VYO PRIVACY POLICY

Effective Date: Upon electronic acceptance by the user through the Vyo mobile app; Last Updated: May 1, 2026

Company: Vyo Corp

IMPORTANT PRIVACY, BIOMETRIC, CAMERA, AND TELEMETRY NOTICE

This Privacy Policy explains how Vyo collects, uses, shares, stores, and protects information in connection with the Vyo app, Vyo Go, websites, vehicles, cameras, biometric verification, telemetry, payments, property deployments, rentals, and support.

This Policy includes Vyo's biometric data notice, written release support language, and biometric retention/destruction policy. Audio recording is currently disabled for Florida rentals unless Vyo later enables legally sufficient notice and consent controls.

If you do not consent to required identity, payment, biometric, camera, GPS, telemetry, account, safety, and rental data processing, do not create or use a Vyo account and do not use Vyo services.

1. Scope; Relationship to Other Vyo Documents

This Privacy Policy (this "Policy") applies to Vyo Corp ("Vyo," "we," "us," or "our") and describes how Vyo collects, uses, stores, discloses, and otherwise processes information when you access or use the Vyo mobile application, Vyo Go in-vehicle application, Vyo websites, Vyo vehicles, support channels, property deployments, cameras, biometric/facial-verification systems, telemetry systems, payment systems, identity systems, routing tools, and related services (collectively, the "Services").

This Policy is incorporated into the Vyo Terms of Service, Vyo Rental Agreement, Vyo Liability Waiver, trip-specific rental records, payment authorization, camera/video/audio/biometric notices, and all rental-start safety acknowledgments. It does not reduce any release, assumption of risk, indemnity, payment obligation, insurance reimbursement obligation, passenger-notice obligation, arbitration agreement, class-action waiver, jury-trial waiver, or limitation of liability in those documents.

Where this Policy contains required privacy notices, biometric notices, biometric retention/destruction rules, consents, authorizations, or written releases, those provisions are intended to be binding as part of your Vyo documents to the maximum extent permitted by law. This Policy does not waive rights that applicable law says cannot be waived and does not create rights beyond applicable law or Vyo's express written commitments.

2. Summary of Vyo Data Practices

Vyo is an app-controlled, property-restricted, self-drive low-speed vehicle rental platform. Vyo collects and uses data to verify users, prevent anonymous access, provide rentals, process payments, operate vehicles, support insurance and claims, preserve evidence, enforce safety rules, comply with law, and protect people, property, vehicles, and Vyo systems.

Vyo uses a minimized-data architecture where high-risk identity and payment functions are handled through providers such as Plaid and Stripe, while Vyo maintains operational records needed for account control, rentals, safety, claims, and evidence. Vyo may receive verification results, tokens, risk scores, timestamps, logs, screenshots, images, clips, metadata, or other records depending on provider configuration and business need.

Vyo Vehicles may use edge-based, local, onboard, removable-media, camera-manufacturer, BlackVue or other dashcam systems, Vyo-controlled systems, and third-party cloud systems. Vyo does not represent that all footage is continuously livestreamed, centrally monitored, or centrally stored. Vyo may selectively retrieve, preserve, upload, review, disclose, or use data when Vyo determines it is useful or necessary for the purposes described in this Policy.

3. Information You Provide to Vyo

We may collect information you provide directly, including name, email address, phone number, home address, date of birth, driver-license information, account credentials, profile details, property/resident/guest information, payment method information, support messages, incident reports, photos, videos, damage reports, charge disputes, feedback, surveys, and other information you submit through the app, website, Vyo Go, support, email, phone, SMS, or other channels.

If you submit photos, videos, reports, statements, or support messages, they may contain faces, vehicles, license plates, property areas, passengers, bystanders, injuries, road conditions, damage, police reports, insurance information, health-related information, or other sensitive information. You must not submit information you are not authorized to provide.

You are responsible for ensuring that information you provide is accurate, current, complete, and lawful. If you provide passenger, guest, property, incident, witness, insurance, or third-party information, you represent that you have authority to provide it or that disclosure is necessary for safety, support, legal, insurance, claims, or incident purposes.

4. Account, Eligibility, Identity, and Driver Verification Information

Vyo may collect and process information needed to verify that you are eligible to create an account, access a property deployment, and operate a Vehicle, including your legal name, date of birth, address, phone number, email address, driver-license data, license status, identity verification status, liveness check status, facial match results, fraud-risk signals, Plaid Protect or similar risk scores, DMV/AAMVA-related validation results, property eligibility, and account history.

