VEYRO TECHNOLOGIES

Enterprise Privacy Policy

Master Policy — Applies to All Products and Services Under the Veyro Technologies Brand

Effective Date: March 17, 2026 | Last Updated: March 17, 2026

Legal Entity: Global Solutions Consulting Tech LLC

State of Incorporation: New Mexico, United States

Principal Place of Operations: New Jersey, United States

Governing Law: United States Federal Law • New Mexico State Law • New Jersey State Law • Other Applicable State Laws

---

Scope and Applicability of This Policy

This Enterprise Privacy Policy ("Policy") is the master privacy document of Veyro Technologies, a brand operated by Global Solutions Consulting Tech LLC ("Company," "we," "us," or "our"), a limited liability company organized and registered under the laws of the State of New Mexico, with its principal place of operations in the State of New Jersey, United States.

This Policy applies universally to all products, services, platforms, mobile applications, websites, APIs, and digital properties that are currently operated, or that may in the future be developed, acquired, or launched, under the Veyro Technologies brand or by Global Solutions Consulting Tech LLC (collectively, the "Services"). Current Services subject to this Policy include, but are not limited to:

- veyrotech.io — Corporate website and developer portal
- Veyro Food — Consumer food delivery and ordering application
- Veyro Driver — Delivery driver management and earnings application
- Any future consumer applications, SaaS platforms, B2B tools, marketplaces, or financial services products launched under the Veyro Technologies brand

The launch of any new product or service under the Veyro Technologies brand does not require a separate privacy policy, provided the new product does not process categories of personal information materially different from those described herein, and does not operate in a sector subject to specialized federal privacy regulation (such as HIPAA for healthcare or GLBA for financial services). In such cases, a product-specific privacy addendum will be issued and incorporated by reference into this Policy.

By accessing or using any of our Services, you acknowledge that you have read, understood, and agree to the collection and use of your information as described in this Policy. If you do not agree, please discontinue use of the applicable Service immediately.

1. Applicable Legal Framework

This Policy is designed to comply in full with the following applicable United States federal and state privacy, consumer protection, and data security laws. Additional product-specific legal obligations are addressed in the Product Addenda attached to this Policy.

1.1 New Mexico Law (State of Incorporation)

- New Mexico Data Breach Notification Act, N.M.S.A. 57-12C-1 et seq.
- New Mexico Unfair Practices Act (NMUPA), N.M.S.A. 57-12-1 et seq.

1.2 New Jersey Law (State of Principal Operations)

- New Jersey Data Privacy Act (NJDPA), P.L. 2023, c. 266, effective January 15, 2025
- New Jersey Identity Theft Prevention Act (NJITPA), N.J.S.A. 56:11-44 et seq.
- New Jersey Consumer Fraud Act (NJCFA), N.J.S.A. 56:8-1 et seq.

1.3 Federal Law

- Children's Online Privacy Protection Act (COPPA), 15 U.S.C. § 6501 et seq.
- Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 et seq.
- CAN-SPAM Act, 15 U.S.C. § 7701 et seq.
- Telephone Consumer Protection Act (TCPA), 47 U.S.C. § 227
- Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2510 et seq.
- Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. § 6801 et seq. — applicable to any future financial services products

1.4 Other State Privacy Laws

- California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA), Cal. Civ. Code § 1798.100 et seq.
- Virginia Consumer Data Protection Act (VCDPA), Va. Code Ann. § 59.1-575 et seq.
- Colorado Privacy Act (CPA), C.R.S. § 6-1-1301 et seq.
- Connecticut Data Privacy Act (CTDPA), Conn. Gen. Stat. § 42-515 et seq.
- Texas Data Privacy and Security Act (TDPSA), Tex. Bus. & Com. Code § 541.001 et seq.
- Other applicable state consumer privacy statutes in jurisdictions where our Services are available

2. Information We Collect

We collect personal information across our Services. The specific categories collected depend on the Service you use. “Personal information” means any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked to a particular individual or household.

