Cultioo

# Cultioo Scanner App — United States Privacy Policy

**Effective Date:** January 1, 2026
**Version:** 1.0
**Governing Entity:** Cultioo Inc., a Delaware Corporation

---

Cultioo Inc., a Delaware corporation, understands that privacy and the security of Personal Information (PI) are fundamental concerns for its users. This Privacy Policy details the data collection, usage, sharing, and security practices implemented by Cultioo in connection with the **Cultioo Scanner App**, in compliance with United States federal and state laws, including the regulations set forth by the Federal Trade Commission (FTC), the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA), and other applicable state privacy laws.

Cultioo is committed to maintaining the trust of its users by prioritizing data protection, implementing technical and organizational measures (TOMs) to secure user data, and ensuring transparency regarding all data processing activities.

---

## Table of Contents

---

# 1. Scope and Application

## 1.1 Scope

This Privacy Policy applies to all users of the Cultioo Scanner App ("App") and associated services within the United States of America. The Cultioo Scanner App functions as the physical-world verification layer of the Cultioo ecosystem — a professional logistics inspection and cargo verification tool for on-site operators at seller and buyer facilities participating in the Cultioo agricultural supply chain platform.

The App enables Operators to:

- Verify Delvioo™ drivers at facility gates using QR Code and Security Code dual-authentication
- Execute inbound and outbound cargo check-in and check-out workflows
- Record weights, temperatures, photographs, seal numbers, batch data, and compliance documents
- Generate and digitally sign immutable Chain of Custody Records and automated Delivery Notes
- Manage facility gate assignments and department configurations

## 1.2 Relationship to Other Cultioo Privacy Policies

This Privacy Policy applies specifically to the Cultioo Scanner App. Users who also access the Cultioo Business App (sellers, drivers, administrators) or the Cultioo App (buyers) are subject to the privacy policies applicable to those platforms. Where data flows between platforms — for example, seller-side dispatch data transmitted to buyer-side Operators — the handling of that data is governed by this Policy with respect to the Scanner App and by the Business App Privacy Policy with respect to the Business App.

### 1.3 Legal Framework

Cultioo's commitment to data privacy aligns with:

- Federal Trade Commission (FTC) Act — Requirements for fair data practices
- California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)
- Virginia Consumer Data Protection Act (VCDPA)
- Colorado Privacy Act (CPA)
- Connecticut Data Privacy Act (CTDPA)
- Utah Consumer Privacy Act (UCPA)
- Other applicable state privacy laws

### 1.4 Consent Through Use

By registering for or using the Cultioo Scanner App, you provide explicit consent to the collection and processing of your data in accordance with this Privacy Policy.

---

## 2. Company Information and Contact Details

**Responsible Entity:**

Cultioo Inc.
A Delaware Corporation
8 The Green, Ste A

Cultioo

Dover, DE 19901
United States of America

**Privacy Contact:** privacy@cultioo.com
**General Support:** support@cultioo.com
**Online Privacy Portal:** https://cultioo.com/en/en_cultioo_app_info#privacy

---

# 3. Definitions

## 3.1 Personal Information (PI)

Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Includes: names, email addresses, physical addresses, phone numbers, IP addresses, device IDs, and usage data.

## 3.2 Sensitive Personal Information (SPI)

A subcategory of Personal Information requiring enhanced protection, including:

- Precise geolocation data (GPS coordinates)
- Contents of private communications
- Other highly sensitive identifiers

## 3.3 Operational Data

Data generated by the Operator through the execution of logistics verification workflows within the App, including weight measurements, photographs, temperature records, seal numbers, batch data, compliance documents, digital signatures, and timestamps. Operational Data forms part of the Chain of Custody Record.

## 3.4 Chain of Custody Record

The complete, chronological, tamper-evident digital record of all verification events, Operational Data, and timestamps associated with a specific Order. Permanently stored in the Cultioo database. Immutable once the final QR departure scan is executed.

### 3.5 Sale

The selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating a consumer's personal information to another business or third party for monetary or other valuable consideration.

### 3.6 Sharing

The sharing, renting, releasing, disclosing, disseminating, making available, or transferring of a consumer's personal information to a third party for cross-context behavioral advertising.

### 3.7 Service Provider

A business that processes personal information on behalf of Cultioo and is contractually bound to use the data exclusively for the agreed-upon purposes.

---

## 4. Registration and Consent

### 4.1 Registration Requirement

Use of the Cultioo Scanner App requires the creation of a verified Cultioo account. Certain personal information must be provided during registration. Full operational access (Scanner Tab and Orders Tab) additionally requires membership in at least one Group via the 8-digit invitation code issued by the Group Founder.