Vyo may use Plaid, AWS Rekognition, payment processors, property partners, fraud-prevention providers, identity-verification providers, biometric providers, and other service providers to collect or process this information. Vyo is designed to minimize raw identity-document retention by relying on regulated providers, but Vyo or its providers may process, access, or retain identity-related records, images, tokens, results, logs, or metadata where necessary for verification, safety, account administration, fraud prevention, claims, insurance, legal compliance, law enforcement, chargebacks, disputes, or evidence preservation.

Vyo may deny, suspend, terminate, re-check, or condition access based on identity, license, payment, property, fraud, safety, insurance, or compliance information. If applicable law gives you a right to request human review or appeal of certain automated decisions, you may contact Vyo as described in this Policy.

5. Payment and Billing Information

Vyo uses Stripe or replacement payment processors to process payments, store tokenized payment methods, verify payment validity, place holds, charge rental amounts, charge Additional Charges, handle disputes, process refunds, collect debts, and prevent fraud. Vyo generally does not need to store your full card number to charge a tokenized payment method.

Payment-related information may include payment tokens, billing name, billing address, payment method type, last four digits, expiration information, authorization results, transaction history, chargebacks, failed payments, refunds, invoices, receipts, bank/card network data, risk data, and communications with payment processors, banks, card networks, collection agencies, insurers, and dispute-resolution providers.

Payment information may be used and disclosed for billing, fraud prevention, chargebacks, collections, taxes, accounting, insurance reimbursement, claims, legal compliance, and enforcement of the Terms, Rental Agreement, Waiver, and Fee Schedule.

6. Vehicle, Rental, GPS, Telemetry, and Operational Information

When you access or use Vyo, we may collect vehicle and rental information, including account ID, rental ID, vehicle ID, VIN, QR scan, BLE/proximity event, start/end timestamps, app version, Vyo Go activity, GPS location, route, speed, acceleration, braking, steering-related signals where available, battery state, charger state, plug-in status, geofence events, red-road events, route alerts, navigation selections, destination filters, warnings, vehicle health, maintenance events, collision or motion events, tamper alerts, support events, and return-to-origin status.

Vyo may collect, store, analyze, disclose, and use this information for vehicle access, identity binding, driver authentication, billing, charging, routing, range estimates, geofencing, safety alerts, claims, insurance, legal compliance, maintenance, recovery, towing, fraud prevention, property deployment, underwriting, product improvement, and dispute resolution.

GPS, telemetry, routing, battery, and geofence data may be inaccurate, incomplete, delayed, or unavailable. Vyo does not guarantee that these systems will prevent prohibited use, accidents, citations, route violations, unauthorized driver events, or losses.

7. Cameras, Video, Motion Detection, Audio-Capable Systems, and Edge Storage

Vyo Vehicles may use interior cameras, forward-facing cameras, exterior/environment-facing cameras, dash cameras, motion-detection recording, incident-triggered recording, parking/security-mode recording, camera metadata, GPS-linked video records, and local/edge storage systems. Recording may occur before, during, or after a rental when the Vehicle is powered, accessed, moved, approached, tampered with, involved in an incident, parked in security/motion-detection mode, or otherwise configured to record under Vyo parameters.

Vehicle video, images, metadata, and related evidence may be stored on local data cards, onboard storage, removable media, vehicle hardware, Vyo systems, Vyo-controlled storage, BlackVue systems, other camera

manufacturer systems, cloud storage, identity-verification systems, insurers, claims platforms, support systems, law-enforcement systems, or other third-party systems Vyo uses now or later. Vyo may change camera, biometric, cloud, storage, hardware, dash-camera, payment, identity-verification, routing, telemetry, or evidence providers at any time for the same or similar purposes.

Audio recording is currently disabled for Florida rentals. Vyo may use audio-capable hardware, and audio may be enabled in a jurisdiction or deployment only where Vyo determines audio recording is lawful and Vyo has implemented legally sufficient notice and consent controls. If audio is enabled and lawful, audio may be collected and used for safety, security, evidence, support, claims, insurance, legal compliance, and dispute-resolution purposes. If you or any passenger objects to required camera, video, audio-capable, biometric, GPS, telemetry, or evidence systems, do not use Vyo and do not allow that passenger to ride.