2.1 Universal Categories (All Services)

The following categories of personal information may be collected across all current and future Veyro Technologies products:

- **Identity Data:** Full name, username, and account credentials.
- **Contact Data:** Email address, phone number, and mailing address.
- **Account Data:** Account preferences, settings, communication history, and support interactions.
- **Device and Technical Data:** Device identifiers, operating system, browser type, IP address, and network information.
- **Usage and Behavioral Data:** Features accessed, content viewed, search queries, session duration, and interaction logs.
- **Transaction Data:** Purchase history, payment status, and order records.
- **Communications Data:** Messages, feedback, and support correspondence submitted through any Service.
- **Log Data:** Server logs, access timestamps, referring URLs, and error reports.

2.2 Service-Specific Categories

In addition to the universal categories above, specific Services may collect the following additional categories of personal information. See the Product Addenda at the end of this Policy for full details by product.

- **Geolocation Data:** Precise GPS coordinates, collected by location-dependent Services such as delivery and mapping applications.
- **Driver and Contractor Data:** Government-issued identification, vehicle information, insurance documentation, and banking/payout details, collected by driver-facing platforms.
- **Business and Professional Data:** Company name, job title, business address, and industry, collected by B2B and SaaS products.
- **Financial and Payment Data:** Payment instrument details processed by PCI-DSS certified third-party processors. Full card numbers are never stored by Veyro Technologies.
- **Commercial and Inventory Data:** Product listings, pricing, inventory levels, and store configurations, collected by marketplace and merchant-facing products.
- **Financial Services Data:** For any future financial services products, income, credit, banking, and related data, subject to GLBA and applicable state financial privacy laws.

2.3 Information Collected Automatically

- **Cookies and Tracking Technologies:** Used on web properties for session management, analytics, and personalization. See Section 10.
- **Mobile Analytics:** Resettable device advertising identifiers used for aggregate analytics in mobile applications.
- **Performance Monitoring:** Crash reports, error logs, and performance metrics to maintain Service quality.

2.4 Information from Third Parties

- **Payment Processors:** Transaction metadata from PCI-DSS certified processors. We do not receive full card numbers.
- **Identity Verification Providers:** Verification results from FCRA-compliant background check providers, used for contractor and driver onboarding.
- **Authentication Providers:** Name and email address from third-party sign-in providers (e.g., Google, Apple) when you use social login.
- **Biometric Authentication:** Biometric authentication is handled entirely by your device's built-in security hardware. Veyro Technologies does not collect, store, or process biometric identifiers.

3. How We Use Your Information

We process personal information only for lawful purposes consistent with applicable federal and state law. Our processing purposes include:

3.1 Service Delivery

- Providing, operating, maintaining, and improving all current and future Veyro Technologies products and services.
- Processing transactions, fulfilling orders, and disbursing payments and earnings.
- Enabling real-time features such as order tracking, live notifications, and location-based services.
- Authenticating users and managing account security across all Services.

3.2 Communications

- Sending transactional notifications essential to Service operation (order confirmations, security alerts, OTP codes).
- Responding to customer support inquiries and resolving disputes.
- Notifying users of material changes to this Policy or our Terms of Service.

- Sending promotional and marketing communications with your prior express consent where required by applicable law.

3.3 Safety, Security, and Fraud Prevention

- Detecting, investigating, and preventing fraudulent, abusive, or illegal activity across all Services.
- Verifying the identity and eligibility of contractors, drivers, and business partners.
- Maintaining the integrity and security of our platforms and infrastructure.

3.4 Legal and Regulatory Compliance

- Complying with applicable federal, New Mexico, New Jersey, and other state laws and regulations.
- Responding to valid legal process from courts, government agencies, and law enforcement.
- Maintaining records required for tax, financial, and regulatory compliance.

3.5 Business Development and Analytics

- Conducting internal research and analytics to develop new products and improve existing Services.
- Analyzing aggregate usage patterns to optimize platform performance and user experience.
- Evaluating potential new markets, product categories, and business opportunities.

3.6 Personalization

- Personalizing your experience across Services based on preferences, history, and usage patterns.
- Providing relevant recommendations, content, and offers tailored to your interests.