### 4.2 Authentication Options

The App supports the following account creation and login methods:

- **Email/Password:** Standard registration with 8-digit email verification code activation
- **Google Login:** One-tap authentication via Google account
- **Apple Login:** One-tap authentication via Apple ID — compatible with Face ID and Touch ID

### 4.3 Explicit Consent

Upon registration or when modifying your data in Settings, you explicitly consent to the processing of your personal information in accordance with this Privacy Policy.

### 4.4 Right to Withdraw

You have the right to withdraw your consent at any time by deleting your account. Withdrawal does not affect the lawfulness of processing based on consent before its withdrawal. Completed Chain of Custody Records associated with your verified actions are subject to legal retention obligations (see Section 17) and may be retained following account deletion.

### 4.5 Data Storage Upon Registration

When registering or modifying account data, your information is securely stored in the Cultioo database. Passwords are stored exclusively in hashed (encrypted) form using industry-standard cryptographic protocols (e.g., bcrypt, Argon2). No Cultioo employee has access to your original password.

---

## 5. Categories of Personal Information Collected

In accordance with CCPA/CPRA, Cultioo discloses the following categories of personal information collected in connection with the Cultioo Scanner App:

### 5.1 CCPA/CPRA Category A: Identifiers

| | |
|---|---|
| **Data Collected** | Real name, username, email address, phone number, device ID, IP address |
| **Source** | User registration, device |
| **Primary Purpose** | Account management, authentication, security, operational access control |
| **Disclosed To** | Service Providers / Contractors |

### 5.2 CCPA/CPRA Category B: Personal Records Information

| | |
|---|---|
| **Data Collected** | Name, contact details |
| **Source** | User input |
| **Primary Purpose** | Group membership verification, operational coordination |
| **Disclosed To** | Service Providers / Contractors |

### 5.3 CCPA/CPRA Category F: Internet or Other Similar Network Activity

| | |
|---|---|
| **Data Collected** | App interaction data, session duration, settings changes, device/OS details, app version |
| **Source** | Device, app usage |
| **Primary Purpose** | Debugging, quality assurance, service improvement, security monitoring |
| **Disclosed To** | Analytics Providers / Service Providers |

### 5.4 CCPA/CPRA Category K: Sensitive Personal Information (SPI)

| | |
|---|---|
| **Data Collected** | Precise geolocation (device GPS coordinates) |
| **Source** | Device (with explicit device permission) |
| **Primary Purpose** | Geofenced arrival detection, detention timer activation |
| **Server Transmission** | **NEVER** — location data stored exclusively locally on device (see Section 10) |

---

# 6. Operational Data — Scanner App Verification Workflows

This section describes the Operational Data generated through the use of the App's verification workflows. This data is distinct from standard account Personal Information and is generated in the course of executing the logistics verification service.

## 6.1 Legal Basis for Processing Operational Data

Operational Data is processed under the legal bases of:

- **Contract Performance** — necessary to execute the logistics verification service and generate the Chain of Custody Record
- **Legitimate Business Interest** — necessary for dispute resolution, regulatory compliance, fraud prevention, and audit purposes
- **Legal Compliance** — required retention under applicable food safety, transport, and commercial record-keeping laws

## 6.2 Seller-Side Operational Data (Orders Tab)

The following data is generated, recorded, and permanently stored when an Operator executes the outbound cargo verification workflow:

**Check-In Data:**

- Gate and loading bay assignment selections (Department entries)
- Driver identity verification records (visual confirmation with timestamp)
- Vehicle license plate entries (scanned or manually entered)
- PPE compliance records (Pass ✅ / Fail ❌ with timestamp)
- Vehicle type suitability confirmation records
- Refrigeration unit and cooling aggregate status records (cold chain cargo)
- Load compartment hygiene inspection records (Pass ✅ / Fail ❌ with timestamp), including:
    - Visual cleanliness assessment
    - Odor-free confirmation

    - Moisture and condensation check
    - Prior cargo residue inspection
- Cleaning Certificate status records (Valid ✅ / Missing ❌ / Expired ⚠️)
- Cleaning Certificate physical verification records
- Pre-loading damage inspection photographs (timestamped, geotagged, permanently stored)
- Pre-loading vehicle exterior and interior inspection records
- Tare weight entries (empty vehicle weight, pre-loading) with scale identifier
- Arrival timestamp (automatic system capture)
- Check-in QR Code scan confirmation records