Vyo does not promise that any camera, data card, cloud system, upload, retrieval, recording, or preservation system will capture, preserve, upload, or retrieve every event, angle, clip, or data point. Systems may be unavailable, delayed, inaccurate, obstructed, corrupted, overwritten, offline, disabled, affected by lighting/weather/connectivity/power/storage limits, or controlled in part by third-party providers.

8. Facial Recognition, Biometric Verification, and Written Biometric Notice

Vyo and its providers may collect, capture, scan, receive, process, compare, convert, transmit, store where applicable, use, disclose, and rely on facial images, liveness checks, face geometry, biometric identifiers, biometric information, biometric comparison results, identity-verification results, driver-license verification results, authentication logs, and related records for identity verification, driver eligibility, account security, vehicle access, ignition/restart authorization, continuous or randomized driver authentication, anti-fraud screening, unauthorized-driver detection, safety enforcement, incident response, claims, insurance, dispute resolution, legal compliance, and records retention.

This Policy, together with your electronic acceptance of the Vyo Terms, Rental Agreement, and Waiver, is intended to provide written notice, state the specific purpose and length of term, and operate as your written release, electronic consent, and signed authorization to the fullest extent required or permitted by biometric privacy, consumer protection, electronic signature, vehicle rental, and related laws.

Biometric and facial-recognition systems may be operated by Vyo, AWS Rekognition, Plaid, BlackVue or other camera/cloud providers, or any replacement or additional provider Vyo selects. Vyo may receive verification results, authentication logs, risk scores, timestamps, screenshots, images, clips, metadata, or other records depending on the provider and system configuration.

If a state or jurisdiction requires an additional notice, disclosure, separate consent, checkbox, written release, or retention notice before biometric processing, Vyo may require that acceptance before account creation, update, rental start, or continued use. If the required consent process is unavailable or you decline it, you may not create or use a Vyo account or operate a Vehicle.

9. Biometric Retention and Destruction Policy

This Section is Vyo's biometric retention and destruction policy. It applies to biometric identifiers and biometric information to the extent Vyo or its providers possess or control them and to the extent applicable law treats Vyo's facial-verification records, face geometry, liveness checks, or biometric comparison data as biometric identifiers or biometric information.

Vyo retains or causes retention of biometric-related records only for the period reasonably necessary for identity verification, driver authentication, fraud prevention, account administration, rental operations, safety, security, insurance, claims, chargebacks, collections, investigations, legal holds, dispute resolution, arbitration, litigation defense, regulatory compliance, tax/accounting, and other legitimate business purposes, unless a shorter period is required by non-waivable law.

For biometric identifiers or biometric information subject to Illinois BIPA or a similar law requiring a public retention schedule, and absent a valid warrant, subpoena, court order, legal hold, or other non-waivable lawful basis requiring different retention, Vyo will permanently destroy or cause destruction of such biometric identifiers or biometric information when the initial purpose for collecting or obtaining them has been satisfied or within 3 years after your last interaction with Vyo, whichever occurs first.

For purposes of this biometric retention schedule, 'last interaction with Vyo' means the date of your last account access, rental, payment transaction, support contact, privacy request, dispute submission, or other active use of Vyo services. It does not include Vyo's internal use, review, storage, preservation, legal hold, claims handling, insurance processing, fraud prevention, litigation, compliance, evidence preservation, or other back-office processing of retained records after your account or rental activity has otherwise become inactive.

Biometric identifiers and biometric information will not be sold, leased, traded, or otherwise profited from in a manner prohibited by law. Vyo may disclose biometric-related information only as described in this Policy, including to service providers, for authorized transactions, with your consent, to comply with law, to respond to valid legal process, to protect safety/security, to prevent fraud, to support insurance/claims/legal defense, or where otherwise permitted by applicable biometric law.

Vyo uses reasonable administrative, technical, and physical safeguards appropriate to the nature of biometric information and seeks to protect biometric identifiers and biometric information at least as carefully as other confidential and sensitive information in Vyo's possession. Providers may maintain their own retention, deletion, and security controls, and Vyo may rely on provider deletion, de-identification, unenrollment, or tokenization processes where applicable.

10. App, Device, Website, Cookies, and Analytics Information

Vyo may collect device and usage information, including IP address, device ID, device type, operating system, app version, user agent, browser type, crash logs, diagnostics, push token, session IDs, timestamps, screen interactions, clickstream, rental-start flow completion, document acceptance records, security logs, and performance data.