4. Disclosure of Your Information

We do not sell your personal information as defined under the NJDPA, CCPA/CPRA, NMUPA, or any other applicable state privacy law. We disclose personal information only as described below:

4.1 Service Providers and Data Processors

We engage trusted third-party vendors who process personal information on our behalf under written data processing agreements that prohibit use of your data for any purpose other than providing contracted services:

- **Payment Processors (e.g., Stripe):** PCI-DSS certified payment processing and fraud detection.
- **Cloud Infrastructure Providers:** Hosting, storage, and computing infrastructure for all Services.
- **Analytics Providers:** Anonymized, aggregated usage analytics.
- **Communication Providers:** SMS, email, and push notification delivery.
- **Identity and Background Verification Providers:** FCRA-compliant contractor and driver screening.
- **Mapping and Geolocation Providers:** Route optimization and location services.
- **Customer Support Platforms:** Ticketing and support management tools.
- **Marketing and CRM Platforms:** Campaign management tools, subject to your consent where required.

4.2 Operational Counterparties

Depending on the Service used, we may share necessary information with operational counterparties:

- **Restaurant and Merchant Partners:** Order details and customer first name and delivery address, solely to fulfill orders.
- **Delivery Contractors:** Customer first name, delivery address, and phone number, solely for delivery fulfillment.
- **B2B Customers (future SaaS products):** Usage and configuration data necessary to provide contracted software services.
- **Marketplace Sellers and Buyers (future marketplace products):** Transaction information necessary to complete marketplace orders.

All operational counterparties are contractually prohibited from retaining or using your personal information for any purpose beyond the specific transaction for which it was shared.

4.3 Legal Process and Government Requests

We may disclose personal information in response to valid legal process including subpoenas, court orders, or lawful government requests under federal, New Mexico, New Jersey, or other applicable law. We will make reasonable efforts to notify affected users prior to disclosure where permitted by law.

4.4 Protection of Rights and Safety

We may disclose personal information where reasonably necessary to protect the rights, property, or safety of Veyro Technologies, our users, partners, or the public, or to investigate and prevent fraud or illegal conduct.

4.5 Corporate Transactions

In connection with a merger, acquisition, reorganization, or asset sale, personal information may be transferred to a successor entity. We will provide at least 30 days' advance notice via email and in-app notification, and any successor must honor this Policy or obtain your affirmative consent to materially different terms.

4.6 With Your Consent

We may share your personal information with third parties outside the categories above only with your specific, informed, and unambiguous prior consent, which you may withdraw at any time.

5. Geolocation Data

Where our Services use precise geolocation data, we apply the following standards:

- Location data is collected only for Services where it is operationally necessary (e.g., delivery, mapping, or location-based search features).
- Foreground location is collected when the applicable app is open and in active use.
- Background location is collected only where explicitly required for service operation (e.g., active delivery tracking for drivers), with clear in-app notice provided before collection begins.
- Location data is not used for targeted advertising and is not sold to third parties.
- You may revoke location permissions at any time through your device settings, though this may limit functionality of location-dependent Services.
- Location data is retained only for the period necessary to fulfill the stated purpose and in accordance with the retention schedule in Section 6.

6. Data Retention

We retain personal information only as long as necessary to fulfill the purposes described in this Policy or as required by applicable federal, New Mexico, and New Jersey law:

- **Account and Profile Data:** Retained during account activity and for 3 years following closure or verified deletion.
- **Transaction and Order History:** Retained for 5 years for tax and legal compliance under the Internal Revenue Code and applicable state tax statutes.

- **Contractor and Driver Records:** Retained for the duration of the relationship and 3 years following termination, consistent with FCRA and applicable employment laws.
- **Financial and Payment Records:** Retained for 7 years per IRS recordkeeping requirements and applicable financial regulations.
- **Server and Access Logs:** Retained for 12 months for security monitoring.
- **Marketing Consent Records:** Retained for the consent period plus 3 years to demonstrate regulatory compliance.
- **B2B and SaaS Customer Data:** Retained per the terms of the applicable customer agreement, not to exceed 5 years after contract termination absent a legal hold.
- **Financial Services Data (future products):** Retained in accordance with GLBA, applicable state financial privacy laws, and product-specific addenda.

Upon expiration of applicable retention periods, personal information is securely deleted or anonymized. You may request early deletion as described in Section 7.

7. Your Privacy Rights

We honor all privacy rights granted under applicable federal and state law. We will not discriminate against you for exercising any right described in this Section.

