



Cultioo App: United States Privacy Policy

Effective Date: January 1, 2026

Version: 1.0

Governing Entity: Cultioo Inc., a Delaware Corporation

Table of Contents

1. Scope and Application
 2. Company Information and Contact Details
 3. Definitions
 4. Registration and Consent
 5. Categories of Information Collected and Processing Purposes
 6. Data Storage and Data Security
 7. Payment Processing via Stripe Inc.
 8. Data Disclosure and Display
 9. Messenger Function and Communication Data
 10. Location Data (My Location)
 11. User Account and Personal Settings
 12. System and App Settings
 13. Data Usage: Business and Commercial Purposes
 14. Data Sharing with Third Parties
 15. Sale and Sharing of Personal Information
 16. Your Privacy Rights
 17. Retention Period
 18. Privacy of Minors
 19. Do Not Track and Tracking Technologies
 20. Changes to This Privacy Policy
 21. Contact Information
-



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 compliance with United States federal and state laws, including the regulations set forth by the Federal Trade Commission (FTC) and the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), as well as 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.

1. Scope and Application

1.1 Scope

This Privacy Policy applies to all users of the Cultioo mobile application and associated services within the United States of America. The Cultioo App functions as a marketplace platform facilitating transactions between buyers and sellers, including payment processing and logistics services.

1.2 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

1.3 Consent Through Use

By registering for or using the Cultioo 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
Dover, DE 19901
United States of America

Contact: privacy@cultioo.com

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, including but not limited to: names, email addresses, physical addresses, phone numbers, IP addresses, purchase history, device IDs, and usage data.



3.2 Sensitive Personal Information (SPI)

A subcategory of Personal Information requiring enhanced protection, including:

- Precise geolocation data (GPS location)
- Financial account information and credentials
- Contents of private communications (messenger messages)
- Other highly sensitive identifiers

3.3 Sale

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

3.4 Sharing

The sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information to a third party for cross-context behavioral advertising.

3.5 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 App requires registration. Certain personal information must be provided to utilize the app's features.

4.2 Explicit Consent

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

4.3 Right to Withdraw

You have the right to withdraw your consent at any time. The withdrawal does not affect the lawfulness of processing based on consent before its withdrawal.

4.4 Data Storage Upon Registration

When registering or modifying your data in the settings, your data is securely stored in the Cultioo database. Passwords are exclusively stored in hashed (encrypted) form in the database.

5. Categories of Information Collected and Processing Purposes

In accordance with CCPA/CPRA, Cultioo discloses the following categories of personal information collected in the last 12 months:

5.1 Detailed Overview of Data Categories

CCPA/CPR A Category	Examples of Data Collected	Source of Collection	Primary Purpose	Disclosed to Third Parties
A: Identifiers	Real name, username, email address, physical address, phone number, device ID, IP address	User registration, transactional input, device	Account management, security, order fulfillment, delivery	Yes (Service Providers/Contractors)
B: Personal Information	Name, address, phone number	User input, transactional input	Order fulfillment, emergency contact (Delvioso Driver)	Yes (Service Providers/Contractors)
D: Commercial Information	Purchase history, transaction records, payment method display (last four digits)	Transaction, user activity	Order processing, auditing, internal research	Yes (Service Providers/Contractors)
F: Internet or Other Similar Network Activity	Interaction with app, session duration, settings changes,	Device, app usage	Debugging, quality assurance, service improvement	Yes (Analytics Providers/Service Providers)



CCPA/CPR A Category	Examples of Data Collected	Source of Collection	Primary Purpose	Disclosed to Third Parties
K: Sensitive Personal Information (SPI)	device/OS details Precise geolocation (device location), financial account information (last 4 digits/payme nt type), contents of user messages	Device, transaction, user communicatio n	Service provision (communicatio n), transaction management, localization	Yes (Payment Processor, Communication Storage Service Provider)

5.2 Detailed Description of Data Categories

A. Identifiers

Data Collected:

- Full name / username
- Email address
- Physical address (delivery address)
- Phone number
- Device ID and unique identifiers
- IP address

Processing Purposes:

- Creation and management of your user account



- Authentication and access control
- Communication with you
- Order processing and delivery
- Fraud prevention and security

Sources: Direct input by user upon registration; automatic collection by device.

