

PĒRL DATA PROTECTION POLICY

Last Updated: 22 June 2026

This Data Protection Policy ("Policy" or "DPP") sets out the basis on which PĒRL Pte. Ltd. and its corporate affiliates (collectively, "PĒRL", "we", "us", or "our") collect, use, disclose, process, or otherwise handle your Personal Data in accordance with the Singapore Personal Data Protection Act 2012 (No. 26 of 2012) (the "PDPA").

Section 1: Scope and Operational Capacity

1.1 Application of this Policy

This Policy governs the processing of Personal Data across all touchpoints within the PĒRL ecosystem, including but not limited to:

- (a) The primary PĒRL digital marketplace platform;
- (b) Our proprietary artificial intelligence agent ("Whisk"); and
- (c) The PĒRL B2B Ad-Locum Portal.

1.2 Statutory Capacities

For the purposes of applicable data protection laws, PĒRL operates in two distinct legal capacities depending on the context of the data transaction:

Data Controller — Management of platform accounts, user profiles, transactional interfaces, and general marketplace infrastructure. PĒRL independently determines the purposes and specific technical means of processing.

Data Intermediary — Processing of specific operational or patient data strictly on behalf of, and under the explicit instructions of, our partner clinics. PĒRL acts solely as a data intermediary under contract, subject to the security and retention obligations under the PDPA.

1.3 Technological Horizons and Evolution

The specific provisions of this Policy applicable to your interaction with us will depend on the nature of your transactions and agreements as they relate to PĒRL's development horizons:

- (a) Horizon 1: Preventive dental care and off-peak clinic capacity yield management.
- (b) Horizon 2: B2B Ad-Locum healthcare staffing and clinical labor matching.
- (c) Horizon 3: Proactive longevity services and Continuous Context Engines.

1.4 Regulatory Exclusions

PĒRL operates strictly as an operational capacity-optimization, administrative routing, and clinical scheduling engine. PĒRL does not perform clinical diagnostics or medical interventions, and its software is not classified as Software as a Medical Device (SaMD). Partner clinics utilizing our platform are independently subject to sectoral Medical Laws (including the Healthcare Services Act 2020), which may impose overriding statutory duties that supersede standard PDPA obligations in specific healthcare scenarios.

Section 2: Scope of Personal Data

2.1 Definition of Personal Data

"Personal Data" refers to any data, whether true or not, about an individual who can be identified from that data, or from that data combined with other information to which PĒRL has or is likely to have access.

2.2 Categories of Personal Data Processed

Depending on the nature of your interaction with the platform, we may process the following categories of Personal Data:

- (a) Identity and Account Information: Full name, mobile telephone number, email address, and authentication telemetry (including Mobile One-Time Passwords (OTPs), Singpass records, or HealthHub verifications).
- (b) Operational and Scheduling Data: Calendar data synced from third-party applications (including Google Calendar and Apple Calendar) utilized exclusively to identify meeting vacancies for off-peak slot matching.
- (c) Biometric and Wearable Telemetry (Horizon 3): Health telemetry data, including but not limited to Heart Rate Variability (HRV), sleep architectures, and disrupted rapid eye movement (REM) cycles, synchronized via authorized external wearable devices (including Apple Watch, Oura Ring, and Whoop).
- (d) Unstructured Qualitative Data: Voice recordings, audio prosody (tone, pitch, and delivery speed), and qualitative journal logs processed via automated pipelines for administrative summaries and contextual routing.
- (e) Locum Professional Data: Ministry of Health (MOH) registration status (including Full Registration and Conditional Registration metrics), professional certifications, clinical credentials, and shift availability records.

2.3 Data Anonymization

Personal Data does not include information that has been subjected to irreversible technical anonymization. PĒRL implements robust safeguards to anonymize Personal Data where appropriate, specifically when aggregating fragmented platform data to generate marketplace intelligence, pricing benchmarks, and capacity yield metrics.

Section 3: Consent and Tiered Architecture

3.1 Consent Principle

By accessing the platform, creating an account, or transacting with PĒRL, you acknowledge and agree that your Personal Data may be Handled in accordance with this Policy.

