Documentation Suite for Q-Platform, Q-TMS and Q-WMS

Effective Date: May 1st 2026
Last Updated: June 1st 2026

1. TERMS OF SERVICE / SAS AGREEMENT

Purpose
Defines the contractual relationship between the Platform and its customers.

Key Clauses

Definitions

- Platform
- Customer
- User
- Services
- Subscription
- Confidential Information
- Personal Data

License Grant
The Company grants Customer a limited, non-exclusive, non-transferable, revocable right to access and use the Platform during the Subscription Term. A subscription is free, but the Company is free to impose extra fees for extra functionality specific for the Customer. At all times the Company is free to not accept a Customer without any obligations or even with our giving reasons of refusal.

Acceptable Use
Users shall not:

- Violate applicable laws;
- Upload malicious code;
- Circumvent security measures;
- Reverse engineer the Platform;
- Access data belonging to other customers;
- Use the Platform for unlawful purposes.

Customer Responsibilities
Customers are responsible for:

- Accuracy of uploaded data;
- Maintaining account security;
- Obtaining all required consents;
- Compliance with applicable laws.

Intellectual Property
All intellectual property rights in the Platform remain the exclusive property of the Company.

Service Availability
The Company will use commercially reasonable efforts to maintain Platform availability but does not guarantee uninterrupted service.

Fees and Payment

- Usage of the Platform is free, some additional Services are not.. Always see the latest price list as advertised on the Company's website.
- Payment terms; The Platform is free, but using the Services (logistic services) is not. The company will invoice transport and handling, arranged in a separate agreement. Payment terms are payment within 14 days.
- Taxes; if taxes apply, these will accounted for from the Companies address to the Customer address as guidance. VAT therefore is applicable within the EU.
- Late payment provisions; the company has the right, when payments are late to suspend the logistic Services
- Suspension rights; the Company has every right to suspend a Customer's account at any moment if and when a payment is late, customers responsibilities are breached or any situation the company finds suit.

Confidentiality

Mutual confidentiality obligations covering technical, commercial and project information.

Warranties
Limited warranty that the Platform will substantially perform as described.

Disclaimer
To the maximum extent permitted by law, services are provided "as available" and "as is."

Limitation of Liability
Typical cap:

- Total liability limited to Services paid during the preceding 3 months.
- Exclusions for indirect, consequential and special damages.

Indemnification
Customer indemnifies Company against claims arising from Customer Data and unlawful use.

Term and Termination

- Subscription term
- Renewal
- Termination for breach
- Effect of termination
- Data export period

Governing Law

- Netherlands law

Jurisdiction
Exclusive jurisdiction of competent courts in:

- Amsterdam, Netherlands

2. DATA PROCESSING AGREEMENT (ARTICLE 28 GDPR)
PARTIES

All users of the Q-Platform, Q-TMS, Q-WMS directly or indirectly through an online connection; customers.
and the Processor Qonnected-Logistics BV

Subject Matter
Provision of the Platform and processing of Customer Personal Data.

Duration
For the duration of the SaS Agreement.

Nature of Processing

- Collection
- Storage
- Organization
- Retrieval
- Consultation
- Transmission
- Deletion

Categories of Data Subjects

- Employees, users by role or user definitions; so-called "clients"
- (Sub) Contractors, also know as "clients" connected to a "project"
- Suppliers of building materials, machinery, people or other services to the "clients"
- Carriers of building materials, machinery, people or other services to the "clients"
- Property owners as in warehouse owners or lessees
- All machinery and trucks used in transports including CO2 usage, in type, capacity, drivers and all fields used in a Transport Management System.
- All transport movements and its contents, including but not exclusively; GPS data, fixed locations, timelines, capacity, weights, volume, storage etc.
- All fields used in a Warehouse Management System, such a capacity, storage, cross dock, etc.
- Materials list, defined as materials used in the construction sector in the widest sense, including all specs.
- Machinery list, defined as machinery used in the construction sector in the widest sense, including all specs.
- People list, here defined as external people hired by the clients, nameless when not hired, named if hired For the named part all GDPR rules apply, as in Personal Data.