Vyo websites and apps may use cookies, pixels, SDKs, local storage, analytics tools, crash-reporting tools, fraud-prevention tools, and similar technologies. These tools may help operate the Services, remember preferences, secure accounts, understand usage, improve performance, prevent fraud, measure marketing, and support advertising or property-sponsor analytics.

You may be able to manage cookies or tracking technologies through browser, device, app, or platform settings. Disabling essential technologies may prevent Vyo from verifying identity, processing payments, confirming location/proximity, enforcing safety rules, or providing rentals.

11. How Vyo Uses Information

Vyo may use information for the following purposes:

- provide, operate, secure, maintain, and improve the Vyo platform, app, Vyo Go, vehicles, chargers, support, rental flow, and property deployments;
- verify identity, age, driver eligibility, license status, liveness, facial match, address, payment validity, property eligibility, account status, and fraud risk;
- start, manage, monitor, restrict, end, bill, audit, and document rentals, including return-to-origin, charging, navigation, and safety acknowledgments;
- process payments, holds, deposits, taxes, fees, charges, refunds, chargebacks, collections, and financial reporting;
- provide routing, maps, geofence alerts, battery estimates, red-road overlays, safety prompts, drive monitoring, vehicle health, maintenance, recovery, and operational support;
- detect, investigate, prevent, and respond to unauthorized use, driver swapping, account compromise, payment fraud, chargebacks, theft, tampering, property violations, unsafe operation, incidents, and legal violations;
- preserve and use evidence for insurance, claims, disputes, lawsuits, arbitration, law enforcement, property partner issues, maintenance, warranty, and vehicle recovery;
- communicate with you about account, safety, billing, support, incidents, claims, legal notices, updates, promotions, and customer service;
- analyze and improve Vyo products, safety systems, pricing, vehicle deployments, property partnerships, underwriting, routing, support, and user experience;
- comply with legal obligations, government requests, subpoenas, warrants, court orders, arbitration rules, tax/accounting duties, insurer requirements, and regulatory requirements.

12. How Vyo Shares Information

Vyo may disclose information to the following categories of recipients for the purposes described in this Policy:

- identity verification, driver-license verification, fraud prevention, biometric/facial-recognition, liveness, and risk-screening providers, including Plaid, AWS Rekognition, and replacement or additional providers;
- payment processors, Stripe or replacement processors, banks, card networks, financing providers, payment gateways, billing vendors, collection agencies, and chargeback/dispute providers;
- camera, dashcam, storage, cloud, telemetry, GPS, cellular, router/modem, Vyo Go, mapping, routing, analytics, communications, support, cybersecurity, hosting, maintenance, and software providers;
- insurers, reinsurers, brokers, underwriters, claims administrators, adjusters, appraisers, attorneys, investigators, arbitrators, courts, regulators, law enforcement, emergency responders, and legal process recipients;

- Property Partners, property owners, property managers, HOAs, landlords, ground lessors, security providers, parking operators, Fleet Captains, on-site logistics contractors, and property staff, where reasonably necessary for eligibility, access, parking, charging, safety, incident response, billing, sponsorship, or property operations;
- towing, recovery, roadside, repair, maintenance, cleaning, storage, impound, vehicle manufacturer, dealer, charger, battery, hardware, and service vendors;
- advertising partners, sponsors, analytics providers, and business partners, using aggregated, deidentified, pseudonymized, limited, operational, safety, property, sponsorship, measurement, or business-reporting data, and not for cross-context behavioral advertising or targeted advertising using personal information unless Vyo first updates this Policy and provides any legally required opt-out mechanism;
- successors, assigns, lenders, investors, purchasers, acquirers, affiliates, or advisors in connection with financing, insurance, merger, acquisition, asset sale, reorganization, bankruptcy, business transfer, or corporate transaction;
- other persons or entities when you consent, when disclosure is necessary to provide the Services, when disclosure is reasonably necessary for safety/security/legal/claims purposes, or when Vyo reasonably believes disclosure is required or permitted by law.

Vyo does not currently sell personal information for money, sell biometric identifiers or biometric information, use biometric information for targeted advertising, or share personal information for cross-context behavioral advertising or targeted advertising as those terms are defined by applicable privacy laws. Vyo does not knowingly sell or share personal information of children. Vyo may share aggregated, deidentified, pseudonymized, limited, operational, safety, property, sponsorship, analytics, measurement, or business-reporting data as described in this Policy. If Vyo later uses cookies, pixels, SDKs, ad networks, cross-context behavioral advertising, targeted advertising, or similar tools in a way that applicable law treats as a sale, sharing, or targeted advertising, Vyo will update this Policy and provide any legally required opt-out mechanism before or at the time such processing begins.