3.2 Unbundled Tiered Consent Framework

To safeguard data subject autonomy, PĒRL utilizes an unbundled, tiered consent architecture:

- (a) Core Services (Mandatory Consent): Consent to process foundational identity, payment, and scheduling metrics is a strict prerequisite for platform onboarding, marketplace operations, and administrative routing.
- (b) Optional Enhancements (Explicit Opt-In Only): Separate, independent consent must be granted to activate Whisk AI's advanced capabilities, including biometric wearable integrations, continuous calendar synchronizations, and voice matrix analysis.

3.3 Revocation of Consent

You retain the right to withdraw consent for any or all categories of processing at any time. Withdrawal of consent for Optional Enhancements will not restrict your access to Core Services.

However, upon the revocation of permissions for calendar syncs, biometric tracking, or voice analysis, Whisk AI will be technically unable to provide proactive scheduling notifications, autonomous slot matching, or longitudinal wellness tracking.

Section 4: Collection Pathways

We collect Personal Data through the following lawful methodologies:

4.1 Foundational Platform Collection

- (a) Upon the submission of digital registration forms on the PĒRL web portal or mobile application;

- (b) Upon the execution of a booking request and the financial settlement of the platform intent deposit;
- (c) Via automated interactions with our "Passive Auditor" push-notification loops following clinical treatments;
- (d) Via administrative inputs executed by authorized partner clinic staff through the PĒRL Institutional Dashboard; and
- (e) Through digital correspondence with our customer service infrastructure via authorized messaging applications (including WhatsApp and Telegram) linked to our secure databases.

4.2 Supplementary Technology Collection

- (a) Via voice-native capture interfaces where audio data is processed for operational intent routing;
- (b) Through authorized application programming interfaces (APIs) connected to approved third-party wearable devices; and
- (c) Through the voluntary submission of text or audio logs into the Whisk AI inbox.

4.3 Third-Party and Proxy Data Representation

The platform permits authorized users to manage health logistics and scheduling for dependents or third parties. If you provide PĒRL with Personal Data relating to a third-party individual, you explicitly warrant and represent to PĒRL that you have obtained prior, explicit, and legally valid consent from that individual (or their lawful legal representative) to authorize the collection, use, and disclosure of their Personal Data under this Policy.

Section 5: Purposes of Processing and Disclosure

5.1 Facilitation of Marketplace Capacity and Appointments

We process Personal Data to fulfill our contractual and operational obligations, including:

- (a) Verifying user identity through national digital identity infrastructure (Singpass) to ensure regulatory compliance;
- (b) Analyzing scheduling metrics to predict clinical optimization options and route individuals to appropriate licensed practitioners;
- (c) Disclosing scheduling intent, specific treatment requirements, and basic identifiers to our verified network of participating clinics strictly to facilitate clinical care; and
- (d) Processing platform intent deposits to formalize contractual appointment bookings and mitigate clinic no-show rates.

5.2 Healthcare Operations and Yield Management

We process Personal Data to maintain the integrity of our marketplace infrastructure by:

- (a) Executing statistical anomaly detection on clinic billing claims via our "Passive Auditor" infrastructure to prevent billing discrepancies or under-declarations;
- (b) Generating real-time operational metrics and capacity notifications on institutional dashboards; and
- (c) Analyzing historical transaction parameters to identify and recommend specialized secondary healthcare pipelines (including dermatology, diagnostics, and proactive longevity protocols).

5.3 Artificial Intelligence and Advanced Infrastructure Processing

PĒRL leverages proprietary automated systems and large language models (Whisk) to:

- (a) Process multi-lingual or dialect-specific voice inputs to enhance accessibility for elderly demographics;
- (b) Maintain a localized, compounding memory matrix to support longitudinal health profile context across successive user interactions; and

(c) Process unstructured voice logs via automated encryption pipelines to generate administrative summaries for healthcare providers, thereby optimizing clinical session efficiency.

