

PRIVACY POLICY

This Privacy Policy applies to all services (our "*Services*") offered or provided by DashDrop Ventures and its subsidiaries (collectively, "*DashDrop*," "*we*," "*us*," or "*our*") whether accessed via our website at dashdrop.ke, our mobile application for customers (the "*Customer App*"), our mobile application for drivers and riders (the "*Driver App*"), our support channels, or any related services (collectively, the "*Platform*").

This Privacy Policy describes how we collect, use, share, store, and protect personal information of: individuals or businesses that request deliveries through DashDrop ("*Customers*"); independent service providers who accept and complete delivery requests via the Driver App ("*Drivers*" or "*Riders*"); individuals who receive deliveries arranged through DashDrop by a Customer ("*Recipients*"); and individuals who visit our website or interact with our online content without creating an account ("*Visitors*"). Customers, Drivers, Riders, Recipients, and Visitors may be referred to in this Privacy Policy as "*you*," "*your*," or "*yours*."

By using the DashDrop Platform, you confirm that you have read and understood this Privacy Policy and agree to the practices described. If you do not agree with any part of this Policy, you must not use the Platform.

This Privacy Policy is issued pursuant to the Kenya Data Protection Act, 2019 ("*DPA 2019*"), the Data Protection (General) Regulations, 2021, the Data Protection (Complaints Handling) Regulations, 2021, the Kenya Information and Communications Act (Cap. 411A), and the National Payment System Act, 2011. DashDrop Ventures is a registered Data Controller and Data Processor under the DPA 2019 and has fulfilled its registration obligations with the Office of the Data Protection Commissioner ("*ODPC*").

This Privacy Policy explains:

- [Data Protection Officer](#)
- [The Personal Information We Collect](#)
- [Sensitive Personal Data](#)
- [Legal Basis for Processing](#)
- [How We Use Your Information](#)
- [How We Share Your Information](#)
- [Recipients — Special Notice](#)
- [Google Maps and Mapping Services](#)
- [Cookies and Tracking Technologies](#)
- [How Long We Keep Your Information](#)
- [Security](#)
- [International Data Transfers](#)
- [Your Rights and Choices](#)
- [Account Deletion](#)
- [Marketing Communications](#)

- [Children](#)
- [Changes to This Policy](#)
- [Governing Law](#)
- [Contact Us](#)

Data Protection Officer

DashDrop Ventures has appointed a Data Protection Officer ("*DPO*") as required under Section 24 of the DPA 2019, given the nature and scale of our personal data processing operations. The DPO is responsible for overseeing compliance with data protection laws, advising on data protection impact assessments, and acting as the primary point of contact with the ODPC. The DPO operates independently of operational decision-making and reports directly to senior management.

DPO Contact: privacy@dashdrop.ke — Attn: Data Protection Officer

The Personal Information We Collect

"Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual.

Recipients

- **Identifiers.** For example, name, delivery address, and phone number, provided to DashDrop by the Customer placing the delivery order.
- **Delivery information.** For example, delivery address, delivery instructions, and proof of delivery records.
- **Communications data.** For example, if you contact DashDrop in connection with a delivery you received, we collect the content of your communication and your contact details.

Customers

- **Account identifiers.** For example, name, phone number, email address, password or authentication credentials, profile photograph, and account preferences.
- **Delivery information.** For example, pickup address, drop-off address, recipient name and contact number, item description, delivery instructions, delivery history, delivery status, and proof of delivery where applicable.
- **Financial information.** For example, payment method type, M-Pesa number or card reference, transaction reference numbers, and delivery payment history. Payments are processed by approved third-party payment providers including M-Pesa (Safaricom) and

Stripe or equivalent licensed gateways. DashDrop does not store full card numbers where payment processing is handled by a third-party provider.

- **Geolocation information.** For example, pickup and drop-off addresses you provide when placing a delivery order. DashDrop does not collect continuous or background location data from Customer devices.
- **Internet activity information.** For example, device type, operating system, IP address, browser type and version, application version, screens or pages viewed, session duration, in-app interactions, crash reports, and performance data.
- **Communications data.** For example, the content of messages sent through support chat, email, phone, SMS, push notifications, in-app messages, or feedback forms, together with your contact details and support history.
- **Inferences.** For example, we may draw inferences about your preferences from your delivery history and usage of our Platform to improve your experience.