**Check-Out Data:**

- Gross weight entries (fully loaded vehicle, post-loading) with scale identifier
- Net weight calculations (Gross minus Tare) — legally binding delivery weight
- CullyAI™ deviation alert records (net weight vs. order quantity)
- Batch data entries:
    - Production Date
    - Best Before / Expiry Date
    - Batch Number
    - Storage Number
    - Optional handling Notes
- Departure temperature measurements (cold chain cargo, cargo core and compartment)
- Cold chain compliance confirmation records
- Cooling aggregate status at point of sealing
- Load security confirmation records (load straps, blocking bars, pallet stability)
- Hazardous material compliance records (ADR/DOT, where applicable)
- Dispatch condition photographs (2–3 images, timestamped, geotagged, permanently stored)
- Seal number entries (scanned or manually entered, immediately transmitted to buyer-side Operator)
- Physical seal application confirmation records

- Compliance document uploads:
  - Organic Certification
  - Origin Certificate
  - Analysis Reports (moisture, protein, pesticide, microbiological)
  - Bill of Lading
  - Other required documents per cargo type
- Document completeness checklist records
- Automated Digital Delivery Note (system-generated, distributed to all parties)
- Seller Operator digital signature (with timestamp)
- Driver digital signature (with timestamp)
- Signature refusal records (where applicable), including dispute record creation
- Departure timestamp (automatic system capture)
- Departure QR Code scan confirmation records

### 6.3 Buyer-Side Operational Data (Scanner Tab)

The following data is generated, recorded, and permanently stored when an Operator executes the inbound delivery verification workflow:

**Scanner Sub-Page Data:**

- QR Code scan events and results (timestamp, outcome)
- Security Code verbal verification confirmation records
- Seal number cross-reference entries and outcomes:
  - Match ✅ — recorded with timestamp
  - Mismatch ❌ — tamper event record with full evidence (timestamps, identity, route data)
  - Missing ⚠️ — absence record with buyer admin notification log

**Check-In Data (Stage 1):**

- Driver identity visual verification records (photo comparison confirmation)
- License plate scan or manual entry and cross-reference results
- Security Code verbal confirmation records
- Seal number entry and cross-reference results
- Seal condition assessment (intact / damaged / broken)

- Arrival vehicle condition inspection records and photographs (timestamped, geotagged)
- Comparison records against seller's pre-loading photographs
- Arrival temperature measurements (cold chain cargo, before fully opening doors)
- Cold chain compliance comparison records (seller departure temperature vs. buyer arrival temperature)
- Temperature deviation alerts (where applicable)
- Cleaning Certificate physical verification records
- Check-in confirmation timestamp
- Unloading instruction transmission records (bay assignment, unloading position, weighing sequence)

**Check-Out Data (Stage 2):**

- Gross weight entries (arrival, vehicle still loaded) with scale identifier
- Tare weight entries (post-unload) with scale identifier
- Net weight calculations (buyer-side received quantity)
- CullyAI™ three-point deviation alert records:
  - Order quantity vs. seller net weight vs. buyer net weight
  - Tolerance level (within ✅ / minor ⚠️ / significant ❌)
  - Payment hold triggers (where applicable)
- Inbound cargo condition photographs (timestamped, geotagged)
- Cargo condition assessments (Good ✅ / Damaged ⚠️ / Rejected ❌)
- Damage records:
  - Damage type classification
  - Photographic evidence
  - Description entries
- Partial rejection records (accepted quantity, rejected quantity)
- Batch data verification records (cross-reference against seller record):
  - Production Date verification
  - Best Before / Expiry Date verification
  - Batch Number verification
  - Note: For bulk goods (grain, oil, liquids) — verification is conducted against digital seller record only, not physical batch markings

- Compliance document verification records (physical vs. digital cross-reference)
- Missing or mismatched document flags
- Delivery Note reconciliation records
- Discrepancy summary records (where deviations exist)
- Buyer Operator digital signature (with timestamp)
- Driver digital signature (with timestamp)
- Signature refusal records (where applicable)
- Departure authorization timestamp
- Final QR Code departure scan confirmation records
- Payment release trigger records

## 6.4 Purpose of Operational Data

All Operational Data described in Sections 6.2 and 6.3 is processed for the following purposes:

- Execution of the logistics verification and cargo inspection service
- Creation and maintenance of the permanent, immutable Chain of Custody Record
- Enabling dispute resolution between commercial parties (sellers, buyers, drivers)
- Supporting regulatory compliance, food safety audits, and transport compliance requirements
- Generating automated Digital Delivery Notes and delivery documentation
- Enabling CullyAI™ anomaly detection, weight deviation alerts, and quality assurance
- Providing evidentiary documentation in the event of cargo damage claims, payment disputes, or fraud investigations
- Supporting food traceability and product recall capability via Batch Number records

## 6.5 Immutability of Chain of Custody Records

Once the final QR departure scan is executed and the check-out workflow is complete, the Chain of Custody Record for that Order is permanently sealed. It cannot be modified or deleted by any party — including Cultioo

employees, Group Founders, or Operators. This immutability is a core security and legal protection feature of the platform.

