LEGAL

Data Processing Agreement

QC Mind Int · Version 1.0 · 19 October 2026 ·

This Data Processing Agreement ("DPA") forms part of the Terms of Service between QC Mind, Curicó, Chile ("Processor") and the Client named in the service order ("Controller"). It applies whenever the Processor processes personal data on behalf of the Controller while providing inspection services and the QC Mind Int platform (the "Service"), and is written to meet Article 28 of the EU General Data Protection Regulation (GDPR) and the UK GDPR.

1. Subject matter, duration, nature and purpose

SUBJECT MATTER	Recording, storing and analysing quality inspections of fruit products at the Controller's suppliers in Chile, and operating the platform where the Controller's users consult them.
DURATION	The term of the Terms of Service, plus the 90-day export period after termination.
NATURE	Collection on site by the Processor's inspectors, storage, structuring, analysis, display to authorised users, export, backup and deletion.
PURPOSE	To provide the Service the Controller contracted; no other purpose.
CATEGORIES OF DATA SUBJECTS	The Controller's employees and authorised users; employees and contacts of the Controller's suppliers (plant staff, growers); the Processor's inspectors.
CATEGORIES OF PERSONAL DATA	Name, work email, role, language; sign-in metadata (device, IP, time); names of people appearing in inspection records (inspector, supplier contact); photos taken at supplier sites, which may incidentally show people; free-text notes.
SPECIAL CATEGORIES	None are required. The Controller shall not load special-category data into the platform.

2. Processor obligations

The Processor shall:

1. process personal data only on the Controller's documented instructions, which are the Terms of Service, the service order and the Controller's use of the platform, unless required by law to do otherwise, in which case it informs the Controller before processing where the law allows;
2. ensure that persons authorised to process the data (inspectors, support staff) are bound by confidentiality;
3. implement the technical and organisational measures described in Annex 1;
4. engage sub-processors only as set out in clause 4;
5. assist the Controller, taking into account the nature of the processing, in responding to data-subject requests, by appropriate technical measures (export, correction and deletion of records);
6. assist the Controller with security, breach notification, data protection impact assessments and prior consultation, taking into account the information available to the Processor;
7. at the Controller's choice, delete or return all personal data at the end of the Service, and delete existing copies, unless the law requires storage; by default data is kept 90 days for export and then deleted, including from backups within a further 30 days;
8. make available the information necessary to demonstrate compliance with this DPA and allow for and contribute to audits, including inspections, conducted by the Controller or an auditor mandated by the Controller, with reasonable notice, at most once a year unless required by a supervisory authority or after a breach, and at the Controller's cost if the Processor is found compliant;
9. inform the Controller immediately if, in its opinion, an instruction infringes applicable data-protection law.

3. Personal data breach

The Processor notifies the Controller without undue delay, and in any case within 48 hours, after becoming aware of a personal data breach affecting the Controller's data, with a description of the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences, and the measures taken or proposed. Notification goes to the Controller's administrator accounts by email.

4. Sub-processors

The Controller gives general authorisation to the sub-processors below. The Processor informs the Controller of any intended addition or replacement at least 30 days in advance by email to the Controller's administrators; the Controller may object on reasonable grounds within that period, in which case the parties will seek a solution and, failing one, the Controller may terminate the

affected Service without penalty. The Processor imposes on each sub-processor the same data-protection obligations as in this DPA and remains liable for their performance.

SUB-PROCESSOR	PURPOSE	LOCATION
Vultr Holdings (The Constant Company, LLC)	Cloud server and backups hosting the platform and the data	Santiago, Chile (data centre); United States (company)
Resend, Inc.	Sending transactional emails (invitations, notices, daily summaries)	United States
Functional Software, Inc. (Sentry)	Error reporting (technical context only; no record content)	United States

5. International transfers

Personal data is stored in Chile. Where the Controller is established in the European Economic Area or the United Kingdom, the transfer of personal data to the Processor in Chile and to the sub-processors above is made under the Standard Contractual Clauses adopted by the European Commission (Decision (EU) 2021/914, Module Two: controller to processor) and, for the UK, the International Data Transfer Addendum, which the parties incorporate by reference and complete as follows: the Controller is the data exporter, the Processor is the data importer, Clause 7 (docking) applies, Option 2 of Clause 9 (general authorisation, 30 days) applies, the governing law and forum under Clauses 17 and 18 are those of the EU Member State in which the Controller is established (or Ireland if it is not established in a Member State), and Annexes I and II are completed by clauses 1 and 4 and Annex 1 of this DPA.

6. Controller obligations

The Controller is responsible for the lawfulness of the data it loads or asks the Processor to collect, for informing its suppliers and staff that inspections are recorded on the platform (including photos at supplier sites), for managing its users' access, and for its instructions to the Processor.

7. Liability and order of precedence

The liability provisions of the Terms of Service apply to this DPA. In case of conflict, this DPA prevails over the Terms of Service for data-protection matters, and the Standard Contractual

Clauses prevail over this DPA.

Annex 1 · Technical and organisational measures

- **Access control**: individual accounts; salted password hashes (scrypt); optional two-factor authentication (TOTP) with recovery codes; role-based permissions; sessions expire after 30 days and on deactivation; rate limiting on sign-in and password reset; new-device sign-in notifications; email-domain restriction per company.
- **Tenant isolation**: every request is scoped to the user's company; automated tests verify that no company can read another's data on each release.
- **Encryption in transit**: HTTPS with automatically renewed certificates; secure, HTTP-only cookies; HTTP redirected to HTTPS.
- **Availability and backups**: hourly database backups kept 48 hours, daily backups kept 30 days, full-server backups by the hosting provider; documented and tested point-in-time restore; automatic rollback of failed releases.
- **Logging and traceability**: activity log of sign-ins, changes and Processor staff access, readable by the Controller; versioned specifications.
- **Confidentiality**: Processor staff bound by confidentiality; access by the support team limited to the companies they support and logged.
- **Deletion**: export on demand; deletion at the end of the Service after the 90-day export period; backups expire within 30 further days.
- **Incident response**: monitoring of server errors; notification of breaches within 48 hours as in clause 3.

Acceptance

This DPA is accepted when the Controller signs a service order or quote that refers to it. A countersigned copy is provided on request by writing to contacto@qcmind.cl.