Privacy Policy

Effective 13 November 2026 · Defy Technologies Pte Limited · Downloaded November 15, 2026 at 3:00 AM Fiji Standard Time

For existing customers, material changes to these terms take effect only in accordance with the notice and change provisions in section 2 of the Terms of Service. Publishing an updated page does not itself replace the required notice.

1. Scope of this Policy

This Privacy Policy explains how Defy Technologies Pte Limited ("Defy", "we", "us") collects, uses, stores, and shares personal data across the Defy platform: Defy Accounts (sign-in), the Defy Authenticator mobile app, Console (infrastructure and purchasing), Billing, My Account, Support, and this website (defy.com.fj). Because Defy Accounts provides single sign-on across these products, your account data may be shared between them as described below; each product's own use of the data it processes (such as ticket content in Support, or infrastructure configuration in Console) is scoped to delivering that specific service.

2. Information We Collect

Account and identity data

Name, email address, phone number, and a securely hashed password when you create a Defy account. Multi-factor authentication is required for Defy Accounts. For authenticator-app codes, the verifying system stores the shared secret encrypted so that it can verify your codes. For passkeys, we store the public credential information needed for verification; the private key remains with your authenticator.

Defy Authenticator app

The Defy Authenticator app generates one-time sign-in codes and lets you approve or deny sign-in requests. The secret behind each one-time code is stored only on your phone, in its secure storage, and is never sent to Defy. The camera is used only to scan the setup QR code; images are not stored or transmitted. The app contains no advertising, analytics, or tracking.

If you turn on sign-in approvals, the app registers your phone with Defy Accounts. We store the phone's public keys (the matching private keys are created and kept in your phone's secure hardware and never leave it), a push notification token, the phone's platform and model name, and when it was paired and last used. When you respond to a sign-in request, we record your response (approved or denied) with the sign-in attempt in your account's security history.

Approving a sign-in, and unlocking the app if you turn on App Lock, uses your phone's own fingerprint, face, or screen-lock check. That check happens entirely on your phone; neither the app nor Defy ever receives your biometric data.

If you turn on backup, your one-time code accounts are encrypted on your phone with a recovery key that only you hold, then stored in your own iCloud account (iPhone) or your Google account's device backup (Android). Defy does not receive the backup, and neither Defy, Apple, nor Google can read it without your recovery key. Sign-in approval keys are never included in backups.

Identity verification (KYC) documents

For services that require identity verification, we collect a photo of a government-issued document (such as a passport or driver's license). These documents are encrypted at rest, access is restricted to the verification workflow and authorized reviewers, and only the fields necessary to confirm your identity are extracted and retained as structured data.

Billing and payment data

Invoice history, billing address, and subscription details. Card and bank payment details are collected and processed by our third-party payment gateway directly — Defy does not store your full card number on its own servers.

Infrastructure and technical data

Where you provision infrastructure through Console (servers, domains, DNS records, SSH keys you choose to attach), we store the configuration data needed to provision and manage that infrastructure on your behalf. SSH credentials you provide for a one-time administrative task (for example, a manual deployment) are encrypted while the task runs and are not retained afterward.

Support interactions

Support ticket content, and if you use our chat-based support assistant, your chat messages and the assistant's responses. Conversations that need a person are handed off to a human support agent; the content of that handoff is retained as part of your support history.

Contact form submissions

If you submit the consultation form on this website, we collect your name, company, email, phone number, and message, in order to respond to your enquiry.

Usage and device data

Standard technical data such as IP address, browser type, device information, and pages visited, collected automatically as part of operating the Services and via cookies as described in Section 4.

Domain registration (WHOIS) data

If you register a domain through us, the registrant information you provide is submitted to the relevant domain registry as required for registration, in addition to being stored in your Defy account. Where the registry offers WHOIS privacy and you select it, your personal contact details are masked from public WHOIS lookups; the underlying data is still held by the registry and registrar as required for the registration to remain valid.

3. How We Use Information

- To provide, maintain, and secure the Services you've signed up for;
- To authenticate you and protect your account, including detecting suspicious activity;
- To process payments and maintain billing records;
- To provision and manage infrastructure you've purchased (servers, domains, hosting, email, licenses);
- To respond to support requests and consultation enquiries;
- To comply with legal obligations, including those imposed by domain registries and payment processors; and
- To improve the Services, including using aggregated, de-identified usage data.