Drivers and Riders

- **Account identifiers.** For example, name, phone number, email address, and profile photograph. Profile photographs are mandatory for Drivers and Riders for safety and identity verification purposes.
- **Identity and verification documents.** For example, National Identity Card or Passport number and document copy, Kenya National Transport and Safety Authority (NTSA) driving licence details, Certificate of Good Conduct issued by the Directorate of Criminal Investigations (DCI), and Kenya Revenue Authority (KRA) PIN. See [Sensitive Personal Data](#) below for how these are handled.
- **Vehicle information.** For example, vehicle type, registration number, and description.
- **Financial information.** For example, M-Pesa number or bank account details for earnings disbursement, payout history, and tax-relevant earnings records.
- **Geolocation information.** For example, real-time GPS location data from the Driver App, collected as follows: (a) when the Driver App is closed, no location data is collected; (b) when the Driver App is open and the Driver is in an "Available" status, location is collected periodically (approximately every 60 seconds) to facilitate delivery matching and dispatch; (c) when the Driver App is open and the Driver is actively on a delivery, location is collected continuously (approximately every 5 to 10 seconds) to enable live tracking, delivery verification, routing, and safety. DashDrop does not collect background location data when the Driver App is fully closed.
- **Commercial information.** For example, delivery history, completion rates, performance metrics, earnings, and payout records.
- **Internet activity information.** For example, device type, operating system, IP address, application version, in-app interactions, crash reports, and performance data.
- **Communications data.** For example, the content of messages sent through support channels, together with your contact details and support history.
- **Biometric information (if introduced in future).** DashDrop may in the future introduce biometric verification mechanisms such as facial or fingerprint authentication to enhance account security and prevent account sharing. If and when this is introduced, we will

update this Privacy Policy, notify affected users at least thirty (30) days in advance, obtain explicit and specific consent before any biometric data is collected, and comply with Section 32 of the DPA 2019. An alternative non-biometric verification method will be provided where technically feasible.

Visitors

- **Internet activity information.** For example, information about usage of our website such as pages viewed, browser type, links interacted with, IP address, browser plug-in types and versions, and operating system.
- **Communications data.** For example, if you contact us through our website or submit a form, we collect the content of your communication and your contact details.

Note on Item Descriptions

Item descriptions and delivery notes submitted by Customers may incidentally contain sensitive personal information, for example if an item is medication or a legal document. DashDrop processes this data solely to facilitate the delivery and does not use item descriptions for any marketing, profiling, or secondary purpose.

Sensitive Personal Data

The DPA 2019 identifies specific categories of personal data that require a higher standard of protection. DashDrop's operations as a courier platform require us to process some of these categories in relation to Driver and Rider onboarding and verification.

Certificates of Good Conduct are collected from Drivers and Riders to verify that they do not have disqualifying criminal history before granting access to customers' premises and goods. National Identity Cards, Passports, and NTSA driving licence documents are collected for identity verification required under our platform safety standards and applicable anti-fraud obligations. These documents are collected with the explicit written consent of each Driver or Rider during onboarding and are processed only for the specific verification purpose for which they were collected.

All sensitive personal data is subject to the following additional safeguards: collection only with explicit, written, informed consent obtained prior to and separately from our general Terms of Service; storage in encrypted form with strict access controls limited to authorised personnel with a documented operational need; Certificates of Good Conduct are reviewed solely for driver eligibility assessment and are not disclosed to Customers or other third parties; document copies are retained only for the period required by law or our driver safety obligations and are securely deleted thereafter; Drivers and Riders may withdraw consent for the processing of sensitive data, subject to the consequence that continued platform operation may not be possible.

DashDrop will never use sensitive personal data — including criminal history records — for any purpose other than the specific driver vetting purpose for which it was collected. This data is never used in marketing, shared with advertisers, or sold to any third party.