13. Property Partners and Local Deployment Data

Vyo may share limited information with Property Partners and related property personnel to confirm eligibility, manage access, support resident/guest programs, locate vehicles, resolve parking or charging issues, investigate incidents, address damage or property complaints, enforce property rules, coordinate property-sponsored rentals, provide aggregate usage reporting, and protect people and property.

Shared property information may include account status, eligibility status, property association, vehicle location on or near the property, rental status, incident information, parking/charging issues, damage reports, violation reports, safety issues, support tickets, and aggregated/deidentified utilization data. Vyo does not intend to share raw biometric identifiers with Property Partners unless required by law, consent, insurance, claims, security, or a specific legal/safety need.

Property Partners may separately collect or control information through their own property systems, access systems, cameras, gates, guest records, resident portals, or management systems. Their privacy practices are governed by their own policies, not this Policy.

14. Evidence Preservation; Edge Storage; No Guarantee of Recording

Upon the occurrence of an incident, Vyo will use commercially reasonable efforts to preserve available footage and telemetry data related to that incident for the duration of any applicable claims period or legal hold. This preservation obligation applies to data Vyo can access through its systems at the time preservation is triggered.

Vyo has no obligation to retrieve or preserve data from third-party provider systems, camera manufacturer systems, BlackVue cloud, AWS, Plaid, Stripe, property systems, or other systems that Vyo does not have independent retrieval rights to at the time of the incident. Vyo has no obligation to preserve routine data that was overwritten, unavailable, corrupted, offline, not captured, not uploaded, or not identified as incident-related before preservation was triggered.

No absence of footage, missing data, corrupted storage, failed upload, or inability to retrieve a clip creates an inference against Vyo or any Released Party.

15. Retention of Non-Biometric Information

Vyo retains personal information for as long as reasonably necessary for the purposes described in this Policy, including account administration, rentals, safety, security, fraud prevention, payment, tax/accounting, property deployment, insurance, claims, vehicle maintenance, legal compliance, dispute resolution, arbitration, litigation, collections, and business operations.

Retention periods vary by data type and context. Routine operational records may be retained for shorter periods, while account, rental, payment, damage, incident, claims, insurance, legal, tax, and safety records may be retained

longer. Camera footage may be overwritten automatically by local storage limitations unless flagged, retrieved, preserved, or needed for a business/legal purpose.

If you request deletion, Vyo may delete, deidentify, anonymize, restrict, or retain information depending on the nature of the data, applicable law, legal exceptions, safety needs, open balances, pending claims, fraud/security issues, insurance requirements, legal holds, tax/accounting duties, and dispute-resolution needs. Backup or archived data may remain until overwritten or deleted in the ordinary course.

16. Security

Vyo uses reasonable administrative, technical, and physical safeguards designed to protect information in light of its nature, sensitivity, volume, and business context. These safeguards may include encryption, access controls, provider tokenization, audit logs, authentication controls, role-based access, network controls, monitoring, and limited data retention.

No system is perfectly secure. Vyo cannot guarantee that information, cameras, data cards, cloud systems, app systems, provider systems, cellular systems, payment systems, or vehicle systems will be free from unauthorized access, loss, corruption, outage, interception, or misuse.

You are responsible for securing your device, account credentials, payment method, and app access. If you believe your account has been compromised, immediately contact Vyo through the app or hello@vyorides.com.

17. Your Privacy Choices and Rights

Depending on your state or country of residence and applicable law, you may have rights to request access, correction, deletion, portability, limitation, opt-out of sale/sharing/targeted advertising, limitation of sensitive personal information use, withdrawal of consent, appeal of a denied request, or other rights. Vyo will honor applicable non-waivable rights.

To submit a privacy request, contact Vyo at hello@vyorides.com or Vyo Corp, 10179 E Cortez Dr, Scottsdale, AZ 85260. Include your full name, email address, phone number, account identifier if available, state of residence, and the request you are making. Vyo may verify your identity before responding and may request additional information to protect account security.