Categories of Personal Data

- Names
- Email addresses
- Postal addresses
- Telephone numbers
- Project information
- User account information
- Where applicable: availability
- Where applicable: education and experience
- Where applicable: more personal information for social security numbering, bank account information and more; for legal correct renumeration

Processor Obligations
Processor shall:

- Process only on documented instructions.
- Maintain confidentiality.
- Implement Article 32 GDPR security measures.
- Assist Controller with data subject requests.
- Assist with DPIAs.
- Notify Controller of personal data breaches without undue delay.
- Delete or return data upon termination.
- Make information available for audits.

Subprocessors
Processor may engage subprocessors provided:

- Prior notice is given;
- Equivalent contractual protections are imposed;
- Processor remains fully liable.

International Transfers
Transfers outside the EEA require:

- Adequacy decisions;
- SCCs; or
- Other approved transfer mechanisms.

Security Measures
Minimum controls:

- Encryption at rest and in transit;
- Access controls;
- Logging and monitoring;
- Backup procedures;
- Vulnerability management;
- Incident response procedures.

3. ADDITIONAL COMPLIANCE POLICIES

A. Cookie Policy

Categories of Cookies
Strictly Necessary
Authentication, security and session management.
Functional
User preferences and settings.
Analytics
Platform performance and usage measurement.
Marketing
Only where applicable and with prior consent.
Consent
Users located in the EEA shall be presented with a consent banner meeting GDPR and ePrivacy requirements.
Withdrawal
Users may withdraw consent at any time.

B. Information Security Policy

Technical Controls

- Encryption (TLS 1.2+)
- Multi-factor authentication
- Role-based access control
- Security monitoring
- Vulnerability scanning
- Secure software development lifecycle

Organisational Controls

- Employee confidentiality obligations
- Security awareness training
- Vendor due diligence
- Incident management procedures

Business Continuity

- Disaster recovery procedures
- Backup testing
- Recovery objectives

C. Acceptable Use Policy

Customers may **not:**

- Use the Platform for unlawful activities;
- Upload malware;
- Interfere with Platform operations;
- Attempt unauthorised access;
- Use automated scraping tools;
- Infringe intellectual property rights.

Violations may result in suspension or termination.

D. Data Retention & Deletion Policy

Account Data
Retained during active (free) subscription and for a reasonable period thereafter.
Project Data
Retained according to customer instructions and legal obligations.
System Logs
Typically retained for security and compliance purposes.
Deletion
Data shall be securely deleted or anonymised following expiration of retention requirements.

E. Incident & Data Breach Policy

Detection
Continuous monitoring and incident reporting procedures.
Investigation
Security incidents are investigated promptly.
Notification
Where required under Articles 33 and 34 GDPR:

- Supervisory authority notified within 72 hours where applicable.
- Affected customers notified without undue delay.

Remediation
Corrective actions implemented to prevent recurrence.

F. Subprocessor Policy
The Company shall maintain a current list of subprocessors including:

- Cloud hosting providers
- Email service providers
- Authentication providers
- Analytics providers
- Support providers

Customers shall be informed of material changes.

G. Service Level Agreement (SLA)
Availability
99.9% monthly uptime.
Support

- Critical incidents: 1-hour response during working hours, 4 hours outside working hours. Critical incidents are only handled in person by phone by the Processor's appointed account manager.
- High priority: 1 business day. Processor offers aan online ticket system.
- Standard: 2 business days by Processors online ticket system

H. Confidentiality and Non-Disclosure Policy
All employees, contractors and subprocessors shall be subject to written confidentiality obligations covering:

- Customer Data
- Project information
- Technical information
- Commercial information
- Trade secrets