DashDrop does not intentionally collect other categories of sensitive personal information including racial or ethnic origin, religious beliefs, political opinions, or health information, unless required by a specific legal or safety obligation, in which case this Policy will be updated accordingly.

Legal Basis for Processing

The DPA 2019 requires that every processing activity be grounded in a recognised legal basis. DashDrop processes personal information on the following bases under Section 26 of the DPA 2019:

Contractual necessity (Section 26(1)(b)). We process personal information where it is necessary to perform our contract with you, including creating and managing accounts, processing delivery requests, matching Drivers with Customers, processing payments, disbursing driver earnings, and sending service-related notifications.

Legal obligation (Section 26(1)(c)). We process personal information where required to meet our obligations under Kenyan law, including retaining tax and financial records as required by the Kenya Revenue Authority, responding to lawful requests from regulators, courts, and law enforcement, and fulfilling obligations under the National Payment System Act.

Legitimate interest (Section 26(1)(f)). We process personal information where necessary for our legitimate interests or those of third parties, including fraud detection and prevention, platform security, analytics and service improvement, Driver location collection when the Driver App is open and the Driver is in an "Available" status, dispute resolution, and product development, provided these interests do not override your fundamental rights and freedoms. Where we rely on legitimate interest, we have conducted a balancing test confirming this, and records of these assessments are maintained by our Data Protection Officer and are available upon written request to privacy@dashdrop.ke.

Explicit consent (Section 26(1)(a)). We process sensitive personal data, including identity documents and background verification records, only with explicit written consent obtained separately from our general Terms of Service. We also rely on consent for marketing communications, which are only sent where you have opted in.

Vital interests (Section 26(1)(d)). In exceptional circumstances involving a safety emergency affecting a Driver, Customer, or Recipient, we may process personal information to protect the vital interests of that individual.

How We Use Your Information

DashDrop uses personal information strictly for the purposes set out below. We do not use your information for purposes incompatible with those for which it was collected without your consent or a separate legal basis.

All Users

- To create, verify, and manage your DashDrop account
- To connect Customers with available Drivers and Riders
- To process, track, and confirm delivery requests
- To provide live delivery tracking to Customers and Recipients
- To calculate delivery pricing and estimates
- To process Customer payments and disburse Driver earnings
- To generate receipts, invoices, and transaction records
- To communicate delivery updates, account alerts, and service announcements
- To detect, prevent, and investigate fraud, abuse, and unsafe activity
- To respond to customer support inquiries and resolve disputes
- To improve our Platform, routing algorithms, and features
- To comply with legal, tax, accounting, and regulatory obligations
- To enforce our Terms of Service and Community Guidelines
- To respond to lawful requests from courts, regulators, and law enforcement
- Where you have given consent, to send marketing communications about our Platform and Services

Drivers and Riders

- To verify your identity and assess your eligibility to operate on the Platform
- To facilitate the delivery services you provide
- To determine whether you are accepted to perform deliveries for a particular Customer
- To administer your earnings and disburse payouts
- To track delivery progress and confirm completion

DashDrop does not use your personal information to build behavioural advertising profiles, sell data to third-party advertisers, engage in automated decision-making that produces significant legal effects without human review, or train third-party artificial intelligence or machine learning models. Any future use of AI-assisted features will be disclosed and governed by a specific notice.

How We Share Your Information

DashDrop does not sell your personal information. Sharing of personal information occurs only in the circumstances described below and always on a need-to-know basis proportionate to the purpose.

Information Shared Between Platform Users

To complete deliveries, certain information must flow between Customers, Drivers, and Recipients. If you are a Customer, we provide your first name, pickup address, drop-off address, delivery notes, and contact number as needed to the Driver assigned to your delivery, so that the Driver may contact you and facilitate pickup and delivery. If you are a Driver or Rider, we provide your first name, profile photograph, vehicle type and description, real-time location during the delivery, and delivery status to the Customer and Recipient so that they can track their delivery and confirm the correct Driver. If you are a Recipient, we provide your name, delivery address, phone number, and delivery instructions to the assigned Driver to facilitate delivery. Driver real-time location sharing ceases immediately upon delivery completion or cancellation. DashDrop does not provide Customers with historical location data of Drivers beyond the specific delivery they have placed.