### 6.6 Multi-Section Vehicle Operational Data

For vehicles with multiple registered compartments (sections), each section generates a completely independent set of Operational Data. Each section's Chain of Custody Record is independent. A tamper event in one section does not affect other sections' records. Each section receives its own seal number, dispatch photographs, weight records, batch data, compliance documents, Digital Delivery Note, digital signatures, and QR departure scan record. Section-level data is transmitted to the corresponding buyer (per section assignment) — not to all buyers simultaneously.

---

## 7. Data Storage and Data Security

### 7.1 Our Commitment

**Protection and Privacy Are Our Priority.**

Cultioo treats data security as a core business function and implements comprehensive technical and organizational measures (TOMs) to protect user data from unauthorized access, use, or disclosure.

### 7.2 Technical and Organizational Measures (TOMs)

**a) Cryptography and Password Security**

- Irreversible Hashing: All user passwords are immediately encrypted upon creation using an irreversible hashing procedure
- No Plain Text Storage: Passwords are never stored in plain text
- No Employee Access: Cultioo employees and administrators have no access to your original passwords
- Industry Standard: Use of cryptographic standards (e.g., bcrypt, Argon2)

**b) Encrypted Data Transmission**

- Transport Layer Security (TLS): All data transmissions between the App and Cultioo servers occur over encrypted HTTPS/TLS connections
- End-to-End Protection: Protection against eavesdropping and man-in-the-middle attacks

**c) Access Control**

- Strict Internal Access Policies: Only authorized employees with legitimate business needs have access to personal information
- User-Exclusive Modifications: Personal account data can only be changed by the authenticated user via the secure App
- Operational Data Immutability: Completed Chain of Custody Records cannot be modified by any party after check-out completion

**d) Secure and Irreversible Deletion**

- Final Data Deletion: When you delete your account, all associated account data is finally and irrevocably removed from the database
- Exception: Completed Order Chain of Custody Records are subject to legal retention obligations (minimum 7 years) and may be retained beyond account deletion, in compliance with IRS and applicable food safety and transport record-keeping requirements

**e) Infrastructure Security**

- Secure Server Environment: Use of professional, certified data centers
- Regular Security Audits: Conducting penetration tests and security reviews
- Incident Response Plan: Established procedures for handling security incidents
- Regular Backups: Secure data backups to ensure data integrity

**f) Employee Training**

- Regular training of all employees on data privacy and data security
- Commitment to confidentiality

## 7.3 No Sharing with Third Parties for Marketing

Your personal information and Operational Data are not shared with third parties for advertising or marketing purposes.

---

# 8. Payment Processing

The Cultioo Scanner App does not directly process payment transactions by Operators. Operational data (specifically net weight calculations and delivery confirmations) may trigger automated payment processes within the Cultioo platform governed by the seller's and buyer's respective account agreements.

Where payout functionality applies (e.g., for Operators who also function as drivers within Delvioo™), all payment processing is conducted exclusively through **Stripe Inc.**, a leading PCI-DSS certified payment service provider.

- Cultioo does not store complete credit card numbers or bank account information
- Complete financial data is processed and stored exclusively by Stripe
- Stripe acts as an independent data controller for payment data it processes
- Users are subject to Stripe's separate privacy policy: https://stripe.com/privacy
- Cultioo assumes no responsibility for data processing by Stripe

---

# 9. Data Disclosure and Third-Party Access

## 9.1 Access by Commercial Transaction Parties

Operational Data recorded through the App is shared with the authorized parties to the corresponding Order as a necessary function of the service:

**Seller-side check-out data transmitted to buyer-side Operators and drivers:**

- Seal number (immediately upon entry — transmitted to buyer's Deliveries list and driver's order screen)
- Departure temperature
- Gross weight (loaded)
- Dispatch condition photographs
- Batch data (Production Date, Best Before Date, Batch Number, Notes)
- Compliance documents (certifications, analysis reports, Bill of Lading)
- Automated Digital Delivery Note

**Buyer-side check-out data stored in the permanent Order record accessible to:**

- The seller (via Cultioo Business App)
- The Group Founder and authorized Hosts of the seller's group
- Cultioo (for dispute resolution and compliance purposes)

## 9.2 Access by Group Administrators

Group Founders and authorized Group Hosts within the Cultioo Business App have access to all Order records, Chain of Custody Data, and operational documentation generated by Operators within their group. This access enables:

- Review of all outbound and inbound verification records
- Download of Delivery Notes and compliance documents
- Monitoring of detention time records
- Financial reconciliation (accepted quantities and payment release records)

## 9.3 Disclosure Due to Legal Obligations

Cultioo is obligated to disclose personal information and Operational Data upon lawful request to:

- **Law Enforcement Agencies:** In response to court orders, subpoenas, or statutory requirements
- **Government Agencies:** To fulfill regulatory obligations (e.g., food safety regulators, transport authorities)

- **Tax and Financial Authorities:** To comply with IRS and other tax-related retention requirements

Cultioo will notify users of such requests where legally permissible.

