guarantees in accordance with Articles 46 or 47 of the GDPR: (i) binding corporate rules; (ii) standard contractual clauses adopted and approved by the European Commission or the national supervisory authority; (iii) other ad hoc contractual clauses, if approved by the competent national supervisory authority; (iv) an approved code of conduct together with a binding and legally enforceable commitment by the third-country data controller or processor to apply the relevant safeguards; (v) an approved certification mechanism together with a binding and legally enforceable commitment by the third-country data controller or processor to apply the relevant safeguards; or

(c) there is an exception set out in Article 49 of the GDPR ((i) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible

risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards; (ii) where the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; (iii) the transfer is necessary for the establishment, exercise or defence of legal claims; (iv) where the transfer is necessary for important reasons of public interest; (v) where it is necessary for the protection of the vital interests of the data subject or of another natural person, where the data subject is physically or legally incapable of giving consent.

Upon a written request, the User can receive more detailed information on the transfer of Personal Data to countries outside the EU / EEA.

In the event of any onward transfer, the Company will comply with all other safeguards, in particular the purpose limitation. The Company will take all steps reasonably necessary to ensure that your Personal Data is treated securely and in accordance with this Privacy Policy and no transfer of your Personal Data will take place to an organization or a country unless there are adequate controls in place including the security of your Personal Data and other personal information.

9. CAMERA SURIVEILLANCE

With the purpose of conducting video-surveillance as part of the Company's safety measures, the Company is using video-surveillance at premises of the Company. The video-surveilled areas are marked with informative signs.

Personal Data Processed when the Company conducts video-surveillance are contained in visual images and video recordings.

The Company carries out video-surveillance based on legitimate interests to ensure the security of the Company's visitors, employees (as well Candidates), premises and assets; defend legal claims and legitimate interests; detect and prevent unlawful activities.

Visual images and video recordings containing Personal Data are shared with relevant Recipient in case the recorded material is needed for criminal investigation, or with a Recipient that maintains and services the video-surveillance systems on behalf of the Company.

10. RETENTION PERIOD

Personal Data will be retained for the period which depends on the particular purpose of Processing for which these data are collected. Retention period is as long as the recruitment process activities (application, evaluation and selection) take place.

In cases when the processing of Personal Data takes place based on the Candidate's consent, the Personal Data will be retained as long as the consent is valid:

a) If the Candidate gives its consent to process Personal Data in the recruitment process for the advertised vacancy, the Personal Data will be stored for 4 (four) months after the end of the selection process or until the withdrawal of the consent. In case of withdrawal of the consent, the Candidate's Personal Data will be deleted, unless the Company needs to retain the Personal Data for a longer period;
b) If the Candidate gives its consent to process Personal Data for all vacancies within other recruitment processes, the Personal Data will be stored for 1 (one) year after the conclusion of the recruitment process or until the consent is withdrawn. In case of withdrawal of the consent, the Candidate's Personal Data will be deleted, unless the Company needs to retain the Personal Data for a longer period.

If the Candidate has not received an invitation to the next round within 1 (one) month after the closing date of the advertised vacancy, it may be considered that the selection recruitment process has ended and the Candidate will not be selected for further rounds.

If the Candidate is recruited, the Candidate's recruitment information will be stored together with its employment information (for the relevant retention periods).

Other deadlines may be applicable when the Personal Data is Processed for purposes based on legitimate interest of the Company, for example, for the establishment, exercise or defence of legal claims. In all cases, the Company limits the Processing of Personal data to a minimum.

Personal Data Processed in regard to video-surveillance carried out by the Company will be retained no longer than necessary, with a maximum retention period of 30 (thirty) days from the moment of recording, unless there is another purpose of Processing (for example, in connection with criminal investigation).

Where the same personal data are processed for more than one purpose, they shall be kept for the longer applicable retention period.

If none of the legal grounds for processing personal data no longer exist and the normative acts do not provide for a longer period of storage of personal data, the Company shall delete the personal data.