7.1 Rights Under the New Jersey Data Privacy Act (NJDPA, P.L. 2023, c. 266)

- **Right to Access:** Confirm whether we process your personal data and obtain a portable copy.
- **Right to Correction:** Request correction of inaccurate personal data.
- **Right to Deletion:** Request deletion of personal data, subject to legal exceptions.
- **Right to Data Portability:** Obtain your data in a portable, machine-readable format.
- **Right to Opt Out of Targeted Advertising:** Opt out of processing your data for targeted advertising.
- **Right to Opt Out of Sale:** Opt out of the sale of your personal data. We do not sell personal data.
- **Right to Opt Out of Profiling:** Opt out of profiling that produces legal or similarly significant effects.
- **Right to Appeal:** Appeal our decision if we decline your request. Unresolved appeals may be directed to the New Jersey Division of Consumer Affairs at www.njconsumeraffairs.gov.

Response time: 45 days, with one 45-day extension where necessary.

7.2 Rights Under the CCPA/CPRA (California Residents)

- Right to Know: categories and specific pieces of personal information collected, sources, purposes, and recipients.
- Right to Correct inaccurate personal information (CPRA § 1798.106).
- Right to Delete (CCPA § 1798.105), subject to exceptions.
- Right to Opt Out of Sale or Sharing for behavioral advertising (CCPA § 1798.120). We do not sell or share.
- Right to Limit Use of Sensitive Personal Information (CPRA § 1798.121).
- Right to Non-Discrimination (CCPA § 1798.125).

Response time: 45 days, with one 45-day extension where necessary.

7.3 Rights Under Other State Laws

Residents of Virginia (VCDPA), Colorado (CPA), Connecticut (CTDPA), Texas (TDPSA), and other states with enacted consumer privacy laws have substantially similar rights. We will honor requests from residents of those states consistent with applicable law.

7.4 Opt-Out of Marketing

You may opt out of promotional emails via the “Unsubscribe” link in any marketing communication (CAN-SPAM Act). You may opt out of SMS promotions by replying STOP (TCPA). You may manage push notification preferences through your device settings or in-app under Account Settings > Notifications. Transactional and security notifications cannot be disabled while your account is active.

7.5 Submitting a Privacy Rights Request

To exercise any right described in this Section: (a) email privacy@veyrotech.io with subject line “Privacy Rights Request,” including your full name, account email, state of residence, the specific Service involved, and the nature of your request; or (b) use the in-app Privacy Settings under Account Settings > Privacy. Authorized agents must provide written authorization. We will verify your identity before processing any request.

8. Children’s Privacy (COPPA)

No Veyro Technologies Service is directed to children under the age of 13. We do not knowingly collect personal information from children under 13 without verifiable parental consent, in accordance with COPPA (15 U.S.C. § 6501 et seq.). All Services require users to be at least 18 years of age to register.

If we discover we have inadvertently collected data from a child under 13, we will promptly delete it. Parents or guardians may contact us at privacy@veyrotech.io.

9. Financial Information and Payment Data

Payment data submitted across all Veyro Technologies Services is processed by PCI-DSS Level 1 certified third-party payment processors. Veyro Technologies does not receive, store, or access full payment card numbers, CVV codes, or complete bank account credentials.

We receive only transaction metadata (identifiers, amounts, status, last four digits) used for confirmation, receipts, and fraud monitoring. Contractor and driver payout information is transmitted to payout partners using industry-standard encryption and retained per IRS and applicable state tax regulations.

For any future financial services products subject to the Gramm-Leach-Bliley Act (GLBA), a product-specific privacy addendum will be issued detailing the additional data practices and consumer rights applicable to those products, consistent with GLBA's privacy and safeguards rules.

10. Cookies and Tracking Technologies

We use cookies and similar technologies across our web properties:

- **Strictly Necessary Cookies:** Required for core functionality. Cannot be disabled.
- **Functional Cookies:** Remember preferences and settings to enhance your experience.
- **Analytics Cookies:** Collect anonymized, aggregated usage data with IP anonymization enabled.
- **Marketing Cookies:** Deliver relevant promotional content. Third-party behavioral advertising cookies require your prior consent.

We honor Global Privacy Control (GPC) and Do Not Track (DNT) signals to the extent required by applicable law. Mobile applications use resettable device advertising identifiers manageable through your device's privacy settings.