Third Parties Providing Services on Our Behalf

DashDrop works with trusted third-party service providers to operate our Platform. We may provide these providers with access to the categories of personal information described in this Policy, but only to the extent necessary for them to perform their specific service. These providers are contractually bound by data protection obligations equivalent to or exceeding those under the DPA 2019 and are prohibited from using data for their own purposes. Our service providers include payment processors such as M-Pesa (Safaricom) and Stripe or equivalent licensed providers; cloud hosting providers such as AWS, Google Cloud, or Azure; SMS and notification services such as Africa's Talking or Twilio or equivalent; mapping and routing providers including Google Maps Platform; analytics providers; customer support tools; fraud prevention specialists; and identity verification providers. A current list of our key data processors is available upon written request to privacy@dashdrop.ke.

Legal and Regulatory Disclosures

DashDrop may disclose personal information to government authorities, regulators, courts, or law enforcement bodies where we are required to do so by a valid and binding legal obligation, court order, or lawful authority direction; where disclosure is necessary to establish, exercise, or defend legal claims involving DashDrop; where disclosure is necessary to protect the vital interests of a data subject or third party; or where we are responding to a request from the ODPC or another competent supervisory authority. Where legally permitted, DashDrop will notify affected individuals of such disclosures.

Corporate Transactions

If DashDrop is involved in a merger, acquisition, joint venture, investment, restructuring, or sale of business assets, personal information may be transferred as part of that transaction. The receiving party will be required to honour this Privacy Policy or provide equivalent protections, affected users will be notified before personal data is transferred to a materially different privacy policy, and you will be given the opportunity to request deletion of your data before any transfer takes place if you do not consent to the new arrangements.

DashDrop will never sell personal information to third parties for any purpose, share personal information with advertisers for targeted advertising, provide bulk data exports of user information to any commercial third party, or share sensitive personal data — including identity documents and Certificates of Good Conduct — beyond the authorised verification provider and DashDrop's authorised internal personnel.

Recipients — Special Notice

Recipients are individuals who receive deliveries through DashDrop but have not themselves created a DashDrop account. When a Customer places a delivery order, they provide DashDrop with the Recipient's name, delivery address, and phone number. Recipient data is processed by DashDrop under the legal basis of legitimate interest, specifically the legitimate interest of the sending Customer to have their delivery completed and DashDrop's legitimate interest in providing that service.

Recipient data is used solely to enable the Driver to navigate to and deliver to the correct address; to allow the Driver to contact the Recipient if access or confirmation is required; to generate proof of delivery records; and to allow the Customer to track the delivery to the Recipient. Recipient data is not used for marketing or promotional communications to Recipients, for creating Recipient profiles or accounts without the Recipient's consent, or for any purpose beyond completing the specific delivery for which it was shared.

Recipients who have concerns about how their personal data was shared with DashDrop — including those who did not consent to receive a delivery or whose data was shared without their knowledge — may contact us at privacy@dashdrop.ke. We will investigate and respond within twenty-one (21) days.

Google Maps and Mapping Services

DashDrop uses Google Maps Platform and may use equivalent mapping services to power address search and autocomplete, pickup and drop-off location selection, route calculation and navigation for Drivers, Driver matching based on proximity, live tracking display for Customers, and estimated delivery time calculation. When these services are used, location-related data — including addresses, route waypoints, and real-time location coordinates — may be transmitted to and processed by Google LLC or the relevant mapping provider in accordance with their own privacy terms. DashDrop's agreement with Google requires that Google not use DashDrop customer data for Google's own advertising or product improvement purposes without appropriate authorisation. Customers and Drivers should be aware that Google's use of data from Google Maps Platform is governed by Google's Privacy Policy at <https://policies.google.com/privacy>.

Cookies and Tracking Technologies

DashDrop uses cookies and similar tracking technologies on our website and, where applicable, in our mobile applications. Cookies are small text files placed on your device when you visit our website. Similar technologies include pixels, web beacons, SDKs, and local storage objects. These technologies allow us to recognise your device and collect information about how you use our Platform.

