PRIVACY POLICY

Document Type: PP | **Jurisdiction:** GLOB | **Language:** EN

Version: v2026.02.rev001 | **Last Updated:** 2026-02-02

Diggy Ltd ("**Diggy**", "**we**", "**us**", "**our**") is the operational system of record for mining, construction, and heavy-asset industries. We unify field teams, machine data, and operational workflows into one platform—bridging the gap between physical worksites and back-office systems. Built offline-first and shaped by real customer feedback, Diggy gives organisations a single source of truth for their operations (the "**Platform**" or "**Services**").

This Privacy Policy explains how we collect, use, share, and protect personal data when you use the Services.

1. WHO WE ARE AND HOW TO CONTACT US

Data Controller

Diggy Ltd Company Registration Number: 13825 3801-C2.D011, 38th Floor, Tamouh, Addax Port Office Tower Al Reem Island, Abu Dhabi, United Arab Emirates

Email: info@diggy.app Legal Notices: notices@diggy.app Legal Portal: https://diggy.app/legal

2. CONTROLLER VS. PROCESSOR (B2B CONTEXT)

Controller (typical): We are the controller for personal data related to our website, account administration, billing, marketing preferences, and our own business operations.

Processor (often): If you use Diggy through your employer or another organisation (a "**Customer**"), that Customer typically controls the operational data entered into Diggy and decides how it is used. In those cases, Diggy processes personal data on the Customer's instructions, subject to the applicable Customer Agreement and Data Processing Addendum ("DPA"), which may provide additional details about processing, security measures, subprocessors, and breach notification.

Note: If you are an end user accessing Diggy through a Customer, privacy requests about Customer-controlled operational records may need to be directed to your organisation first.

3. PERSONAL DATA WE COLLECT

We collect personal data from you, your organisation, connected systems (where enabled by the Customer), and automatically through your use of the Services. The personal data we process depends on how the Services are configured and used. Categories may include:

"Account and profile data" May include name, email address (which may be personal or business), phone number (where provided), username, user identifiers, organisation details, and role/permission assignments.

"Authentication and access data" May include login and access information (such as hashed credentials), authentication events, access logs, IP address, device and browser/app information, and security-related logs.

"Compliance and credentialing data (where provided)" May include certifications, licences, training/competency records, and related validity or expiry details, where Customer or its Authorised Users choose to store such information in the Services.

"Communications" May include messages within the Services and communications with support.

"Technical and usage data" May include diagnostics, performance data, feature usage, and audit/usage logs generated through use of the Services.

"Customer content and submissions" Customer Data (as defined in our agreements) may include content that Customer or its Authorised Users submit to the Services (e.g., notes, comments, approvals, timestamps, photos, and attachments). Such content may include personal data depending on what Customer and its Authorised Users submit. Not all users will have all data elements.

"Operational, asset, and telematics data (Customer-controlled)" The Services may also process operational records, asset information, and machine/telematics data (where integrated). This data is typically Customer-controlled and is not

inherently personal data, but it may become personal data where it is linked to, identifies, or can reasonably be associated with an identifiable individual.

"Payment, billing, and verification data (if applicable)" If paid Services or checks apply, we may process billing details (e.g., invoice contacts and payment status) and verification/KYC information as required in the relevant context.

Offline-first note: The mobile app may store data locally on your device when connectivity is limited and sync it when a connection is restored.

4. HOW WE USE PERSONAL DATA

We use personal data to:

Provide and operate the Services: User access, permissions, operations capture, syncing, reporting, and support.

Maintain safety and integrity: Secure authentication, fraud/abuse prevention, auditing, and enforcing our terms.

Improve the Platform: Analytics, performance monitoring, troubleshooting, and feature development.

Enable integrations and exports: Support integrations and data exports/APIs to customer systems (including ERPs), at the Customer's direction.

Billing and administration: Manage subscriptions or paid Services (if applicable) and maintain business records.

Compliance: Meet applicable legal obligations and respond to lawful requests.

Marketing (where permitted): Send product updates and offers, with opt-out options.

Where required by law, we rely on an appropriate legal basis (such as contract necessity, legitimate interests, consent, and/or legal obligation).

5. HOW WE SHARE PERSONAL DATA

We may share personal data:

Within a Customer organisation: With Authorised Users according to roles/permissions (e.g., supervisors or admins viewing submissions) as configured by the Customer.

With service providers: Hosting, storage, analytics, communications, support tooling, security, and verification providers that process data on our behalf.

With integration partners: Telematics/IoT providers and other systems you connect, to the extent needed to run the integration and as directed/configured by the Customer.