B. Commercial Information

Data Collected:

- Purchase history and order details
- Transaction records
- Display of last four digits of payment methods

Processing Purposes:

- Processing purchases and sales
- Customer service and support
- Dispute resolution
- Internal analysis to improve the platform

Sources: User activity within the app.

C. Internet and Network Activity

Data Collected:

- Interaction data with the app
- Pages and features visited
- Click and scroll behavior
- Session duration
- Device type, operating system, browser information
- App version

Processing Purposes:

- Ensuring app functionality



- Identifying and fixing errors (debugging)
- Analyzing usage to improve user experience
- Security monitoring

Sources: Automatic collection during app usage.

D. Sensitive Personal Information (SPI)

1. Precise Location Data

- Data Collected: GPS coordinates, precise geographic location
- Processing Purposes: Localized services (e.g., displaying nearby sellers)
- **IMPORTANT: Location data is stored exclusively locally on your device and is NOT transmitted to Cultioo servers or third parties.**
- Sources: User's device (with explicit device permission)

2. Financial Account Information

- Data Collected: Last four digits of credit cards or bank accounts
- Processing Purposes: Display and management of payment methods
- Special Note: Complete financial information is processed and stored exclusively by Stripe Inc.
- Sources: User input during payment transactions

3. Contents of Private Communications

- Data Collected: Message contents in the messenger between buyer and seller
 - Processing Purposes: Enabling communication for transaction processing
 - Sources: Direct input by user in the messenger
-

6. Data Storage and Data Security

6.1 Highest Priority

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.

6.2 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:** Even 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 your 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 data can only be changed by the authenticated user themselves via the secure app
- **Multi-Factor Authentication:** Critical operations (account deletion, password change) require password confirmation

d) Secure and Irreversible Deletion

- **Final Data Deletion:** When you delete your account, all associated data is finally and irrevocably removed from the database
- **No Recovery Possible:** Deleted data cannot be restored
- **Secure Deletion Protocols:** Use of secure deletion methods that prevent recovery

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

6.3 No Sharing with Third Parties for Marketing

Your data is fundamentally not shared with third parties for advertising or marketing purposes.

7. Payment Processing via Stripe Inc.

7.1 Exclusive Use of Stripe

Cultioo Inc. works with Stripe Inc., a leading PCI-DSS certified payment service provider. All payment processing is conducted exclusively through Stripe.

7.2 Security of Your Payment Data

- **Secure Storage:** All payment processing and bank data are securely stored and processed by Stripe Inc.
- **Cultioo Does Not Store Complete Financial Data:** Cultioo never receives or stores your complete credit card numbers or bank account information.
- **PCI-DSS Compliance:** Stripe meets the highest security standards of the payment card industry (PCI-DSS Level 1).

7.3 Display of Payment Information

For security and verification purposes, Cultioo displays exclusively the last four digits of your payment methods:

- In your personal account settings ("Payments" section)
- To the seller for transaction confirmation

7.4 Stripe as Independent Controller

- **Independent Responsibility:** Stripe Inc. acts as an independent data controller for the personal information it processes.
- **Separate Privacy Policy:** Users are subject to Stripe's separate privacy policy and terms of service.
- **Stripe Privacy Policy:** <https://stripe.com/privacy>

7.5 Disclaimer

Cultioo assumes no responsibility or liability for the security or use of data processed by Stripe. Use of Stripe occurs at the user's own risk as a third-party service.