Strictly Necessary Cookies enable core website functionality including login sessions, security, and form submissions. The website cannot function without these and they cannot be disabled.

Functional Cookies enable our website to remember your preferences, language, and settings across sessions. You may disable these through your browser settings, though some features may not function properly as a result.

Analytics Cookies measure traffic, identify popular features, track user journeys, and improve Platform design. Data collected is aggregated and anonymised where possible. You may disable these through your browser settings or our cookie preference centre.

Security Cookies detect and prevent fraud, bot activity, and malicious behaviour. These cannot be disabled as they are required for platform security.

Marketing Cookies measure the effectiveness of DashDrop marketing campaigns where used. No third-party advertising network cookies are used without your separate consent. You may opt out through our cookie preference centre.

You may control and manage cookies through your browser settings, device settings for mobile applications, or DashDrop's cookie preference centre where available on our website. Disabling strictly necessary or security cookies may prevent you from using parts of the Platform. Disabling analytical cookies does not affect your ability to place or track deliveries.

How Long We Keep Your Information

DashDrop retains personal information only for as long as necessary for the purposes described in this Policy, including to comply with legal obligations. When the applicable retention period expires, DashDrop will securely delete, anonymise, or destroy the relevant personal information. Anonymised data from which no individual can be identified may be retained indefinitely for statistical and operational analysis.

Customer account data is retained for the duration of the account and for three (3) years after account closure to allow for dispute resolution and legal claims. Driver and Rider account data is retained for the duration of the contract and for five (5) years after termination to allow for legal claims, regulatory audit, and safety record requirements. Individual delivery records are retained for five (5) years from the delivery date for dispute resolution and fraud investigation purposes. Transaction and payment records, including Driver earnings and payout records, are retained for seven (7) years from the date of the transaction in compliance with Kenya Revenue Authority requirements and the National Payment System Act. Driver identity documents including

National Identity Cards and Passports are retained for the duration of the driver contract and for three (3) years thereafter. Certificates of Good Conduct are retained for the duration of the driver contract and for one (1) year thereafter and are deleted promptly once their utility expires. Location data from completed deliveries is retained for ninety (90) days and then aggregated or anonymised. Real-time live location data is not stored persistently and is discarded upon delivery completion. Customer support records are retained for three (3) years from the date of the last interaction. Raw website analytics logs are retained for ninety (90) days. Aggregated analytics data is retained for two (2) years. Marketing consent records are retained for the duration of the consent period and for three (3) years after withdrawal as compliance evidence. Fraud and security incident records are retained for five (5) years from the date of the incident. Minimal account identifiers for deleted accounts are retained for three (3) years after deletion to prevent re-registration fraud.

Security

DashDrop implements technical, administrative, and physical safeguards to protect personal information. Technical safeguards include encryption of data in transit using TLS 1.2 or higher, encryption of sensitive data at rest including identity documents and payment credentials, multi-factor authentication for internal systems and administrative access, automated vulnerability scanning and regular penetration testing, Web Application Firewall and DDoS protection, and API authentication and rate limiting. Administrative safeguards include role-based access controls limiting personnel to the data required for their specific role, background checks for personnel with access to sensitive personal data, mandatory data protection training for all personnel, data protection impact assessments for high-risk processing activities, contractual data protection obligations with all third-party processors, and regular internal privacy and security audits.

DashDrop maintains a formal Data Breach Response Plan. In the event of a personal data breach, DashDrop will contain and assess the breach immediately upon detection, notify the ODPC within seventy-two (72) hours of becoming aware of a breach that poses a risk to data subjects as required under Section 43 of the DPA 2019, and notify affected data subjects directly without undue delay where the breach is likely to result in a high risk to their rights and freedoms. Breach notifications will include the nature of the breach, the categories and approximate number of affected individuals, likely consequences, and measures taken or proposed.

No internet-based service can guarantee absolute security. You are responsible for maintaining the confidentiality of your DashDrop account credentials. DashDrop will never ask you for your password via email, phone, or chat. If you suspect unauthorised access to your account, contact us immediately at info@dashdrop.ke or through in-app support.