### 9.4 Disclosure in Corporate Transactions

In the event of a merger, acquisition, restructuring, or sale of assets, personal information and Operational Data may be transferred to the successor entity. The successor will be obligated to continue compliance with this Privacy Policy. Users will be informed in advance of such a transaction.

### 9.5 Aggregated and Anonymized Data

Cultioo may share aggregated, anonymized, or pseudonymized data that cannot be traced back to individual users for market research, industry analysis, and academic research. Such data is not considered personal information and is not subject to the restrictions of this Privacy Policy.

---

## 10. Location Data

### 10.1 How the App Uses Location Data

The Cultioo Scanner App accesses your device's GPS location data exclusively for the following operational purposes:

- **Geofenced Arrival Detection:** Determining when a Delvioo™ driver is within the 5 km/mi geofence radius of a declared delivery address, enabling the Arrived button and activating the waiting time timer
- **Detention Time Calculation:** The timestamp associated with geofenced arrival is used for automated detention billing calculations within the Cultioo platform
- **Operational Dashboard:** Displaying the count of trucks "in territory" (within the facility geofence) on the Home Tab

### 10.2 Privacy by Design — Local Storage, No Server Transmission

**IMPORTANT PRIVACY NOTICE**

Your precise GPS location as an Operator is stored **exclusively locally on your device** and is **NOT transmitted to Cultioo servers**.

- Location data is **NEVER** transmitted to the Cultioo database
- Location data is **NEVER** sent to Cultioo servers
- Location data is **NEVER** shared with or sold to third parties

This technical decision follows "Privacy by Design" principles and significantly minimizes the risk of misuse of your highly sensitive location information.

## 10.3 Driver Location Data

The real-time GPS position of Delvioo™ drivers is used for geofence detection, Arrived status triggering, route optimization within the Delvioo™ platform, and CullyAI™ transport opportunity matching. Driver location data is governed by the Cultioo Business App Privacy Policy and the Delvioo™ Terms applicable to drivers.

## 10.4 Control Over Location Access

You have complete control over location access at all times via your mobile device settings (iOS or Android):

- Completely disable location access
- Allow location access only while using the App
- Disable precise location (approximate location only)

**Note:** Disabling location services may limit geofence-dependent features, including Arrived status detection and the facility territory dashboard.

## 10.5 Classification as Sensitive Data

Precise location data is classified as Sensitive Personal Information (SPI) under CCPA/CPRA and receives enhanced protection. The use of location data occurs exclusively with your explicit consent, which you grant through your device's permission settings.

# 11. User Account and Personal Settings

## 11.1 Modifiable Account Data

You may modify your personal account data at any time via Account Settings in the App. Modifiable data includes:

- Name / username
- Email address
- Phone number
- Profile picture

All modifications are processed exclusively through the authenticated App session, preventing unauthorized changes by third parties.

## 11.2 Account Deletion

Account deletion requires entry of your current password and is immediate and irreversible upon confirmation. After confirmation:

- All account data associated with your account is finally and irrevocably removed from the database
- Data recovery is not possible
- Completed Order Chain of Custody Records associated with your verified actions are subject to legal retention obligations (see Section 17) and may be retained in accordance with applicable law

**Deletion Process:**

1. Navigate to Account Settings
2. Select "Delete Account"
3. Enter your current password for confirmation
4. Confirm final deletion

## 11.3 Password Change

Password changes require entry of the current password before a new password may be set. This prevents unauthorized password changes by anyone with physical device access.

**Recommendations:**

- Use a strong, unique password
- Never share your password with third parties
- Change your password if you suspect unauthorized access

### 11.4 Group Membership Management

You may join and leave groups via Account → Groups. Leaving a group immediately revokes your operational access to that group's Order data within the App. Chain of Custody Records generated during your group membership are permanently stored and remain accessible to authorized parties.

---

## 12. Department and Gate Management Data

### 12.1 Data Collected

The Departments Sub-Page within the Orders Tab enables Operators to create and manage named gates, loading bays, and facility sections. The following data is stored:

- Gate and loading bay names (e.g., "Gate A," "Bay 3," "Cold Storage Entrance")
- Section assignments linked to specific check-in workflows
- Import and export records of department lists

### 12.2 Purpose

Department data is used exclusively to:

- Populate the gate selection interface at the start of each check-in workflow

- Record which gate a driver was assigned to as part of the Chain of Custody Record
- Enable efficient facility management across multiple gates and loading zones

### 12.3 Retention

Department configuration data is retained as long as the associated Seller Group membership is active. It is not shared with third parties and is not used for any purpose beyond facility operations management within the App.