Section 6: Specific Data Subject Regimes

6.1 Healthcare Professionals and Ad-Locum Talent

If you utilize the platform as a medical professional via the PĒRL Locum Lab, we process your Personal Data to:

- (a) Verify professional credentials, practicing certificates, Ministry of Health registration categories, and supervisory frameworks;
- (b) Align your recorded availability with localized surges in off-peak patient demand at partner clinics; and
- (c) Provide centralized dashboards for scheduling management, credential tracking, and financial reconciliation.

6.2 Clinic Partners and Branch Personnel

If you access the PĒRL Institutional Dashboard or Terminal Fast-Switch interface, we process your data to:

- (a) Register corporate clinic entities, verify institutional identification metrics, and provision secure credential access for authorized staff; and
- (b) Facilitate secure data migration from legacy Clinic Management Systems (CMS) to PĒRL's cloud-based interfaces.

6.3 Proxy Caregivers and Dependent Distributions

Where users utilize cross-generational synchronization features to manage health logistics for elderly or technologically dependent family members, PĒRL executes processing strictly within a zero-trust verification architecture. Proxy access authorization requires explicit digital validation via Singpass authentication or the presentation of verified legal proxies to eliminate assumed or implied third-party consent.

Section 7: Third-Party Proxy Access Framework

7.1 Scope of Proxy Access

PĒRL provisions cross-generational synchronization capabilities allowing authorized users ("Caregivers") to coordinate logistics, book off-peak slots, and monitor preventive tracking for third-party individuals ("Dependents"). Data processed under this framework may encompass highly sensitive biometric, operational, and clinical scheduling records.

7.2 Dependent Categorization and Consent Thresholds

The technical activation of proxy access is strictly conditioned upon the legal status of the Dependent:

- (a) Minor Dependents (Under 21 Years of Age): The Caregiver must be a parent or legally recognized guardian. By registering a minor, the Caregiver provides explicit parental consent on behalf of that minor for all processing detailed under this Policy.
- (b) Adult Dependents (Aged 21 and Above): PĒRL rejects implied, verbal, or assumed third-party consent. Proxy access to an adult Dependent's profile will remain inactive until either: (i) the adult Dependent logs in via their independent Singpass credentials to explicitly authorize the link; or (ii) a certified digital copy of a valid legal instrument (including a registered Lasting Power of Attorney (LPA) or a court-issued Deputyship Order) is uploaded and verified by PĒRL's legal compliance team.

7.3 Caregiver Indemnity and Warranties

Whenever a Caregiver applies for or exercises proxy access to a Dependent's profile, the Caregiver explicitly warrants, represents, and covenants to PĒRL that:

(a) They possess the verifiable legal authority to provide the Dependent's National Identification Number (NRIC/FIN/Passport), contact info, and operational health metrics to PĒRL; and

(b) The Dependent has reviewed, understood, and consented to the processing of their Personal Data under this Policy.

(c) Indemnity Clause: The Caregiver agrees to fully and unconditionally indemnify, defend, and hold harmless PĒRL, its corporate affiliates, directors, officers, and employees from and against any and all administrative penalties, financial directions issued by the Personal Data Protection Commission (PDPC), third-party claims, legal costs, liabilities, or regulatory investigations arising directly or indirectly out of any misrepresentation, breach of warranty, or unauthorized proxy access caused by the Caregiver.

7.4 Absolute Revocation Rights

An adult Dependent retains an inalienable right to audit proxy access permissions and unilaterally revoke Caregiver links at any time. Upon receipt of a revocation request through our Data Protection Officer or directly via the application interface, PĒRL will immediately terminate the caregiver data link.

PĒRL disclaims all liability toward the Caregiver or any third party for any disruptions in care coordination, appointment cancellations, or tracking lapses resulting from a lawful data revocation executed by a Dependent.

Section 8: Insurance Integration and Cost Modeling

8.1 Aggregate Data Analytics

To optimize private healthcare capacity allocation and support the benchmarking of facility fees, PĒRL may utilize aggregated, completely anonymized transaction metrics for predictive cost modeling and premium optimization analyses.