International Data Transfers

DashDrop is headquartered in Kenya and our primary operations serve the Kenyan market. However, some of our technology infrastructure and service providers are located outside Kenya, which means your personal data may be processed in other jurisdictions including the United States, the European Union, and South Africa.

Transfers of personal data outside Kenya occur only in compliance with Section 49 of the DPA 2019 and the Data Protection (General) Regulations, 2021, specifically where we have executed data transfer agreements with our processors imposing data protection obligations equivalent to Kenyan law; where you have explicitly consented to the specific transfer after being informed of the risks; where the transfer is necessary to perform a contract entered into at your request; or where the transfer is necessary for the establishment, exercise, or defence of legal claims. Where data is transferred to the United States or European Union, we rely on Standard Contractual Clauses. You may request a copy of the applicable transfer mechanism by contacting privacy@dashdrop.ke.

Your Rights and Choices

Under the DPA 2019, you have comprehensive rights over your personal data. DashDrop is committed to facilitating the exercise of these rights promptly, transparently, and without unnecessary barriers. We will respond to all valid requests within twenty-one (21) days of receipt. In complex cases, this period may be extended by a further twenty-one (21) days, in which case we will notify you of the extension and the reason for it. We will never charge a fee for exercising your rights unless a request is manifestly unfounded or excessive.

Right of Access (Section 26, DPA 2019). You may request a copy of all personal data DashDrop holds about you and information about how it is processed. To submit an access request, email privacy@dashdrop.ke with the subject line "Data Access Request."

Right to Rectification (Section 26, DPA 2019). You may request correction of inaccurate or incomplete personal data. Many account details can be updated directly through the DashDrop app. For other corrections, email privacy@dashdrop.ke.

Right to Erasure (Section 27, DPA 2019). You may request deletion of personal data where we have no legal obligation to retain it. To submit a deletion request, email privacy@dashdrop.ke with the subject line "Deletion Request." Note that deletion requests cannot override legally mandated retention periods such as the seven-year financial records requirement under KRA regulations.

Right to Restrict Processing (Section 26, DPA 2019). You may request that we limit how we use your data in specified circumstances, for example while the accuracy of your data is disputed. Email privacy@dashdrop.ke with your specific request.

Right to Object (Section 30, DPA 2019). You may object to processing of your personal data based on legitimate interest, including profiling. Email privacy@dashdrop.ke with your specific objection.

Right to Data Portability (Section 28, DPA 2019). You may request your personal data in a structured, machine-readable format for transfer to another provider. Email privacy@dashdrop.ke with the subject line "Portability Request."

Right to Withdraw Consent (Section 35, DPA 2019). Where processing is based on your consent, you may withdraw that consent at any time without affecting the lawfulness of processing prior to withdrawal. You may withdraw consent for marketing emails via the unsubscribe link in any marketing email, withdraw consent for marketing SMS by replying STOP to any DashDrop marketing SMS, or manage push notification preferences through your device settings or the DashDrop app notification centre. For other consent-based processing, contact privacy@dashdrop.ke.

Right to Lodge a Complaint (Section 58, DPA 2019). If you are not satisfied with DashDrop's response to a rights request or privacy concern, you have the right to lodge a complaint directly with the Office of the Data Protection Commissioner (ODPC), which is Kenya's independent supervisory authority for data protection. You may contact the ODPC at www.odpc.go.ke or write to P.O. Box 41079-00100, Nairobi, Kenya.

To exercise any of the above rights, contact privacy@dashdrop.ke. We may need to verify your identity before processing a request to ensure we do not disclose or delete data at the direction of an unauthorised party.

Account Deletion

You may request deletion of your DashDrop account at any time by using the "Delete Account" option in the DashDrop app settings where available, by emailing privacy@dashdrop.ke with the subject "Account Deletion Request" from the email address associated with your account, or by contacting DashDrop support through the in-app chat.

Upon receiving a verified account deletion request, DashDrop will deactivate your account and remove your ability to log in within five (5) business days, delete or anonymise personal data not subject to a legal retention obligation within thirty (30) days, and confirm completion of the deletion process by email.

