RegiCargo — Data Processing Agreement

GDPR Article 28

1. Parties

This Data Processing Agreement is entered into between:

Data Controller

A Customer/Company ("Data Controller") that uses RegiCargo to manage drivers, vehicles, trips, and geolocation data.

Data Processor

RegiCargo B.V. (or related legal entity) ("Processor"), a Dutch-registered company executing this data processing agreement on behalf of the Data Controller.

2. Definitions

"Personal Data"

Any information relating to an identified or identifiable natural person.

"Processing"

Any operation performed on personal data, such as collection, recording, organization, structuring, storage, adaptation, modification, retrieval, consultation, use, disclosure, erasure, or destruction.

"Geolocation Data"

Precise GPS coordinates (latitude/longitude, 8 decimals ≈ 1 cm accuracy) recorded by drivers during trips, including accuracy, speed, and heading.

"Sub-processor"

A natural or legal person that processes personal data on behalf of the Processor.

3. Subject Matter and Duration

The Processor processes personal data on behalf of the Data Controller for the following purposes:

- Management of user accounts (names, emails, phone numbers, addresses)
- Management of company data (KvK numbers, VAT numbers, contact information)
- Management of vehicles (license plates, make, model, type)
- Processing of driver geolocation data during trips
- Storage of delivery data (documents, photos, signatures)
- Proposal workflow and negotiations

This Agreement remains in force for as long as the Data Controller uses RegiCargo services, unless terminated earlier in accordance with Article 11.

4. Processor Obligations

The Processor commits to the following obligations:

- Process personal data only under instruction from the Data Controller
- Maintain confidentiality (employees under NDA)
- Implement appropriate technical and organizational security measures
- Cooperate with DPIA requests
- Notify Data Controller of sub-processors and obtain approval
- Notify of data breaches within 24 hours of discovery
- Allow audits and inspections by the Data Controller

5. Sub-processors

The Data Controller is notified of the following sub-processors. Changes will be communicated with at least 14 days prior notice:

For Google services, Standard Contractual Clauses (SCCs) apply for data transfers outside the EU.

6. Security Measures

The Processor implements the following technical and organizational security measures:

Encryption in Transit:

All communication uses HTTPS/TLS with modern encryption standards.

Password Security:

User passwords hashed with bcrypt or equivalent.

Access Control:

Role-based access: Company Admin, Dispatcher, Driver, Platform Admin.

Audit & Access Logs:

Admin access, company verifications, and status changes are logged.

Virus Scanning:

All documents asynchronously scanned for malware.

Immutable Records:

GPS tracks, documents, and status transitions are append-only.

Backup & Disaster Recovery:

Regular backups with disaster recovery procedures.

Vulnerability Management:

Regular security assessments, penetration testing, and patching.

7. Data Breach Notification

Upon discovery of a data breach, the Processor will notify the Data Controller within 24 hours, including:

- Nature and scope of the breach
- Likely consequences for data subjects
- Measures taken or proposed to contain the breach

8. International Data Transfers

For transfer of personal data to countries outside the EEA, the Processor will implement Standard Contractual Clauses (SCCs), as required under GDPR Article 46.

Google services (US-based) subject to SCCs.

9. Audits and Inspection

The Data Controller may conduct audits, inspections, and controls of the Processor's security measures. The Processor cooperates and provides reasonable access to facilities, documentation, and personnel.

10. Liability

Each party is liable for damages arising from breach of this Agreement. This does not limit liability under GDPR Article 82.

11. Duration and Termination

This Agreement follows the term of the service agreement. Upon termination, the Processor will delete or return personal data in accordance with Data Controller instructions.

12. Final Provisions

This Agreement is governed by Dutch law. Amendments are made in writing. This Agreement, together with Annexes A, B, and C, constitutes an integral whole.

Annex A — Processing Details

Categories of Data Subjects:

End users of the platform (employees, drivers, company contact persons)

Categories of Personal Data:

- Account data: name, email, phone number, hashed password
- Company data: KvK number, VAT number, address, contact information
- Vehicle data: license plate, make, model, type
- Geolocation data: GPS coordinates (latitude/longitude, 8 decimals)
- Delivery evidence: documents, photos, signatures
- Proposal data: rate numbers, notes, status transitions

Annex B — Sub-processors

Authorized Sub-processors:

All US-based sub-processors subject to Standard Contractual Clauses (SCCs).

Annex C — Technical and Organizational Measures

Encryption in Transit

All connections use HTTPS/TLS with modern encryption standards.

Password Hashing

User passwords hashed with bcrypt or equivalent.

Role-Based Access Control

Platform roles: Company Admin, Dispatcher, Driver, Platform Admin.

Audit & Access Logs

Admin access, company verifications, and status changes are logged.

Document Virus Scanning

All uploaded documents asynchronously scanned for viruses.

Immutable Records

GPS tracks, documents, and status transitions are append-only.

Backup & Disaster Recovery

RegiCargo maintains backup and disaster recovery procedures.

Vulnerability Management

Regular security assessments, penetration testing, and vulnerability patching.

Access Logs

Access logs maintained in accordance with policy.