11. Data Security

We maintain a comprehensive information security program applicable to all Veyro Technologies products, consistent with the New Mexico Data Breach Notification Act, NJITPA, NJDPA, and applicable federal law:

- TLS 1.2 or higher encryption for all data in transit.
- Encryption of sensitive personal information stored at rest.
- Role-based access controls limiting data access to authorized personnel.
- Multi-factor authentication for all internal system access.

- Regular third-party penetration testing and vulnerability assessments.
- PCI-DSS Level 1 compliant payment processing.
- Employee privacy and security training programs.
- Documented incident response procedures consistent with all applicable breach notification laws.

If you believe your account has been compromised, contact security@veyrotech.io immediately.

12. Data Breach Notification

12.1 New Mexico (N.M.S.A. 57-12C-1 et seq.)

- Notification to affected New Mexico residents within 45 days of breach discovery.
- Notification to the New Mexico Attorney General if the breach affects more than 1,000 New Mexico residents simultaneously.
- Notice by written letter, telephone, email, or substitute notice as permitted by law.

12.2 New Jersey (NJITPA, N.J.S.A. 56:11-44 et seq.)

- Notification to affected New Jersey residents without unreasonable delay.
- Notification to the New Jersey Division of State Police if the breach affects more than 1,000 New Jersey residents simultaneously.
- Notification to consumer reporting agencies if more than 1,000 residents are affected simultaneously.

12.3 Multi-State and Federal

We comply with breach notification requirements under the laws of all states where affected users reside, including California (Cal. Civ. Code § 1798.82), New York (SHIELD Act, GBL § 899-aa), Texas (Tex. Bus. & Com. Code § 521.053), Florida (Fla. Stat. § 501.171), and all other applicable statutes.

12.4 General Response Procedure

- Contain the incident and conduct a forensic investigation.
- Assess notification obligations under all applicable laws.
- Notify affected individuals within the most restrictive applicable timeframe.
- Notify the New Mexico Attorney General, New Jersey Division of State Police, and other required authorities.

- Provide a description of the breach, data involved, remediation steps, and recommended user actions.

13. Consumer Protection Compliance

13.1 New Mexico Unfair Practices Act (N.M.S.A. 57-12-1 et seq.)

As a company organized under New Mexico law, we conduct all operations in compliance with the NMUPA. We do not engage in unfair, deceptive, or unconscionable trade practices in connection with any of our Services or data practices. Complaints may be directed to the New Mexico Attorney General's Consumer Protection Division: consumerprotection@nmag.gov | 1-844-255-9210.

13.2 New Jersey Consumer Fraud Act (N.J.S.A. 56:8-1 et seq.)

With respect to our operations in New Jersey, we comply fully with the NJCFA. We do not engage in any deceptive, unconscionable, or fraudulent commercial practice in connection with our Services. Complaints may be directed to the New Jersey Division of Consumer Affairs: www.njconsumeraffairs.gov | 1-800-242-5846.

14. Electronic Communications

All promotional email communications comply with the CAN-SPAM Act (15 U.S.C. § 7701 et seq.) and include a clear opt-out mechanism. SMS promotional messages are sent only with prior express written consent as required by the TCPA (47 U.S.C. § 227); reply STOP to any message to revoke consent. Transactional and security notifications are necessary for Service operation and cannot be disabled while your account is active.

15. Third-Party Links and Integrations

Our Services may link to or integrate with third-party platforms. This Policy applies exclusively to Veyro Technologies Services. We are not responsible for the privacy practices of third parties and encourage you to review their policies before providing personal information.

16. International and Interstate Data Transfers

Global Solutions Consulting Tech LLC is organized in New Mexico and operates principally from New Jersey. All personal information is stored and processed on servers located within the United States. Users accessing our Services from outside the United States acknowledge and

consent to transfer and processing of their personal information in the United States under the protections described in this Policy.

17. Changes to This Policy

We may update this Policy at any time to reflect changes in our data practices, applicable law, or business operations. Material changes will be communicated via in-app notice at least 30 days before taking effect and by email to registered users. Minor changes (such as adding a new product covered by existing data practices) will be reflected by updating the “Last Updated” date and listing the new product in the Scope section. Continued use of any Service after the effective date constitutes acceptance of the revised Policy.