Some personal information will be retained after account deletion where required by law, including transaction and payment records retained for seven (7) years under KRA and National Payment System Act requirements, delivery records relevant to ongoing disputes or legal claims, Driver verification records during any applicable retention period, and fraud prevention records where there is evidence of fraudulent activity. Retained data after account deletion will be accessed only for the specific purpose for which it is retained and will be securely deleted when the applicable retention period expires.

Marketing Communications

DashDrop will only send you marketing communications — including promotional offers, service announcements, and platform news — where you have provided explicit consent to receive such communications. You may withdraw consent for marketing emails at any time via the unsubscribe link in any marketing email. You may withdraw consent for marketing SMS messages by replying STOP to any DashDrop marketing SMS. You may manage push notification preferences through your device settings or the DashDrop app notification centre.

Withdrawal of marketing consent does not affect your receipt of service-related communications necessary to operate your account and deliveries, such as delivery status updates, security alerts, and payment confirmations. DashDrop will never send you marketing communications without prior opt-in consent and will never sell or share your contact details with third-party marketers for their own promotional use.

Children

DashDrop is not intended for use by individuals under the age of eighteen (18) years. You must be at least 18 years old to create a DashDrop account, place a delivery order, or register as a Driver or Rider. Drivers and Riders must also meet all applicable legal requirements under Kenyan law including minimum age requirements for operating motor vehicles or motorcycles under the Traffic Act (Cap. 403) and NTSA regulations.

DashDrop does not knowingly collect personal information from individuals under 18. If we become aware that we have collected personal data from a person under 18 without verified parental consent, we will take immediate steps to delete that information and close the relevant account. If you believe that a child under 18 has provided personal information to DashDrop, please contact us immediately at privacy@dashdrop.ke.

Changes to This Policy

DashDrop may update this Privacy Policy from time to time to reflect changes in our services, technology, legal obligations, or regulatory guidance. The most current version of this Policy will always be available on our website and within the DashDrop app.

Where we make material changes — meaning changes that significantly affect your rights or how we process your personal information — we will notify you via email to the address associated with your account, display a prominent notice within the DashDrop app and website for at least thirty (30) days before the changes take effect, and obtain fresh consent where the change affects consent-based processing. For non-material changes such as clarifications or typographical corrections, the updated version will be effective when posted. The "Effective" date at the top of this Policy indicates when it was most recently revised. If you do not agree to a material change, you may close your account and request deletion of your data before the updated Policy takes effect.

Governing Law

This Privacy Policy is governed by and construed in accordance with the laws of Kenya, including the Data Protection Act, 2019, and all associated subsidiary legislation. Any dispute arising from or in connection with this Privacy Policy that is not resolved through direct contact with DashDrop shall be subject to the non-exclusive jurisdiction of the courts of Kenya. Nothing in this clause limits your right to lodge a complaint with the Office of the Data Protection Commissioner or any other competent supervisory authority.

Contact Us

For questions, privacy requests, or concerns about this Privacy Policy or the handling of your personal information, please contact:

DashDrop Ventures
3 Ojijo Plaza, Ojijo Road
Nairobi, P.O. Box 100187, 00101 Jamia
Kenya

General inquiries: info@dashdrop.ke
Privacy and data requests: privacy@dashdrop.ke
Data Protection Officer: privacy@dashdrop.ke — Attn: Data Protection Officer

We aim to acknowledge all privacy-related inquiries within five (5) business days and to resolve them fully within twenty-one (21) days.

For complaints to the supervisory authority: Office of the Data Protection Commissioner, P.O. Box 41079-00100, Nairobi, Kenya — www.odpc.go.ke

Google Play Account Deletion Addendum

Delete in app: Profile>Account Settings>Delete Account or email privacy@dashdrop.ke.

Deletes profile, addresses, payment methods, orders, tokens, chats, marketing prefs, ratings.

Retains transactions/payments 7y; support 3y; fraud/safety as legally required.

Immediate deactivation; live deletion within 30 days; backups within 90 days; permanent deletion.