8. Data Disclosure and Display

8.1 Disclosure to Sellers

To process and fulfill the order, the seller receives the following information:

- The delivery address selected at checkout
- Your name/username
- The last four digits of your payment method (for payment confirmation)

Purpose: Order processing, shipping preparation, transaction verification.

Legal Basis: Contract performance (necessary to complete the transaction).

8.2 Disclosure to Delvoo Driver (Delivery Service)

The Delvoo driver receives the following data to successfully deliver your order:

Data	Purpose
Delivery address (Delivery Location)	Creation of an optimized delivery route
Name/Username	For correct order assignment
Phone number	Exclusively for emergency contact (e.g., difficulty finding the delivery address)
Email address	Exclusively for emergency contact

Purpose: Creation of an optimized delivery route, successful delivery of the order, emergency communication in case of delivery difficulties.

Legal Basis: Contract performance (necessary to complete delivery).

Contractual Safeguards: Delvoo acts as a Service Provider of Cultioo and is contractually obligated to use the data exclusively for delivery purposes and implement appropriate security measures.

9. Messenger Function and Communication Data

9.1 Purpose of the Messenger Function

Cultioo offers an integrated messenger function that enables direct communication between buyers and sellers to clarify transaction details and facilitate the purchase process.

9.2 Storage of Message History

- The entire message history between sender and recipient is stored in the Cultioo database.
- Storage occurs to make communication permanently available to both parties.
- Messages are not forwarded to third parties or made public.

9.3 Access Restrictions

- **Exclusive Access:** Only sender and recipient have access to the respective message history in the Cultioo App.
- **No Third-Party Sharing:** Message contents are not shared with third parties.
- **Limited Cultioo Access:** Cultioo employees generally have no access to private messages, except:
 - In case of reasonable suspicion of fraud, criminal activity, or violation of terms of service
 - To comply with legal obligations (e.g., court orders)
 - To resolve technical issues (only with explicit consent)

9.4 Pinned Messages

Messages you mark as "pinned" or "important" are stored locally on your device and not additionally stored on Cultioo servers.



9.5 Sensitive Data (SPI)

Message contents are classified as Sensitive Personal Information (SPI) under CCPA/CPRA, as they contain private communications not directed to Cultioo as a business.

9.6 Deletion of Messages

You can request deletion of your entire message history at any time (see Section 16.3).

10. Location Data (My Location)

10.1 Use of Location Data

The Cultioo App can access your device's location function to offer you localized services, such as:

- Displaying sellers in your geographic proximity
- Regional filtering of products and offers
- Optimizing search results based on your location

10.2 Privacy by Design: Local Storage – NO Server Transmission

IMPORTANT PRIVACY NOTICE: Your location is stored exclusively locally on your device.

- 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 Control Over Location Access

You have complete control over location access at all times:

- **Device Settings:** You can control the Cultioo App's access to your location data via your mobile device settings (iOS or Android).
- **Options:**
 - Completely disable location access
 - Allow location access only while using the app
 - Disable precise location (approximate location only)

Note: Disabling location services may limit the functionality of certain features (e.g., local search results).

10.4 Classification as Sensitive Data

Precise location data is classified as Sensitive Personal Information (SPI) under CCPA/CPRA and receives enhanced protection.

10.5 Legal Basis

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 (My Account)

11.1 Payment Information (Payments)

In the "Payments" section of your account, your personal bank accounts and credit cards are managed:

Security:

- All payment accounts are exclusively secured and managed by Stripe Inc.
- Cultioo displays only the last four digits of your payment methods.
- Only you as the user have access to your stored payment methods in the Cultioo App.

Management:

- You can add, modify, or remove payment methods.
- All changes are securely processed through Stripe.

11.2 Modification of Personal Data

You have the ability to modify your personal data at any time:

Security Measure: Modifications can only be made by you via the Cultioo App. Personal data can only be changed through the Cultioo App. This prevents unauthorized modifications by third parties.

