Privacy Policy

Version 0.2 | 12 October 2026 | Owner-approved draft

Professional review and launch requirements remain open. This document is not legally approved or effective for paid rentals. Real payments, refunds and payouts are unavailable.

1. Controller and scope

Powrgen Limited is the intended controller for CarPont's platform processing. Its recorded address is Southerton, Harare, Zimbabwe. Contact support@usecarpont.com for privacy requests once the monitored privacy intake is confirmed. DPO details and verified controller-licence particulars will be published where required; none is claimed by this draft.

This notice covers account holders, guests, named drivers, hosts, authorised owners, support contacts and platform visitors. Hosts may have separate responsibilities for data they lawfully receive; the allocation must be confirmed for launch.

2. Information collected and purposes

We process account/profile/contact information to authenticate users and administer roles; ID/passport, licence, address and selfie/evidence to assess identity and eligibility; vehicle ownership, authorisation, registration, insurance, licensing and condition evidence to review listings; booking dates, parties, approximate/exact coordination locations, pricing and policy versions to administer rentals; and messages, reviews, case evidence, decisions and audit events to support communication, safety and disputes.

Technical records may include timestamps, error/security logs, delivery events and suppression information. Device location is requested only for the feature you choose; search should remain possible by manually entering a place. Do not describe the service as continuously tracking journeys when it does not.

Future payment records may contain provider references and status, but live payment processing is not currently offered. CarPont must not collect card credentials in its own forms. We do not collect criminal-history information or use facial-recognition technology merely because a selfie is uploaded. Any biometric matching or materially new processing requires separate assessment and notice.

3. Legal grounds and your choices

Each processing activity needs an applicable lawful ground under Zimbabwean law, documented in the internal processing register. Depending on the activity this may involve informed consent, contractual necessity, legal obligation or another legally permitted basis. This policy does not claim that a single terms checkbox supplies every basis.

Where consent is required, it must be specific and informed and may be withdrawn, subject to lawful consequences already explained. Required verification cannot be skipped for a rental; refusing genuinely necessary information may prevent participation. Optional marketing, location access and later guest invitations must be separate choices. We do not automatically create guest accounts.

4. Who can see information

Public listings show the intended safe vehicle/host projection and approximate area, not private ID documents, full residential addresses or internal review notes. Booking participants receive only the information necessary for their booking. Appropriate direct coordination details may be released after confirmation; private verification evidence must not be included.

Authorised staff access evidence according to their role and legitimate need. Other recipients may include contracted hosting, authentication, storage, email and payment providers; insurers or advisers

where necessary and lawful; and authorities where legally required or appropriately justified. Provider access and support arrangements must be covered by suitable contracts. CarPont does not authorise sale of private verification evidence or unrestricted marketing sharing.

5. Services outside Zimbabwe

CarPont uses Firebase/Google services and Resend email delivery. Some processing, support, metadata or storage may occur outside Zimbabwe. Actual product regions, recipient countries, subprocessors and transfer safeguards must be verified before the final notice is published. A Firestore region alone does not describe all authentication/email/support processing.

International transfer must satisfy applicable Zimbabwean protections and required POTRAZ procedures. We will disclose validated destinations and safeguards in the final transfer register; this draft is not an assertion that overseas processing has been approved.

6. Messages, email and cookies

Pre-booking messages are screened for obvious contact details and off-platform arrangements. Cases and relevant communications may be reviewed by authorised staff. Transactional account, verification, booking and safety messages differ from promotional marketing. Email delivery/suppression events help prevent repeated unwanted or undeliverable sends; they do not prove a person read a message.

Essential session/security storage supports sign-in and preferences. A cookie/storage inventory is required before publication. Optional analytics or advertising tools require their own lawful configuration and notice; this draft does not claim they are installed. We do not bundle marketing consent into booking acceptance.

7. Retention and security

Keep records only for a documented purpose and applicable period. Account data is needed while the account operates; booking, financial, legal and case evidence may need longer retention for legal obligations or unresolved claims. Raw identity evidence should have a shorter justified review/re-verification period than general transaction records wherever lawful and practicable.

The internal schedule proposes periods subject to approval and technical implementation. No automatic deletion facility or universal retention period is claimed as live. Backups may take longer to expire; lawful holds can suspend deletion for relevant records. We apply appropriate access restrictions, private evidence storage and audit controls, while recognising no service can guarantee perfect security.

8. Rights and complaints

You may ask about your information and seek access, correction, deletion, objection or other applicable rights under Zimbabwean law. We verify identity proportionately before disclosure; do not send identity documents to an unverified requester. Certain information may lawfully be retained or withheld, with reasons where permitted, including other people's data and protected investigations.

Contact the privacy intake. We will record, assess and answer requests under applicable legal time limits; the final operating procedure must confirm those deadlines. You may also complain to POTRAZ or another competent authority. Withdrawal or account closure does not erase lawfully required transaction evidence.

9. Children and changes

Drivers must be 21 or older under platform rules. We do not invite children to provide verification information. A child-seat booking does not require a child's name or ID. If children's information is received, escalate for lawful handling rather than routinely retaining it.

Material changes will be notified and the notice version recorded. New uses requiring consent will not be justified by a silent policy update.