Vyo's designated contact for privacy requests and appeals is hello@vyorides.com. Vyo will respond to verifiable privacy requests within the timeframe required by applicable law, which is generally 45 days from receipt of a verifiable request, subject to extensions permitted by law. If Vyo requires an extension, Vyo will notify you within the initial response period. Response times may vary depending on the nature of the request, applicable law, verification requirements, account-security needs, and whether the request involves safety, insurance, claims, fraud, law-enforcement, legal-hold, or evidence-preservation records.

Vyo may deny or limit a request where allowed by law, including where data is needed for identity verification, security, fraud prevention, rental operations, payments, chargebacks, collections, safety, insurance, claims, legal compliance, tax/accounting, incident evidence, dispute resolution, arbitration, litigation, legal holds, or protecting the rights of Vyo, Released Parties, users, passengers, Property Partners, insurers, or others.

If Vyo denies a request and applicable law gives you an appeal right, Vyo will include information about the basis for denial and instructions for submitting an appeal. You may appeal by replying to the denial or sending a new email to hello@vyorides.com with "Privacy Appeal" in the subject line. Vyo will process appeals as required by applicable law.

18. U.S. State Privacy Disclosures

This Section provides general U.S. state privacy disclosures. The categories of personal information Vyo may collect include identifiers, contact information, driver-license/identity information, government ID information, protected classification information such as age where applicable, commercial information, payment and transaction information, internet/device/app activity, precise geolocation, audio/visual information, biometric information used for identification or authentication, professional or property-related information where relevant, sensitive personal information, inferences/risk scores, and support/incident/legal records.

Vyo may collect these categories from you, your device, vehicles, cameras, telemetry systems, Vyo Go, payment processors, identity-verification providers, biometric providers, property partners, insurers, claims administrators, support vendors, service providers, public or government sources, law enforcement, and other third parties. Vyo may disclose these categories to the recipient categories listed in this Policy.

Vyo uses personal information for the business and commercial purposes listed in this Policy. Vyo does not currently sell personal information for money, sell biometric identifiers or biometric information, or share personal information for cross-context behavioral advertising or targeted advertising as those terms are defined by applicable privacy laws.

If Vyo later uses cookies, pixels, SDKs, advertising networks, analytics tools, cross-context behavioral advertising, targeted advertising, or similar tools in a way that applicable law treats as a sale, sharing, or targeted advertising, Vyo will update this Policy and provide any legally required opt-out mechanism before or at the time such processing begins. A browser or device-level global privacy control may be honored where required and technically feasible for website/app advertising choices, but it will not disable essential identity, payment, safety, GPS, telemetry, camera, biometric, insurance, or rental processing required to provide Vyo services.

California residents may have rights to know, access, delete, correct, opt out of sale/share, and limit certain uses of sensitive personal information, subject to legal exceptions. Florida, Colorado, Virginia, Connecticut, Texas, Oregon, and other state residents may have similar privacy rights depending on applicability thresholds and non-waivable law. Exercising privacy rights will not result in unlawful discrimination, but Vyo may be unable to provide services that require the data you ask Vyo not to process.

19. Sensitive Data Consent and Essential Processing

Vyo services require processing of sensitive data, including government ID information, precise geolocation, driver-license information, payment information, biometric/facial-verification information, camera/video information, and safety/incident data. By accepting this Policy and using Vyo, you consent to Vyo processing sensitive data for the purposes described in this Policy, the Terms, Rental Agreement, and Waiver.

If you withdraw consent or ask Vyo to stop processing information that is necessary for identity verification, payment, biometric ignition, safety monitoring, GPS/telemetry, insurance, claims, or legal compliance, Vyo may be unable to provide the Services and may suspend, restrict, or terminate your account or rental access.

Vyo may use deidentified, anonymized, aggregated, or pseudonymized information for analytics, safety, research, property deployment, insurance, underwriting, fleet management, advertising measurement, and business purposes. Vyo will take reasonable measures required by law to avoid reidentifying deidentified data except as permitted by law.

20. Children and Minors

Vyo accounts are only for users who are at least 21 years old. Vyo services are not directed to children under 13. Vyo does not knowingly allow children under 13 to create accounts or submit account information. If you believe a child under 13 provided account information to Vyo, contact hello@vyorides.com so Vyo can review and delete or restrict the information as required by law, subject to safety, legal, claims, insurance, fraud, and evidence exceptions.