8.2 Identifiable Health Telemetry Restrictions

Identifiable health telemetry, individual biometric records, and specific out-of-pocket transaction costs will never be disclosed to third-party insurance providers or Integrated Shield Plan (IP) underwriters without an explicit, standalone, granular opt-in consent flow.

This consent process is strictly decoupled from standard platform onboarding. Any data transfer executed under this section will be strictly confined to the minimum parameters necessary for specific claims assessment or premium structure calculations, in accordance with the Purpose Limitation Obligation of the PDPA.

Section 9: Cross-Border Transfers and Disclosures

9.1 Transfer Limitation Obligation

In the event that Personal Data is transferred to destinations outside the jurisdiction of Singapore, PĒRL ensures that such cross-border transfers comply strictly with Section 26 of the PDPA. We utilize mandatory Standard Contractual Clauses (SCCs), binding corporate rules, or other legally recognized transfer mechanisms to ensure that overseas recipients provide a standard of protection to the transferred Personal Data that is fully comparable to the protections mandated under the PDPA.

9.2 Authorized Classes of Recipients

Subject to compliance with applicable laws, your Personal Data may be disclosed to the following categories of third-party recipients, located either within or outside Singapore:

(a) Corporate subsidiaries, holding companies, and affiliates within the PĒRL corporate structure;

(b) Our participating network of anchor clinic partners (including Q&M Dental Group, Tanglin Dental Group, Royce Dental Group, and boutique clinic operators utilizing our capacity optimization engines);

- (c) Verified ad-locum medical professionals transacting via the B2B Locum Lab marketplace;
- (d) Technical service providers and database administrators supporting wearable device software integrations (including Apple HealthKit, Google Health Connect, Oura, and Whoop);
- (e) Authorized community agencies, social enterprises, and Active Ageing Centres (AACs) facilitating local patient onboarding;
- (f) Third-party information technology providers managing API bridges to national digital infrastructure (including Singpass and HealthHub) or legacy Clinic Management Systems;
- (g) Government ministries, statutory boards, or law enforcement authorities (including the Ministry of Health and GovTech) to ensure compliance with mandatory statutory rules or judicial orders;
- (h) Financial institutions, clearing houses, and payment gateways (including Stripe and PayNow) for the settlement of platform deposits and off-peak transaction fees; and
- (i) Lawfully authorized Caregivers, next-of-kin, or legal guardians utilizing our cross-generational tracking features.

Section 10: Telecommunication Marketing and DNC Compliance

10.1 Marketing Consent

Where you have explicitly indicated your consent via our platform interfaces to receive marketing, promotional, or promotional notifications, PĒRL may contact you using your registered Singapore telephone number(s) via voice calls, SMS, text formats, or integrated messaging applications. Marketing communications encompass notifications regarding dynamic off-peak slot discounts, product rollouts, and wellness marketplace offerings.

10.2 Do Not Call (DNC) Registry Override

By granting explicit marketing consent to PĒRL, you acknowledge and agree that such consent constitutes a valid, clear, and specific expression of intent that shall fully override any current or future registration of your Singapore telephone number(s) on the Singapore Do Not Call (DNC) Registry, pursuant to the provisions of the PDPA. You may opt out of marketing communications at any time via the application settings or by contacting our Data Protection Officer.

Section 11: Security, Retention, and Technical Protections

11.1 Security Arrangements

PĒRL implements appropriate administrative, physical, and technical safeguards, including AES-256 end-to-end encryption for qualitative data and biometric telemetry, to secure Personal Data against unauthorized access, collection, disclosure, copying, alteration, or accidental loss.

Notwithstanding these measures, you acknowledge that no digital transmission over the internet or cloud storage infrastructure can be guaranteed as entirely absolute, and PĒRL cannot warrant that its platforms are entirely immune to sophisticated cyber-attacks, malicious code, or security vulnerabilities.

11.2 Retention Limitation

PĒRL retains Personal Data only for as long as necessary to fulfill the legal or business purposes for which it was collected, or as required by applicable laws. We utilize automated data-destruction protocols, including Algorithmic Time Decay models within our Whisk AI architecture, to securely delete or permanently anonymize obsolete qualitative inputs and daily journal text strings once they no longer serve an operational purpose.