This policy survives termination of employment and contractual relationships.
Remark: The processor offers data to all customers, to be used as information which is supposed to be of help for customers in general. This data is shared under Q-ADS; Q Advanced data Sharing. This is always done anonymous and can't be refaced to particular customers.
For enterprise customers in Germany and the Netherlands, it is also common to add:

- **EU AI Act Compliance Statement** (if any AI features are used)
- **Records of Processing Activities (Article 30 GDPR)** (internal)
- **Data Protection Impact Assessment (DPIA) Procedure** (internal)
- **Whistleblower Policy** (required or expected for many EU companies)
- **Accessibility Statement** (especially for public-sector customers)
- **Trust Center Documentation** (security, privacy, uptime, subprocessors, certifications, penetration testing summaries). (Knowledge base)

4. ENTERPRISE SAS GOVERNANCE, SECURITY, PRIVACY AND COMPLIANCE FRAMEWORK

NIS2 Compliance Commitment
The Company shall maintain a cybersecurity program aligned with the requirements of the EU NIS2 Directive and applicable national implementing legislation.
The Company shall:

- Maintain risk management measures appropriate to the nature, scale, and complexity of its operations.
- Implement incident detection and response procedures.
- Maintain business continuity and disaster recovery capabilities.
- Conduct periodic security risk assessments.
- Maintain supply chain security controls for third-party service providers.
- Provide security awareness training to personnel.
- Monitor vulnerabilities and apply security patches in a timely manner.
- Maintain documented cybersecurity governance processes.

Where required by law, the Company shall cooperate with competent supervisory authorities and provide relevant information concerning significant cybersecurity incidents.

Data Residency Commitment

Unless otherwise agreed in writing, Customer Data and Personal Data shall be hosted and processed exclusively within the European Economic Area (EEA).

The Company shall not transfer Customer Data outside the EEA unless:

- An adequacy decision exists;
- Standard Contractual Clauses are implemented;
- Another lawful transfer mechanism under Chapter V GDPR applies.

The Company shall disclose all data hosting and processing locations upon request.

Technical and Organisational Measures (TOMs)

Access Security

- Role-based access controls (RBAC).
- Least-privilege access model.
- Multi-factor authentication for administrative users.
- Segregation of duties for privileged accounts.

Encryption

- TLS encryption for all external communications.
- Encryption of data at rest using industry-standard encryption technologies.
- Secure key management procedures.

Infrastructure Security

- Network segmentation.
- Firewalls and intrusion detection mechanisms.
- Continuous monitoring and logging.
- Anti-malware protection.

A

pplication Security

- Secure software development lifecycle (SSDLC).
- Code review procedures.
- Dependency and vulnerability scanning.
- Security testing before deployment.

Operational Security

- Background screening where permitted by law.
- Confidentiality agreements.
- Security awareness training.
- Incident management procedures.

Business Continuity

- Regular backups.
- Disaster recovery testing.
- Documented recovery procedures.
- Business continuity planning.

Security Incident and Breach Notification

The Company shall maintain a documented incident response program.

In the event of a confirmed Personal Data Breach, the Company shall:

- Notify the Customer without undue delay and, where feasible, within seventy-two (72) hours after becoming aware of the breach.
- Provide available information regarding:
    - Nature of the incident;
    - Categories of affected data;
    - Approximate number of affected records;
    - Likely consequences;
    - Remediation measures undertaken.

The Company shall cooperate with the Customer in fulfilling regulatory notification obligations.

Annual Security Assessments

The Company shall perform:

- Annual independent penetration testing.
- Internal vulnerability assessments.
- Continuous vulnerability monitoring.
- Periodic access reviews.
- Annual disaster recovery testing.

Executive summaries of security assessments may be provided to Customers under confidentiality obligations.

Vulnerability Disclosure Program

The Company shall maintain a vulnerability disclosure process allowing security researchers and Customers to report security vulnerabilities.

Reported vulnerabilities shall be:

- Logged and tracked.
- Risk-rated.
- Remediated according to severity.
- Verified following remediation.