---

## 13. Data Usage: Business and Commercial Purposes

### 13.1 Business Purposes

Cultioo uses collected personal and Operational Data primarily for defined business purposes necessary for platform operation:

**a) Service Provision and Transaction Management**
Executing verification workflows, managing gate operations, generating Chain of Custody Records, distributing Delivery Notes, and enabling dispute resolution.
*Data Used: All account and Operational Data categories.*

**b) Security and Fraud Prevention**
Detecting falsified verification data, unauthorized access, tampered seals, fraudulent logistics activities, and suspicious weight deviations.
*Data Used: Identifiers, Chain of Custody Records, seal verification records.*

**c) Debugging and Technical Functionality**
Identifying and fixing errors, ensuring platform functionality, troubleshooting technical problems.
*Data Used: Internet/Network Activity, Identifiers.*

**d) Legal Compliance and Record-Keeping**
Retaining records required by applicable law, including food safety audit records (FSMA), weight and measure documentation, transport compliance records, and commercial transaction records (IRS).
*Data Used: All Operational Data categories.*

**e) Internal Research and Quality Improvement**
Analyzing platform usage (anonymized and aggregated) to improve verification workflows, CullyAI™ accuracy, and user experience.
*Data Used: Aggregated, anonymized usage data.*

### 13.2 No Commercial Use of Operational Data

Chain of Custody Records, weight data, cargo photographs, compliance documents, temperature records, and other Operational Data generated through verification workflows are **not used** for marketing, advertising, or commercial profiling purposes. They are used exclusively for the logistics verification service and legal compliance purposes described above.

---

## 14. Data Sharing with Third Parties

### 14.1 Principle: No Sharing for Advertising Purposes

Cultioo does not share your personal information or Operational Data with third parties for advertising or marketing purposes.

### 14.2 Sharing with Service Providers

Cultioo works with carefully selected service providers who process personal information on behalf of Cultioo. These service providers are contractually obligated to use the data exclusively for agreed-upon purposes and to implement appropriate security measures.

**a) Delvioo™ Drivers (Delivery Execution)**

- **Purpose:** Transmission of dispatch data required for delivery execution

- **Data Shared:** Seal number, departure temperature, gross weight, dispatch photos, batch data, compliance documents, Delivery Note, unloading instructions
- **Legal Basis:** Contract performance (necessary to complete the delivery)
- **Safeguards:** Delvioo™ drivers act as Service Providers of Cultioo. Data shared is limited to what is necessary for delivery execution.

**b) IT and Infrastructure Service Providers**

- **Purpose:** Cloud hosting, database administration, IT security, backups, analytics
- **Data Shared:** All categories of personal information and Operational Data stored in the App (depending on specific service)
- **Contractual Safeguards:** All IT service providers are contractually bound as Service Providers under CCPA/CPRA
- **Examples:** Cloud hosting providers (e.g., AWS, Google Cloud, Microsoft Azure), analytics tools (e.g., Firebase), email delivery services

### 14.3 Disclosure Due to Legal Obligations

Cultioo is obligated to disclose data upon lawful request from:

- Law enforcement agencies (court orders, subpoenas, statutory requirements)
- Government agencies (regulatory obligations)
- Food safety authorities (FSMA audit requirements)
- Tax and financial authorities (IRS retention requirements)

### 14.4 Aggregated and Anonymized Data

Cultioo may share aggregated, anonymized data for market research and industry analysis. Such data cannot be traced back to individual users or individual Orders.

---

## 15. Sale and Sharing of Personal Information

### 15.1 No Sale or Sharing

**Cultioo does NOT sell or share your personal information.**

Cultioo expressly confirms:

- Cultioo does not sell personal information (including sensitive personal information or Operational Data) as defined by CCPA/CPRA
- Cultioo does not share personal information for purposes of cross-context behavioral advertising

### 15.2 Future Changes

Should Cultioo introduce business practices in the future that could be considered "sale" or "sharing" under CCPA/CPRA:

- You will be clearly informed in advance
- A clear and conspicuous "Do Not Sell or Share My Personal Information" link will be provided in the App and on the website
- You will have the right to opt-out

### 15.3 Universal Opt-Out Mechanisms

Cultioo commits to respecting Universal Opt-Out Mechanisms such as Global Privacy Control (GPC) as a valid opt-out request for sale and sharing of personal information, in compliance with CCPA/CPRA.

---

## 16. Your Privacy Rights

Depending on your state of residence, you have specific statutory rights regarding your personal information. Cultioo grants these rights to all U.S. users regardless of state of residence.