We do not sell your personal data.

4. Cookies and Similar Technologies

This website uses cookies to operate securely (for example, maintaining your session) and, where you consent, to understand how visitors use the site. We use a consent management platform to present cookie choices when you first visit and to honor the preferences you set; you can change your cookie preferences at any time using the cookie settings control available on

this site.

5. How We Share Information

We share personal data only where necessary to deliver the Services:

- **Infrastructure providers** — our cloud infrastructure provider, running the servers you provision through us;
- **Email delivery** — our business email provider (sending transactional and support email);
- **Push notifications** — Google Firebase Cloud Messaging and Apple Push Notification service, which receive your phone's push notification token and a sign-in request identifier in order to deliver Defy Authenticator notifications. Request details are fetched by the app directly from Defy, not sent through these services;
- **Domain registries** — for any domain you register through us;
- **Payment processing** — our third-party payment gateway, for billing and subscriptions;
- **Identity verification** — where a service you use requires document or face verification, the minimum data needed is shared with the verification provider used for that step; and
- **Legal and safety** — where required by law, or to protect the rights, property, or safety of Defy, our customers, or the public.

Service providers process shared data for the service they supply, subject to applicable contracts and law. Registries, payment providers and other independent providers may also process data for their own legal, security or regulatory purposes under their applicable privacy notices.

6. Data Storage and Security

Data in transit to and from the Services is encrypted using TLS. Sensitive stored data — including identity verification documents — is encrypted at rest using AES-256. Access to administrative systems requires multi-factor authentication, and access to customer data is scoped to what a given role needs to perform its function. No method of transmission or storage is completely secure, and we cannot guarantee absolute security, but we maintain these controls and review them as the platform evolves.

7. Data Retention

We retain personal data for as long as your account is active. If an account is suspended for non-payment or a Terms of Service violation, associated data is retained for 6 months from suspension, after which it may be permanently deleted. Following termination of your account, you have 30 days to export your data; it may then remain in an inaccessible, non-production state for a further 90 days (to allow recovery from an accidental termination request) before permanent deletion from active systems.

Billing and tax records are retained for the period required by applicable law, regardless of account status. Domain registrant data is retained for as long as required by the relevant registry's own policies, independent of your Defy account status. These account-record periods do not extend the service-specific workload retention and deletion deadlines in our Terms of Service.

A phone registered for sign-in approvals stays registered until you remove it in My Account or pair a different phone; the record is then marked as removed and kept as part of your account's security history. Codes and backups held in the Defy Authenticator app remain under your control: removing an account in the app deletes it from your phone, and turning off backup deletes the encrypted copy from your cloud storage.

The account-record retention and export periods above concern personal information held in account records. They do not promise continued storage, export or recovery of Cloud Server disks, websites, automatic server backups or DNS records.

Those workloads follow their service-specific deletion rules, including the 3-day unpaid Cloud Server deadline and 30-day unpaid Web Hosting deadline. Separately purchased snapshots have separate retention and billing rules.

8. International Data Transfers

Because our infrastructure operates internationally (for example, the data-center regions where your Cloud Servers run and our email provider's global infrastructure), personal data may be processed outside Fiji. Where this happens, it is limited to the providers necessary to deliver the specific service you've chosen — the selected compute region concerns the primary Cloud Server workload. Account, billing, support, security and provider administration records may be processed in other locations needed for those functions.

9. Your Rights

You can:

- Access and update most of your account data directly through My Account, including reviewing and removing phones registered for sign-in approvals;
- Request a copy of the personal data we hold about you;
- Request correction of inaccurate data;
- Request deletion of your account and associated data, subject to the retention obligations described in Section 7; and
- Withdraw cookie consent at any time via the cookie settings control on this site.

To exercise any of these rights, contact info@defy.com.fj. We will respond within a reasonable time and may need to verify your identity before actioning a request.

10. Children's Privacy

The Services are intended for business and individual customers who are able to enter into a binding contract, and are not directed at children. We do not knowingly collect personal data from children.

11. Changes to this Policy

We may update this Privacy Policy from time to time. Material changes will be notified through the Services or by email, with a new effective date shown at the top of this page.

12. Contact Us

For any question about this Privacy Policy or how your data is handled, contact us at info@defy.com.fj, by phone on 999 1688, or by mail at 58 Link Road, Lautoka, Fiji (P.O. Box 2521, Lautoka).