Data Processing Policy
Last updated: 27.08.2025

This Data Processing Policy is part of the agreement between:

Data Controller (Client) – the company or individual using the Digi-CRM system and entering their customer personal data into it.
Data Processor (Service Provider) – [SIA DIGI Risinājumi, registration number: 40203598740, info@digirisinajumi.eu], which maintains and provides the Digi-CRM system (available at https://digi-crm-frontend.vercel.app).

1. Subject of Data Processing

The Processor processes personal data on behalf of the Controller in order to ensure the functionality of the CRM system, including:

- storing and structuring client data,
- recording communication history,
- integrations with email, calendar, and payment systems (e.g., Stripe),
- user account management.

2. Categories of Personal Data

Depending on the Controller's activities, the Processor may process:

- contact details (name, surname, email, phone),
- transaction and activity history,
- payment information (via Stripe, without storing full card details),
- client records, notes, and files added to the CRM system,
- technical information (IP address, access logs).

3. Purpose and Legal Basis of Processing

Data is processed solely:

- for the performance of contractual obligations (CRM service provision),
- in accordance with documented instructions from the Controller,
- in compliance with applicable data protection laws (e.g., GDPR).

4. Obligations of the Processor

The Processor undertakes to:

- process data only according to the Controller's instructions,
- implement technical and organizational security measures (e.g., encryption, access control),
- ensure that employees processing data are bound by confidentiality,
- never use the data for its own purposes,
- notify the Controller of any data breach within 72 hours,
- assist the Controller in fulfilling data subject rights (erasure, access, rectification, etc.).

5. Third Parties and Subprocessors

The Processor may engage only trusted subprocessors, such as:

- Stripe Payments Europe Ltd. – payment processing,
- Vercel – hosting,
- Google (if Analytics or integrations are used),
- other IT service providers.

The Processor remains responsible for ensuring that subprocessors comply with the same data protection obligations as set out in this agreement.

6. Data Retention

Personal data is stored for as long as the agreement between the parties is in force.
After termination of the agreement, all data will be deleted or returned to the Controller, unless otherwise required by law.

7. Security Measures

The Processor implements the following security measures:

- encryption of data in transit (SSL/TLS),
- password hashing,
- regular backups,
- access control on a need-to-know basis,
- regular security audits.

8. Data Transfers Outside the EU

If data is transferred outside the European Economic Area, the Processor ensures that appropriate GDPR-compliant safeguards are in place.

9. Obligations of the Controller

The Controller guarantees that:

- it has the legal right to transfer data to the Processor,
- it informs data subjects about the processing,
- it determines the legal basis for processing (e.g., consent, contract performance).

10. Term and Termination

This policy remains valid for as long as the Controller uses the CRM service. Upon termination of the agreement, the Processor shall:

- delete or return the Controller's data,
- ensure that backups are deleted within a reasonable period.

11. Governing Law

This document is governed by the laws of the Republic of Latvia and applicable EU data protection legislation (GDPR).

12. Contact

For any questions regarding data processing, please contact:
SIA DIGI Risinājumi
Email: info@digirisinajumi.eu