### 16.1 Applicable Laws

| State | Law |
|---|---|
| California | CCPA / CPRA |

| State | Law |
|---|---|
| Virginia | VCDPA |
| Colorado | CPA |
| Connecticut | CTDPA |
| Utah | UCPA |

## 16.2 Right to Know / Right to Access

You have the right to request that Cultioo disclose:

- (a) Categories of personal information collected about you
- (b) Sources from which the personal information was collected
- (c) Business or commercial purposes for collection
- (d) Categories of third parties to whom information was disclosed
- (e) Specific personal information Cultioo has collected about you

**Time Period:** Preceding 12 months
**Frequency:** Up to twice per 12-month period, free of charge

## 16.3 Right to Delete

You have the right to request deletion of your personal information. Self-service account deletion is available via Account Settings.

**Exceptions:** Cultioo may deny deletion if data retention is necessary for:

- Completing active transactions
- Detecting security incidents or fraud
- Legal compliance (e.g., IRS 7-year retention for commercial transaction records)
- Asserting or defending legal claims

**Note:** Completed Chain of Custody Records are subject to mandatory legal retention and cannot be deleted upon request. They may be anonymized to the extent legally permissible.

## 16.4 Right to Correct

You have the right to request correction of inaccurate personal information. Account data (name, email, phone, profile picture) can be corrected directly via Account Settings.

**Note:** Completed Chain of Custody Records — including weight entries, photographs, timestamps, and digital signatures — cannot be modified after the check-out workflow is finalized. This immutability is a core legal and security protection feature.

### 16.5 Right to Limit Use of Sensitive Personal Information

Precise location data is stored exclusively locally on your device and is not transmitted to Cultioo servers. You can restrict or revoke location access at any time via your device settings.

A clearly visible link "Limit the Use of My Sensitive Personal Information" is available in App Settings.

### 16.6 Right to Opt-Out of Sale or Sharing

Cultioo currently does not sell or share personal information. If this changes in the future, a "Do Not Sell or Share My Personal Information" option will be provided.

### 16.7 Right to Data Portability

You have the right to receive your personal account information in a structured, machine-readable format (e.g., JSON, CSV). Contact privacy@cultioo.com to submit a portability request.

**Note:** Chain of Custody Records and Operational Data are proprietary logistics records that may not be subject to full portability rights under applicable law. Cultioo will evaluate each portability request on its merits.

### 16.8 Right to Non-Discrimination

Cultioo expressly commits: you will **NOT** be discriminated against for exercising any of your privacy rights. Specifically:

- ✅ You will not be denied service

- ✅ You will not be charged different prices or rates
- ✅ You will not receive a different level or quality of service
- ✅ You will not be treated differently in any way

### 16.9 Exercising Your Rights

Submit privacy rights requests through:

**a) Email:** privacy@cultioo.com
**b) Online Portal:** https://cultioo.com/en/en_cultioo_app_info#privacy
**c) Mail:** Cultioo Inc., Attn: Privacy Rights Department, 8 The Green, Ste A, Dover 19901, United States

**Verification Process:**
Cultioo must verify your identity before fulfilling your request:

1. Matching: We match your provided information against stored records
2. For sensitive requests (deletion, specific data access): additional verification may be required
3. Authorized Agents: You may authorize a representative with written authorization

**Response Time:**
Cultioo will process and respond to your request within 45 days of receipt. In complex cases, this period may be extended by an additional 45 days; you will be informed. Exercising your rights is free of charge.

---

## 17. Retention Period

Cultioo stores personal information and Operational Data only as long as necessary to fulfill processing purposes or comply with legal retention requirements.

### 17.1 Retention by Category

| Data Category | Retention Period | Justification |
|---|---|---|
| Account Data (name, email, username, phone) | Until account deletion by user | Necessary for service provision and account management |
| Group Membership Records | Until account deletion or group exit; group-level records for legal compliance | Group administration and access management |
| **Chain of Custody Records (all Operational Data)** | **Minimum 7 years from Order date** | IRS commercial record requirements; food safety audit records (FSMA); potential dispute resolution; transport compliance documentation |
| Batch Data (Production Date, BBD, Batch Number) | Minimum 7 years | Food traceability and product recall capability under FSMA |
| Compliance Documents (certifications, analysis reports) | Minimum 7 years | Regulatory compliance and audit requirements |
| Photographs (dispatch, arrival, damage) | Minimum 7 years | Evidence for cargo damage claims and dispute resolution |
| Digital Signatures | Minimum 7 years | Legal validity of delivery documentation |
| Usage and Technical Data (logs, IP addresses, device IDs) | 12–24 months | Security, troubleshooting, analysis |
| Location Data | Device only; no server storage | Complete user control |
| Department / Gate Configuration Data | Duration of Seller Group membership | Facility operations management |

| Data Category | Retention Period | Justification |
|---|---|---|
| Legally Required Retention | Varies by data type and applicable requirement | Compliance with legal, tax, or regulatory obligations |

### 17.2 Retention of Chain of Custody Records After Account Deletion

If you delete your account, completed Chain of Custody Records associated with your Operator actions are retained for the legally required minimum period. These records may be partially anonymized (your personal identifier removed) to the extent legally permissible, while the operational verification data (weights, photographs, timestamps, seal records) is maintained for legal compliance purposes.