Children under 12 are prohibited from riding in Vyo Vehicles. Passengers under 16 must comply with the Rental Agreement and Waiver minor-passenger rules, and minors may be incidentally captured by vehicle or property-area cameras where a renter violates passenger rules or where lawful recording captures surrounding activity. Such incidental data is processed for safety, security, legal, claims, insurance, and evidence purposes.

Vyo does not knowingly sell or share personal information of children for targeted advertising. If Vyo ever collects information online from a child under 13 with actual knowledge in a context covered by COPPA, Vyo will follow applicable parental notice and consent requirements or delete/restrict the information as required by law.

21. Passengers, Bystanders, and Third Parties

Passengers do not necessarily create Vyo accounts or separately accept Vyo documents. The renter is responsible for providing passenger notice before any passenger enters or remains in a Vehicle. The required passenger notice is set forth in the Rental Agreement and Waiver and includes notice of cameras, video, audio-capable systems where enabled and lawful, GPS, telemetry, biometric/identity systems, local storage, provider storage, Vyo storage, and possible disclosure to insurers, attorneys, law enforcement, regulators, property partners, service providers, and dispute-resolution providers.

If you are a passenger or bystander, Vyo may collect or process your image, video, location, incident involvement, statements, contact information, insurance information, claim information, or other data if you are in or near a Vyo Vehicle, property deployment, incident, support event, legal request, or claims process. You may contact hello@vyorides.com with privacy questions, but Vyo may retain and use information as needed for safety, security, claims, insurance, legal compliance, dispute resolution, and evidence preservation.

Vyo is not responsible for a renter's failure to provide passenger notice. The renter's failure to provide notice does not limit Vyo's right to process data for lawful safety, claims, insurance, legal, and evidence purposes, nor does it void the renter's indemnity obligations.

22. Law Enforcement, Legal Process, and Emergency Disclosure

Vyo may disclose information where Vyo reasonably believes disclosure is required or permitted by law, subpoena, warrant, court order, arbitration order, legal process, regulator request, law enforcement request, emergency responder request, insurance requirement, claims process, property safety issue, fraud investigation, security incident, or to protect the rights, safety, property, or operations of Vyo, Released Parties, users, passengers, Property Partners, insurers, providers, or the public.

Vyo may disclose relevant account, rental, vehicle, GPS, telemetry, camera, biometric, payment, support, incident, and identity records to emergency responders, law enforcement, insurers, claims administrators, attorneys, arbitrators, courts, regulators, property personnel, or others where Vyo determines disclosure is reasonably necessary or appropriate.

23. International Users

Vyo is intended for use in the United States and is not directed to residents of the European Economic Area, United Kingdom, Switzerland, or other countries unless Vyo expressly makes the Services available there. If you access Vyo from outside the United States, you understand that information may be processed in the United States and by U.S.-based or other providers.

If non-U.S. privacy law applies, Vyo will process requests required by non-waivable law, but Vyo may deny access to the Services where Vyo cannot comply with required identity, payment, rental, insurance, vehicle, biometric, or safety controls.

24. Changes to This Policy

Vyo may update this Policy from time to time. Updated versions may be posted in the app, on the website, or provided by email, support notice, in-app notice, or another reasonable method. The "Last Updated" date identifies the current version.

Material changes to biometric processing, audio recording, sensitive data processing, sale/sharing/targeted advertising, or dispute-related data practices will be presented for affirmative acceptance where required by law or by Vyo's Terms. Your continued use after a lawful update indicates acceptance where permitted by law. If you do not agree to a required change, do not use Vyo.

25. Contact Information; Privacy Requests; Notices

Routine privacy questions and requests may be sent to hello@vyorides.com. Legal notices to Vyo must be sent to Vyo Corp, 10179 E Cortez Dr, Scottsdale, AZ 85260, and by email to hello@vyorides.com, unless Vyo designates a different notice address in the app, website, or written notice.

When submitting a privacy request, include enough information for Vyo to verify your identity and locate your account. Do not send unnecessary sensitive information by unsecured email. Vyo may respond through the app, email, support channel, or other contact information associated with your account.

EXHIBIT A - BIOMETRIC NOTICE, CONSENT, WRITTEN RELEASE, AND RETENTION SUMMARY

This Exhibit A is incorporated into the Vyo Privacy Policy, Terms of Service, Rental Agreement, Liability Waiver, and every applicable account/rental acceptance. It is intended to be a public written biometric policy and written notice to the extent required by applicable law.

