

Panel Quote – API Privacy Policy

Version 1.0 - Effective date: 1 February 2024

1. Purpose and Scope

This Privacy Policy explains how Panel Quote Limited (“PQL,” “we,” “our,” or “us”) collects, uses, discloses, and protects Personal Information processed through the PQL API (“API”). It applies to Personal Information submitted, stored, or accessed via the API by you (“Developer,” “Integrator,” or “you”) when integrating your application, service, or system with PQL’s platform.

Note: This Privacy Policy forms part of, and is incorporated by reference into, the Panel Quote API Terms & Conditions. Capitalised terms have the meaning set out in those Terms unless defined otherwise below.

2. Definitions

- **Personal Information:** Any information about an identified or reasonably identifiable individual, as defined in the NZ Privacy Act 2020 and the AU Privacy Act 1988 (Cth).
 - **Process / Processing:** Any operation performed on Personal Information, including collection, storage, use, disclosure, transfer, or deletion.
 - **End-User:** An individual whose Personal Information is processed via the API (for example, vehicle owner, insurer representative, or repair-shop contact).
-

3. Categories of Personal Information Collected via the API

We may process the following types of Personal Information:

- Contact data (name, phone, email)
- Vehicle identifiers (for example, VIN or registration linked to owner data)
- Images or attachments (for example, vehicle-damage photos, licence-plate shots, PDF invoices) that may incidentally include Personal Information or EXIF metadata

- Insurance-claim or work-order references (claim number, sum insured, assessment type)
- Audit logs (IP address, API key, timestamps, request metadata)

Children's Data: The API is not intended for children under 16 years of age, and we do not knowingly process their Personal Information.

Special-Category Data: You warrant that you will not deliberately transmit special-category data (for example, health, biometric, or criminal-record information) unless explicitly authorised in writing by PQL.

4. Lawful Basis for Processing

We rely on the following legal bases when processing Personal Information:

- **Contractual necessity** – to deliver API services under the API Terms.
- **Legitimate interests** – such as fraud prevention, security monitoring, and service improvement.
- **Legal obligation** – to comply with NZ and AU privacy or financial-services regulations.

You must ensure you have a lawful basis (for example, user consent or insurer-policy terms) before submitting End-User data via the API.

5. How We Use Personal Information

- **Service delivery:** Routing estimate data and returning labour-rate or part-pricing information.
- **Security and abuse monitoring:** Logging API calls, identifying anomalous traffic, and enforcing rate limits.
- **Analytics and improvement:** Using aggregated, de-identified data to optimise performance.
- **Legal and compliance:** Maintaining audit trails and responding to lawful requests.

We do not rent or sell Personal Information.

6. Disclosure of Personal Information

Personal Information may be disclosed to:

1. **Service providers** – including SiteHost (Auckland-based data centres) and log-monitoring tools.

2. **Authorised counterparties** – for example, insurers receiving quotes.
 3. **Regulators or law enforcement** – where legally required (for example, the NZ Privacy Commissioner, OAIC, courts, or police).
 4. **Corporate transactions** – such as mergers, acquisitions, or asset sales, subject to confidentiality obligations.
-

7. International Transfers

- **Primary data residency:** All customer data is stored in SiteHost’s Auckland data centres, New Zealand.
 - **Transfers to Australia:** May occur (for example, for insurer access) and are handled under APP 8 “reasonable-steps” safeguards because Australia offers comparable privacy protection.
 - **Other international transfers:** Will only occur under contractual safeguards (for example, EU Standard Contractual Clauses) or with explicit consent.
-

8. Security Measures

- **Data in transit:** Encrypted using HTTPS and TLS 1.2 or higher.
 - **Data at rest:** Encrypted with AES-256 on SiteHost-managed volumes.
 - **Access control:** Scoped API keys, role-based permissions, and MFA for administrators.
 - **Monitoring and logging:** Centralised logs with anomaly alerting.
 - **Penetration testing:** Annual CREST-certified tests with critical issues remediated within five Business Days.
 - **Attachments:** Stored in encrypted object storage with public-read access disabled.
-

9. Data Retention and Deletion

Data Type	Default Retention	Deletion Trigger
Transactional logs	365 days	Automatic deletion
Estimate and quote data	Seven years (regulatory)	Manual deletion on request, if lawful
Vehicle images / attachments	Seven years (regulatory)	Manual deletion on request, if lawful
API keys / test accounts	Until revoked (test keys auto-expire after 30 days)	Immediate on revocation
Encrypted backups	35 days	Automatic deletion

Upon termination of access (API Terms § 7.3) you must delete all Personal Information obtained via the API and certify deletion within five Business Days.

10. Your Responsibilities as Developer / Integrator

1. **Lawful collection** – obtain any required consents or provide appropriate notices under NZ and AU law.
 2. **Minimum-necessary principle** – transmit only data required for each API call.
 3. **Security on your side** – use HTTPS, secure storage, and access logging for any cached data.
 4. **Breach notification** – email support@panelquote.co.nz within 24 hours of any suspected breach involving Personal Information and provide daily updates so PQL can meet regulatory deadlines.
-

11. Rights of Individuals

End-Users have the right to:

- Request access to Personal Information held via the API.
- Request correction of inaccurate data.
- Lodge a complaint with the NZ Privacy Commissioner or the OAIC.

If PQL forwards a Data-Subject Request (DSR) relating to data you supplied, you must provide all information PQL reasonably requests within five Business Days.

Contact for DSRs and complaints: **support@panelquote.co.nz**

12. Liability and Indemnity

12.1 Indemnity – You agree to indemnify, defend, and hold harmless PQL and its directors, officers, employees, and agents from and against any and all losses, damages, liabilities, penalties, costs, and expenses (including reasonable legal fees) arising out of or relating to:

- a. Your breach of this Privacy Policy or the API Terms;
- b. Any Personal Information processed via the API by you in violation of applicable law; or

c. Any claim by an End-User or third party resulting from your acts or omissions.

12.2 Liability cap – To the maximum extent permitted by law, PQL’s aggregate liability arising out of or in connection with this Privacy Policy, the API, or any Personal Information processed through the API, whether in contract, tort (including negligence), equity, statute, or otherwise, is limited to NZD 10,000 **or** the total fees paid by you to PQL for API access in the 12 months preceding the event giving rise to the claim, whichever is lower. Nothing in this clause limits liability for wilful misconduct or fraud.

13. Updates to This Policy

We may amend this Privacy Policy from time to time. Any material changes will be posted at <https://panelquote.co.nz/privacy> and we will provide at least 30 days’ prior notice via the API dashboard or email.

If you do not agree to a material change, you must cease using the API and certify deletion of all Personal Information obtained via the API within that 30-day notice window. **Continuing to use the API after the effective date constitutes acceptance of the revised Policy.**

14. Contact

Privacy Officer – Panel Quote Limited

Email: support@panelquote.co.nz

By using the API you confirm that you have read, understood, and will comply with this Privacy Policy.