

PAYMARK PRIVACY POLICY

Effective Date: 2 June 2026

1. Who We Are

This policy applies to **Paymark Ltd** ("we", "us"). We are the leading New Zealand 'Fintech', and processor of secure payments and trusted transactions.

In New Zealand, we operate as a payments processor and a **digital intermediary**. This means we often act as the secure bridge between you, your bank (Data Holder), and the businesses you want to pay or share data with (merchants). This policy applies to both personal information we collect from our customers (merchants) and to information we collect by processing transactions on behalf of merchants and banks.

2. Our Approach to Privacy

We value trust above all else. We handle your information in accordance with:

- The **Privacy Act 2020** and its Information Privacy Principles (**IPPs**).
- The **Customer and Product Data Act 2025 (CPD Act)**, specifically where we act as an Accredited Requestor for secure consent-based sharing of your banking data (**Open Banking**).

We only collect personal data where (and to the extent) reasonably necessary in connection with our services or functions.

3. Information We Collect

We collect personal information in three main ways:

A. Information you give us directly

- **Contact details:** Name, email, phone number (e.g., if you contact support or use our website).
- **Payment details:** Bank account details to process direct debits, or card details.
- **Device Details:** IP address, domain name, device type, operating system, browser information, screen size, geographic location, website usage information including cookies.
- **Verification data:** ID documents or biometrics if we are required to verify your identity for anti-money laundering (AML) or digital identity services.

B. Information we collect from others

We collect information from the following third-party sources

Source	Information Collected	Purpose
Your Bank (Data Holder), Resellers / Partners	<ul style="list-style-type: none"> • Account balances, transaction history, customer details, 	To facilitate the services you have requested, or to establish a merchant account with us.

Source	Information Collected	Purpose
	<ul style="list-style-type: none"> Information required to provide you with access to our payment processing facilities 	
Merchants	Transaction amounts, time, location, card tokens, authorisation data.	To process payments and prevent fraud.
Fraud Agencies & Identity Issuers	Credit scores, identity verification flags, fraud alerts.	To meet AML/CFT obligations and protect the payment network.

C. Information we access as an Accredited Requestor

When you use our services to make a payment using our API account-to-account payment services (Online Eftpos and Direct Pay):

- **Designated Customer Data:** Account balances, transaction history, or customer details held by your bank.
- **Authorisation Data:** Records of your explicit consent to share this data.

We collect personal information in a manner that is designed to be fair and not unreasonably intrusive.

We assign and use unique identifiers (such as merchant or terminal IDs) only where necessary, and we do not use them in a way that could unfairly disadvantage you.

4. How We Use Your Information (Lawful Purpose)

We only use your data for the purpose for which it was collected.

Purpose	Description
Processing Payments	To route your payment to the correct bank and confirm the transaction to the merchant.
Open Banking (Accredited Requestor)	To access and retrieve your data from your bank and deliver it to the party you have authorised (e.g. a merchant). We do not access or store authorisation data for our own use beyond what is necessary to provide services or comply with legal obligations.
Security & Fraud	To detect unusual patterns, prevent fraud, and secure the payments ecosystem.
Compliance	To meet our obligations under NZ and any other relevant laws (e.g., AML/CFT Act, CPD Act). Communicating with Merchants about terminals connected to our systems

Purpose	Description
	(e.g. relating to software or hardware upgrades)
Analytics	Understanding how people use our website, merchant portals, and apps.
Marketing	Providing you with information about our products and services (e.g. via email or text message), subject to your consent to receive such messages

Automated Decision Making: We may use automated systems to assist with fraud detection or compliance, but decisions with legal or significant effects are subject to appropriate safeguards.

5. Your Control

Under the **Customer and Product Data Act**, you are in control of your data.

- **Explicit Consent:** We will never process a payment without your authorisation. You will be redirected to your bank to approve payments or consents.
- **Managing Access:** You can view, manage, and revoke your authorisations at any time via your banks mobile app or online bank services.
- **Revocation:** If you cancel a consent, we will not process any further payments that would have been authorised by that consent after the time of cancelling.

6. Sharing Your Information

We do not sell your personal information. We only share it when necessary:

- **With Merchants/Requestors:** Only the data you have authorised us to pass on to complete a transaction or service.
- **With Banks/Data Holders:** To initiate a payment or data request you have asked for.
- **With Service Providers:** IT, cloud storage, and security vendors who support our infrastructure (subject to strict confidentiality).
- **With Regulators:** If required by law (e.g., The Privacy Commissioner, FMA, Police, or our AML / CFT supervisor).
- **Business Transitions:** If our ownership changes or if we sell part of our business, your personal information may be transferred to the new owner, but would remain subject to this Privacy Policy.

7. Storing and Protecting Information

- **Security:** We use industry-standard encryption, tokenization, and access controls to protect your data.
- **Retention:** We hold your data only as long as necessary for the purpose (or as required by law), after which it is securely deleted or anonymized.

8. International Transfers

We may process data in Australia, Europe, or other locations where cloud computing services are provided from.

- We ensure your data remains protected by relying on **comparable safeguards** (IPP 12).
- Transfers to European locations are protected by **GDPR standards**, which are recognised as providing protection at least equal to New Zealand law.

9. Your Rights

Under the Privacy Act 2020, you have the right to:

1. **Ask for access** to the personal information we hold about you.
2. **Ask for correction** if you believe the information is wrong.

We'll aim to respond to any requests within a reasonable time frame, taking into account the level of complexity and volume of information involved.

If a privacy breach occurs that is likely to cause serious harm, we will notify affected individuals and the Office of the Privacy Commissioner as required by law.

Processing of EU Personal Data (GDPR)

If you are in the EU or an EU citizen, we process your personal data in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR). We rely only on the following lawful bases: consent, performance of a contract, our legitimate interests (balanced against your rights), legal obligations, or legal claims.

You have the right to access, correct, delete, restrict, or object to our processing of your data, and to request your data in a portable format. We collect only the data we need, keep it accurate, store it only for as long as required for the relevant purpose, and limit access to authorised personnel.

You may contact our Privacy Officer to exercise your GDPR rights.

To exercise these rights, or if you have a complaint about how we handled your Open Banking authorisation:

Contact our Privacy Officer:

- **Email:** support@paymark.co.nz
- **Address:** Level 18, 88 Shortland St, Auckland 1010

If we are unable to resolve your complaint about how we handle your Open Banking transactions or other transaction processing services, we are a member of Financial Services Complaints Ltd, which is an independent service for dispute resolution and you may lodge a complaint with them. Information on how to do so can be found on their website, <https://fscl.org.nz>

10. Changes to this Policy

We may update this policy to reflect changes in the Privacy Act, the CPD Act or our technology. The latest version will always be available on our website.