A. Categories

Vyo and its providers may collect or process facial images, liveness checks, face geometry, biometric identifiers, biometric information, biometric comparison results, verification outputs, authentication logs, screenshots, clips, timestamps, risk scores, and metadata, depending on provider and system configuration.

B. Purposes

The purposes are identity verification, age and driver eligibility, account security, vehicle access, ignition/restart authorization, continuous or randomized driver authentication, fraud prevention, unauthorized-driver detection, safety enforcement, incident review, claims, insurance, legal compliance, records retention, and dispute resolution.

C. Consent and Written Release

By accepting this Policy and the Vyo documents electronically, you provide informed written consent, written release, electronic signature, and authorization for Vyo and its providers to collect, capture, receive, process, store where

applicable, use, disclose, and rely on biometric-related information for the purposes described above and elsewhere in this Policy.

D. Retention and Destruction

Vyo retains or causes retention only as reasonably necessary for the purposes described in this Policy and, for biometric identifiers or biometric information subject to a law requiring a public retention schedule, absent a valid warrant, subpoena, court order, legal hold, or other non-waivable lawful basis requiring different retention, Vyo will destroy or cause destruction when the initial purpose has been satisfied or within 3 years after your last interaction with Vyo, whichever occurs first.

For purposes of this Exhibit, 'last interaction with Vyo' has the meaning stated in Section 9 of this Policy and does not include Vyo's internal use, review, storage, preservation, legal hold, claims handling, insurance processing, fraud prevention, litigation, compliance, evidence preservation, or other back-office processing of retained records after your account or rental activity has otherwise become inactive.

E. No Sale

Vyo will not sell, lease, trade, or otherwise profit from biometric identifiers or biometric information in a manner prohibited by law. Vyo will not use biometric information for targeted advertising.

F. Disclosure

Vyo may disclose biometric-related information to authorized providers, for transactions you authorize, with your consent, where required or permitted by law or valid legal process, for safety/security/fraud prevention, for insurance/claims/legal defense, and as otherwise permitted by applicable biometric law.

EXHIBIT B - DATA CATEGORY AND RECIPIENT SUMMARY

This summary is provided to help users, reviewers, insurers, and privacy reviewers understand Vyo's data model. It does not limit the full Policy.

- Identity and eligibility: name, DOB, address, phone, email, driver license, verification results, fraud scores, property eligibility, liveness/facial match records.
- Payments: payment tokens, billing data, card metadata, authorizations, transaction records, chargebacks, refunds, collections.
- Rental and vehicle operations: vehicle ID, VIN, start/end, GPS, route, telemetry, speed, battery, charger, geofence, return-to-origin, vehicle health, support, incidents.
- Camera and evidence: video, images, motion events, incident clips, cabin and roadway views, local data card records, BlackVue or other camera-provider storage, cloud or Vyo storage.
- Biometric: facial images, liveness, face geometry, comparison results, authentication logs, verification outputs, timestamps and related metadata.
- Recipients: Vyo providers, Plaid, Stripe, AWS Rekognition or replacements, camera/cloud/telemetry/mapping/communications providers, insurers, claims administrators, attorneys, law enforcement, regulators, property partners, Fleet Captains, repair/recovery vendors, collection vendors, and business transaction parties.

PRIVACY POLICY ACCEPTANCE

BY ACCEPTING THIS PRIVACY POLICY, CREATING OR USING A VYO ACCOUNT, USING THE APP OR VYO GO, PRESSING AGREE & BEGIN RENTAL, UNLOCKING, ACCESSING, ENTERING, RIDING IN, OPERATING, OR USING ANY VYO VEHICLE OR SERVICE, YOU ACKNOWLEDGE THAT YOU HAVE READ, UNDERSTOOD, AND AGREED TO VYO'S PRIVACY, BIOMETRIC, CAMERA, GPS, TELEMETRY, PAYMENT, IDENTITY, AND DATA PRACTICES DESCRIBED IN THIS POLICY.

YOU ALSO PROVIDE THE BIOMETRIC, CAMERA, VIDEO, AUDIO-CAPABLE, GPS, TELEMETRY, PAYMENT, AND IDENTITY CONSENTS AND AUTHORIZATIONS DESCRIBED IN THIS POLICY, THE TERMS, THE RENTAL AGREEMENT, AND THE WAIVER TO THE FULLEST EXTENT PERMITTED BY LAW.

IF YOU DO NOT AGREE, DO NOT USE VYO.