11.3 Exclusion of Medical Records Retention

PĒRL does not hold, maintain, or retain statutory medical records. All clinical case files, medical histories, and treatment records are compiled and held exclusively by the licensed partner clinics where care is delivered.

These partner clinics act as the independent Data Controllers for medical data. They are bound by separate medical regulations, including the Healthcare Services Act 2020, which mandates baseline clinical and transaction record retention intervals and regulates data flows to the National Electronic Health Record (NEHR) system. PĒRL's processing is strictly confined to non-clinical administrative, operational, and user-submitted data.

11.4 Information Technology and Credential Protection

Users are strictly responsible for maintaining the confidentiality of their account credentials, usernames, passwords, and Terminal Fast-Switch access PINs. PĒRL disclaims any and all liability for losses, data exposures, or damages arising out of unauthorized account access resulting from a user's failure to safeguard their security credentials.

11.5 Cookie Protocols and Tracking Mechanisms

Our web interfaces and institutional dashboards utilize cookies and tracking pixels to analyze traffic sources, record server logs, track visitor IP addresses, and monitor clickstream behaviors.

Cookies are small text identifiers stored on your device's storage media. You may configure your browser settings to reject cookies; however, disabling these tracking mechanisms may impair platform functionality, restrict access to certain secured sections, and disable automated off-peak scheduling features.

11.6 Third-Party Digital Environments

Our digital platforms may feature hypertext links to external web environments operated by third parties. PĒRL exercises no operational control over, and assumes no legal responsibility for, the privacy practices, data protection policies, or content of any third-party websites, irrespective of any co-branding or corporate logo configurations. Users access external links at their own risk and are advised to independently review the privacy policies of those respective domains.

Section 12: Statutory Rights and Administration

12.1 Rights of Access and Correction

You are entitled to submit statutory requests to our Data Protection Officer to:

- (a) Access a record of the Personal Data currently in our possession or control, along with information regarding the manner in which such data has been used or disclosed within the preceding calendar year; and
- (b) Correct or rectify any inaccuracies or omissions in your Personal Data records.

PĒRL reserves the right to charge a reasonable administrative fee to process complex data access requests, where permitted under the PDPA.

12.2 Revocation and Third-Party Proxies

Where a user's Personal Data was provisioned to PĒRL via a third party or Caregiver, the data subject must engage that third party directly, or submit a formal identity-verified application to our Data Protection Officer, to execute a revocation of proxy permissions.

12.3 Legal Framework and Jurisdiction

This Policy shall be governed by, and interpreted in accordance with, the laws of the Republic of Singapore. Any dispute arising out of or in connection with this Policy shall be subject to the exclusive jurisdiction of the Courts of the Republic of Singapore. In the event this Policy is translated into secondary languages, the English language text shall remain the sole authoritative version and shall prevail in the event of any interpretive conflict or inconsistency.

12.4 Absolute Limitation of AI Liability and Emergency Exclusions

(a) Administrative Scope Only: PĒRL utilizes its proprietary artificial intelligence infrastructure ("Whisk") exclusively for administrative triage, capacity optimization, and scheduling coordination. The underlying models do not constitute Software as a Medical Device (SaMD) and are explicitly prohibited from rendering clinical, diagnostic, medical, or psychiatric advice or treatment.

(b) Emergency Exclusion: PĒRL is not an emergency, medical, or life-preservation service. While the platform operates a supplementary automated "Deterministic Crisis Override" pipeline configured to flag specific keywords indicating potential self-harm or acute medical trauma, this mechanism is an auxiliary safety routine and does not constitute a guaranteed emergency intervention.

(c) Exclusion of Liability: PĒRL explicitly disclaims any and all statutory or tortious liability for any failure of the Whisk AI models to accurately detect, interpret, translate, or route clinical intent, unstructured qualitative journal logs, or crisis indicators. In any scenario involving an acute medical, physical, or psychological emergency, users are instructed to bypass the platform completely and engage local emergency services (995) immediately.