For legal and safety reasons: To comply with law, protect rights and safety, investigate misuse, or enforce our agreements.

In corporate transactions: If Diggy is involved in a merger, acquisition, financing, or sale of assets (with appropriate safeguards).

As aggregated/de-identified data: Where it cannot reasonably identify an individual.

6. PAYMENTS

If you purchase paid Services:

Stripe / Link: Online payments may be processed by Stripe (including Link, where available). We typically receive payment status and transaction details (and limited metadata such as last four digits where provided), but we do not intentionally store full card numbers.

Bank transfer: If you pay by transfer, we may process transfer details required for reconciliation (e.g., payer name, reference, date, amount).

Payment providers and banks process personal data under their own terms and privacy practices.

7. KYC, AML, AND ABC CHECKS

We may conduct KYC checks from time to time in line with our internal AML, ABC, and KYC policies. Depending on the context, this may include identity/business verification and screening (including via third-party providers), and disclosures to authorities where required by law.

8. COOKIES AND SIMILAR TECHNOLOGIES

We use cookies and similar technologies to support core functionality, security, preferences, analytics, and (where permitted) marketing. You can manage cookies through browser settings and, where available, Platform consent controls. Disabling some technologies may limit features.

9. INTERNATIONAL DATA TRANSFERS

We may process and store personal data in countries where we or our service providers operate. Where required by applicable law, we implement appropriate safeguards for cross-border transfers. Standard Contractual Clauses may be made available upon request where applicable.

10. DATA RETENTION

We retain personal data only as long as necessary for the purposes described above, including providing the Services, maintaining records, meeting legal obligations, resolving disputes, and enforcing agreements. Retention periods may vary depending on whether data is processed for our own purposes or on behalf of a Customer.

11. SECURITY

We use administrative, technical, and organisational measures designed to protect personal data. No system is completely secure. You are responsible for safeguarding your credentials and securing devices used to access the Platform (especially where offline data may be stored temporarily).

12. YOUR RIGHTS AND CHOICES

Depending on your jurisdiction, you may have rights to access, correct, delete, restrict or object to processing, request portability of your personal data, and withdraw consent where applicable.

Requests relating to Diggy-controlled data (Diggy as Controller): You may contact us at info@diggy.app for requests relating to our website, billing/administration, or marketing.

Requests relating to Customer-controlled data (Customer as Controller): If you use the Services through a Customer, the Customer typically controls operational records and related Customer Data. Please contact your organisation's administrator or privacy contact first. We will assist the Customer where appropriate and lawful.

For marketing: You can opt out using unsubscribe links or by contacting info@diggy.app.

We may need to verify your identity before fulfilling requests.

13. CHILDREN'S PRIVACY

The Services are not intended for individuals under 18, and we do not knowingly collect personal data from minors.

14. CHANGES TO THIS POLICY

We may update this Privacy Policy from time to time. We will post the current version (and prior versions) on our Legal Portal at https://diggy.app/legal and update the "Last Updated" date above.

If an update materially changes how we collect, use, share, or otherwise process personal data, we will provide notice prior to the update's effective date by email (to the email address associated with the relevant account, where available) and/or via an in-product notification. Unless a shorter period is required to comply with applicable law, a material update

will be effective no sooner than thirty (30) days after we provide notice.

15. JURISDICTION-SPECIFIC PROVISIONS

South Africa (POPIA)

If you are located in South Africa or if the Protection of Personal Information Act, 2013 (Act No. 4 of 2013) ("**POPIA**") otherwise applies:

- References to "personal data" include "personal information" as defined in POPIA.
- You have the rights set out in POPIA, including the right to request access to, correction of, or deletion of your personal information.
- You may lodge a complaint with the Information Regulator if you believe we have violated your rights under POPIA.
- We will only process your personal information with your consent or as otherwise permitted by POPIA.

United Arab Emirates

If you are located in the United Arab Emirates:

- We process personal data in accordance with applicable UAE data protection laws, including the UAE Federal Personal Data Protection Law (PDPL) (Federal Decree-Law No. 45 of 2021), where applicable.
- You may have rights under applicable UAE law, including rights to access, correction, deletion/erasure, restriction, and objection, depending on the context and applicable law.

16. CONTACT US

Diggy Ltd (Reg. No. 13825)

3801-C2.D011, 38th Floor, Tamouh, Addax Port Office Tower Al Reem Island, Abu Dhabi, United Arab Emirates

Legal Portal: https://diggy.app/legal

General Enquiries: info@diggy.app

Legal Notices: notices@diggy.app