11. RIGHTS OF CANDIDATES AS DATA SUBJECTS

Under the Data Protection Legislation, the Candidate has rights of a data subject regarding Processing of Personal Data. Such rights are:

- **Right to be informed and Right of access**

If you wish to be informed what Personal Data we hold about you and receive a copy of the Personal Data we hold about you, please contact us. Please note that we may ask you to verify your identity before responding to such requests.

- **Right to rectification**

You have rights to request updating any personal information about you if it is inaccurate or incomplete.

- **Right to erasure**

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have Personal Data erased and to prevent processing in specific circumstances: (i) where the Personal Data is no longer necessary in relation to the purpose for which it was originally collected/processed; (ii) the Personal Data is processed in relation to the offer of information society services to a child; (iii) when you withdraws consent; (iii) the Personal Data was unlawfully processed (i.e. otherwise in breach of the GDPR); (iv) when the individual objects to the processing and there is no overriding legitimate interest or other legal basis for continuing the processing; (v) the Personal Data has to be erased in order to comply with a legal obligation.

- **Right to restrict processing**

You have rights under certain circumstances to request to 'block' or suppress processing of Personal Data for a certain period (e.g. if you have objected to Personal Data processing). When processing is restricted, we are permitted to store the Personal Data, but not further process it.

- **Right to object**

You have the right to object to such data processing which is based on the Company's legitimate interest incl. profiling based on our legitimate interest. We shall stop processing your Personal Data when you present an objection, unless we can demonstrate compelling legitimate grounds for the processing or processing is needed for the establishment, exercise or defense of legal claims. You also have the right to object at any time to processing of your Personal Data concerning for direct marketing. Upon receiving such objection, we shall stop processing your Personal Data for direct marketing.

- **Right to data portability**

In case processing the Personal Data is based on your consent or on a contract between us and Personal Data is processed automatically, you have the right to access Personal Data concerning you which you have given to us in a structured, generally usable and in machine readable form. You have rights to move, copy or transfer Personal Data easily from one IT environment to another in a safe and secure way. We will provide all Personal Data in a structured way using open formats like CSV.

- **Right to withdraw your consent**

You have right to withdraw your consent where the personal data is provided to the Company on the basis of your consent (withdrawal of consent does not affect the lawfulness of processing based on consent prior to the withdrawal);

- **Right to not be subject to fully automated decision-making, including profiling**

You have right not to be subject to fully automated decision-making, including profiling, where such decision-making has legal effects or similarly significantly affects you (data subject). This right shall not apply if the decision-making is necessary for entering into or performance of a Contract with the Candidate (data subject), if the decision-making is permitted under applicable laws or regulations or if the Candidate (data subject) has given its explicit consent.

- **Right to contact us, submit a complaint to the Data State Inspectorate of Republic of Latvia and the court**

The Candidate may contact the Company with any request, withdrawal of consent, data subject rights or complaint regarding the Processing of Personal Data.

If the Candidate wants to exercise any of the abovementioned rights, please contact the Company using the e-mail address privacy@ingain.com. In order to respond to your inquiry, we must first authenticate you to avoid granting information to unauthorized persons. We will respond to your inquiries within 30 days.

We respect your privacy and wish that processing your Personal Data by us would be understandable and transparent. For that we have also drafted this Privacy Policy. Should you need further information about processing your Personal Data or exercising your rights, please contact us at e-mail address privacy@ingain.com.

If you believe that processing of your Personal Data violates the GDPR requirements, you have the right to turn to the Data State Inspectorate of Republic of Latvia (info@dvi.gov.lv) and the courts to protect your rights and interests.

12. VALIDITY AND AMENDMENTS OF THE PRIVACY POLICY

The Company is entitled to unilaterally amend this Privacy Policy at any time, in compliance with the Regulatory Legislation, by notifying the Candidates of any amendments on this website: https://www.ingain.com/careers and updating the "effective date" at the top of this Privacy Policy. You are advised to review this Privacy Policy periodically for any changes. Changes to this Privacy Policy are effective when they are posted on this website.

The Privacy Policy enter into force on 28th of July, 2025, and their latest version is available on website: https://www.ingain.com/careers.