### 17.3 Deletion After Purpose Fulfillment

After expiration of the retention period, your data will be securely deleted or anonymized unless legal retention obligations prevent deletion. Cultioo uses secure deletion methods that prevent data recovery.

---

## 18. Privacy of Minors

### 18.1 Age Requirement

The Cultioo Scanner App is intended exclusively for professional use by adults aged 18 and over. It is not designed for or directed at children under 13 years of age.

### 18.2 COPPA Compliance

Cultioo does not knowingly collect personal information from children under 13 years of age. If Cultioo obtains actual knowledge that it has collected personal information from a child under 13 without parental consent, it will:

- Immediately delete the child's information
- Notify the parent or guardian where possible

Parents or guardians who believe their child has provided information to Cultioo without consent should contact privacy@cultioo.com.

### 18.3 State-Specific Requirements (Ages 13–17)

California (AB 2273 — Age-Appropriate Design Code): Cultioo does not sell or share personal information of users known to be under 18 years of age. Default privacy settings for such users are set to the highest level.

---

## 19. Do Not Track and Tracking Technologies

### 19.1 Use of Tracking Technologies

The Cultioo Scanner App may use cookies and similar tracking technologies to ensure functionality and support performance analysis:

**a) Essential Tracking**

- Purpose: Session management, authentication, basic app functionality
- Legal Basis: Contract performance
- Duration: Until session end or up to 12 months

**b) Analytics Tracking**

- Purpose: Analyzing app usage to improve the operator experience and verification workflows
- Legal Basis: Legitimate interest
- Duration: Up to 12 months

**c) Functional Tracking**

- Purpose: Remembering user preferences and settings
- Legal Basis: Legitimate interest
- Duration: Up to 12 months

### 19.2 Do Not Track (DNT) Signals

Cultioo currently does not honor traditional Do Not Track (DNT) signals, as there is no uniform industry standard for responding to such signals in the context of native mobile applications.

### 19.3 Global Privacy Control (GPC)

In compliance with CCPA/CPRA, Cultioo commits to recognizing and honoring the Global Privacy Control (GPC) signal as a valid opt-out request for sale and sharing of personal information. When a GPC signal is detected, Cultioo treats it as a request to opt-out on that browser or device.

### 19.4 Third-Party Analytics

The Cultioo Scanner App may integrate third-party analytics services (e.g., Firebase for crash reporting and app analytics). These third parties operate under their own privacy policies. You can manage third-party tracking through device privacy settings.

### 19.5 Advertising

Cultioo does not currently display third-party advertising within the App. If third-party advertising is introduced in the future, you will be informed and appropriate opt-out mechanisms will be provided.

---

## 20. Changes to This Privacy Policy

Cultioo reserves the right to update this Privacy Policy from time to time to reflect changes in legislation, business processes, the App's features, or best practices in data privacy.

### 20.1 Notification of Changes

Material changes to this Privacy Policy will be communicated clearly and conspicuously through:

- In-app notification
- Email to your registered email address

- Prominent notice on our website

### 20.2 Effective Date

The current version of this Privacy Policy is effective as of January 1, 2026.

### 20.3 Review Recommendation

We recommend that you periodically review this Privacy Policy to stay informed about how we protect your information.

### 20.4 Continued Use

Your continued use of the Cultioo Scanner App after changes to this Privacy Policy constitutes acceptance of the updated terms.

---

## 21. Contact Information

### 21.1 General Inquiries

Cultioo Inc.
A Delaware Corporation
8 The Green, Ste A
Dover, DE 19901
United States of America

**Email:** support@cultioo.com

### 21.2 Privacy-Specific Inquiries

Privacy Department
**Email:** privacy@cultioo.com

### 21.3 Online Request Portal

https://cultioo.com/en/en_cultioo_app_info#privacy

### 21.4 Mailing Address for Privacy Rights Requests

Cultioo

Cultioo Inc.
Attn: Privacy Rights / Legal & Compliance Department
8 The Green, Ste A
Dover, DE 19901
United States of America

## 21.5 Response Time

- **Privacy rights requests:** 45 days (may be extended to 90 days for complex requests)
- **General inquiries:** 5–7 business days

---

*Last Updated: January 1, 2026*
**Version: 1.0**
*Governing Entity: Cultioo Inc., a Delaware Corporation*

---