18. Governing Law and Dispute Resolution

This Policy is governed by a dual-jurisdiction framework:

- **Corporate and Structural Matters:** Governed by the laws of the State of New Mexico, the state of organization of Global Solutions Consulting Tech LLC.
- **Operational and Consumer Matters:** Governed by the laws of the State of New Jersey with respect to consumer-facing Services and obligations.
- **Federal Law:** All applicable federal laws govern their respective subject matters regardless of state.

Disputes not resolved informally shall be submitted to binding individual arbitration under the AAA Consumer Arbitration Rules, except where prohibited by law. Nothing herein limits your right to file complaints with the New Mexico Attorney General, New Jersey Division of Consumer Affairs, Federal Trade Commission, or other applicable regulatory authorities.

19. Contact Information

Veyro Technologies

Trade name of: Global Solutions Consulting Tech LLC

State of Incorporation: New Mexico, United States

Principal Place of Operations: New Jersey, United States

Registered Agent: On file with the New Mexico Secretary of State

Website: veyrotech.io

Privacy Requests: privacy@veyrotech.io

General Support: support@veyrotech.io
Security Incidents: security@veyrotech.io
Legal Inquiries: legal@veyrotech.io

New Mexico regulatory contact: New Mexico Attorney General — consumerprotection@nmag.gov | 1-844-255-9210

New Jersey regulatory contact: NJ Division of Consumer Affairs — www.njconsumeraffairs.gov | 1-800-242-5846

We respond to all privacy inquiries within 45 calendar days of receipt, or within the shorter period required by applicable law.

PRODUCT ADDENDUM A

Veyro Food — Consumer Food Delivery Application

This Addendum supplements the Veyro Technologies Enterprise Privacy Policy and applies specifically to the Veyro Food mobile application.

Additional Data Collected

- Precise delivery address and geolocation for order routing and delivery confirmation.
- Dietary preferences and order history used for personalized recommendations.
- Payment instrument metadata via Stripe for order processing.
- Device push notification token for order status alerts.

Additional Data Shared

- First name, order details, and delivery address shared with the fulfilling restaurant.
- First name, delivery address, and phone number shared with the assigned delivery driver.

Location Data

Foreground location collected while the app is in use. Background location not collected unless explicitly enabled by the user. Location used solely for order delivery and nearby restaurant discovery.

PRODUCT ADDENDUM B

Veyro Driver — Delivery Driver Application

This Addendum supplements the Veyro Technologies Enterprise Privacy Policy and applies specifically to the Veyro Driver mobile application.

Additional Data Collected

- Government-issued identification for identity verification under FCRA.
- Driver's license number, expiration date, and driving record from FCRA-compliant screening providers.
- Vehicle make, model, year, license plate, and proof of insurance.
- Bank account or payment routing information for earnings disbursement.
- Background and foreground geolocation while active on the platform.

Location Data

Foreground and background location collected while the driver is active on the platform and during active deliveries. Location collection stops automatically when the driver goes offline. Drivers receive in-app notice before background collection begins.

FCRA Notice

Background checks conducted during driver onboarding comply with the Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.). Drivers receive a separate FCRA disclosure and authorization prior to any background check being initiated.

PRODUCT ADDENDUM C

Future Products — Reserved Addenda

The following addenda will be issued upon launch of each new product category and incorporated by reference into this Enterprise Privacy Policy.

Addendum C-1 — SaaS and B2B Platform Products (Reserved)

Upon launch of any SaaS or B2B platform product under Veyro Technologies, this addendum will detail business customer data practices, data processing agreements available to enterprise customers, sub-processor lists, and any additional rights applicable to business users.

Addendum C-2 — Marketplace and eCommerce Products (Reserved)

Upon launch of any marketplace or eCommerce product, this addendum will detail seller and buyer data practices, transaction data handling, dispute resolution data use, and any state sales tax data obligations.

Addendum C-3 — Financial Services Products (Reserved)

Upon launch of any product subject to the Gramm-Leach-Bliley Act (GLBA) or state financial privacy laws, a full GLBA-compliant privacy notice will be issued as this addendum, detailing the categories of nonpublic personal financial information collected, how it is shared, and your opt-out rights under applicable law.

Addendum C-4 — Additional Delivery Categories (Reserved)

Upon launch of additional delivery verticals (such as grocery, pharmacy, or alcohol delivery), this addendum will address any category-specific regulatory requirements, including applicable alcohol delivery compliance, pharmacy data handling under state pharmacy laws, and any age verification data practices.