Cyber Insurance
The Company shall maintain commercially reasonable cyber liability insurance covering:

- Data breaches;
- Privacy violations;
- Security incidents;
- Business interruption arising from cyber events.

Evidence of coverage may be provided upon reasonable request.

Audit Rights
Subject to reasonable notice and confidentiality obligations, Enterprise Customers may request information reasonably necessary to verify compliance with:

- GDPR;
- Data Processing Agreements;
- Security obligations;
- Applicable laws.

The Company may satisfy audit requests through:

- Independent certifications;
- Audit reports;
- Security questionnaires;
- Third-party assessments.

On-site audits shall be limited to circumstances where alternative evidence is insufficient.

Exit Assistance and Data Portability
Upon termination of the Agreement:

- Customer may export Customer Data in a commonly used machine-readable format.
- Customer shall be provided a minimum export period of ninety (90) days unless otherwise agreed.
- Following expiration of the export period, Customer Data shall be securely deleted unless retention is legally required.

Reasonable transition assistance may be provided under a separate Statement of Work.

Artificial Intelligence Governance
The Platform includes AI-enabled functionality, the Company shall:

- Maintain compliance with the EU AI Act and applicable legislation.
- Implement human oversight mechanisms.
- Maintain data governance controls.
- Monitor model performance and risks.
- Document AI-assisted outputs where appropriate.
- Prohibit the use of Customer Data for training general-purpose AI models unless expressly authorised by the Customer.

The Company shall provide transparency regarding AI functionality incorporated into the Platform.

ESG and Sustainability Commitment
The Company shall conduct its operations in accordance with applicable environmental, social, and governance principles, including:

- Compliance with applicable labor laws.
- Anti-discrimination commitments.
- Ethical business conduct.
- Anti-corruption controls.
- Responsible management of suppliers and subcontractors.

Source Code Escrow (Enterprise Option)
For designated enterprise subscriptions, the Company may maintain a source code escrow arrangement.
Release conditions may include:

- Insolvency;
- Permanent cessation of services;
- Material breach of contractual support obligations.

Terms shall be governed by a separate escrow agreement.

Confidentiality
Confidential Information includes:

- Customer Data;
- Project information;
- Project addresses;
- Material specifications;
- Technical documentation;
- Trade secrets;
- Pricing information;
- Security documentation.

Confidentiality obligations shall survive termination of the Agreement for a minimum period of five (5) years, and indefinitely for trade secrets and Personal Data where required by law.

Regulatory Compliance
The Company shall maintain compliance programs addressing:
Data Protection

- GDPR
- Dutch UAVG
- German BDSG

Cybersecurity

- NIS2
- National cybersecurity regulations

Corporate Compliance

- Anti-corruption laws
- Anti-money laundering laws where applicable
- Export control regulations

Whistleblower Protection

- EU Whistleblower Directive
- German Hinweisgeberschutzgesetz
- Dutch Whistleblower Protection Act

Accessibility
The Platform shall be designed with reasonable efforts toward compliance with:

- WCAG 2.1 AA standards;
- European Accessibility Act requirements where applicable.

Certifications and Assurance
The Company intends to maintain or obtain the following certifications and assurance reports:

- ISO/IEC 27001
- ISO/IEC 27701
- SOC 2 Type II
- ISO 27017
- ISO 27018

Certification status shall be communicated through the Company's Trust Center.

Trust Center
The Company shall maintain a Trust Center containing:

- Privacy Notice;
- Data Processing Agreement;
- Subprocessor List;
- Security Overview;
- Incident Response Summary;
- Uptime Status;
- Certification Information;
- Vulnerability Disclosure Process;
- Contact Information for Security and Privacy Requests.

The Trust Center shall serve as the primary repository for customer due diligence and compliance documentation.
This language can be incorporated directly into:

1. **Terms of Service / Master Subscription Agreement**
2. **Data Processing Agreement (DPA)**
3. **Privacy Notice**
4. **Information Security Policy**
5. **SLA**
6. **Trust Center**
7. **Enterprise Security Addendum**