Modifiable Data:

- Name/username
- Email address
- Phone number
- Delivery address(es)
- Profile picture

11.3 Account Deletion (Right to Deletion)

Security Procedure: If you wish to delete your account, this is only possible by entering your password. This security measure protects against unauthorized or accidental account deletion.

Deletion Process:

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

Irrevocable Deletion:

- After confirmation, all data associated with your account is finally and irrevocably removed from the database.
- Data recovery is not possible.
- This process ensures complete fulfillment of your right to deletion.

Exceptions: Certain data may be retained for a limited period due to legal retention obligations (e.g., tax requirements).

11.4 Password Change

Security Procedure: When creating a new password, the old password must be entered for confirmation. This prevents unauthorized password changes if someone has access to your device.

Recommendations:

- Use a strong, unique password
- Change your password regularly
- Never share your password with third parties

12. System and App Settings

12.1 Local Processing

All changes you make in the Cultioo App settings are initially processed locally on your device.

12.2 Synchronization

After local processing, settings are securely synchronized with Cultioo servers to:

- Ensure consistency across multiple devices
- Restore your settings upon reinstallation
- Optimize app functionality

12.3 Data Security

Transmission of settings data occurs over encrypted connections (HTTPS/TLS).

13. Data Usage: Business and Commercial Purposes

Cultioo uses the collected personal information and sensitive personal information primarily for defined business purposes necessary for platform operation, and secondarily for commercial purposes that enhance user experience.

13.1 Business Purposes

According to CCPA/CPRA, business purposes are processing activities required for service provision and generally not subject to opt-out rights:



a) Service Provision and Transaction Management

- Processing orders and purchases
- Managing user accounts
- Enabling communication between buyers and sellers
- Coordinating delivery through Delvoo

Data Used: Identifiers, Personal Records Information, Commercial Information

b) Security and Fraud Prevention

- Detecting, preventing, and prosecuting security incidents
- Identifying fraudulent activities
- Protecting against illegal actions
- Performing internal audits
- Verifying transactions

Data Used: Identifiers, Internet/Network Activity, Commercial Information

c) Debugging and Technical Functionality

- Identifying and fixing errors
- Ensuring platform functionality
- Troubleshooting technical problems

Data Used: Internet/Network Activity, Identifiers

d) Customer Account Management and Rights Fulfillment

- Enabling exercise of consumer rights (access, correction, deletion)
- Updating and correcting data
- Secure account deletion

Data Used: All categories of personal information



e) Internal Research and Quality Improvement

- Analyzing platform usage (Internet/Network Activity)
- Improving user experience
- Developing new features
- Optimizing existing functions

Data Used: Internet/Network Activity, aggregated usage data (anonymized)

13.2 Commercial Purposes

Commercial purposes serve business development and are conducted in a manner that does not constitute "sale" or "sharing" of data under CCPA/CPRA:

a) Marketing and Communication

- Sending information about new products or services
- Notifications about special offers and promotions (only with your consent)
- Personalized in-app content

Data Used: Identifiers (email, name), Commercial Information

Opt-Out: You can unsubscribe from marketing communications at any time (see Section 16.7).

b) Personalization and Recommendations

- Displaying personalized product recommendations based on your purchase history
- Adapting the app interface to your preferences

Data Used: Commercial Information, Internet/Network Activity

13.3 Transparency for Sensitive Data (SPI)

Precise Location Data: The decision to store location data exclusively locally on the device and not transmit it to servers inherently reduces Cultioo's liability regarding sensitive data processing and complies with data minimization principles.

Financial Data: Cultioo limits its storage of sensitive financial data by delegating complete account security and processing to Stripe.

Message Contents: Messenger histories are securely stored and accessible exclusively to sender and recipient.

14. Data Sharing with Third Parties

14.1 Principle: No Sharing for Advertising Purposes

Cultioo fundamentally does not share your personal information 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 implement appropriate security measures.

a) Delvoo (Delivery Service / Logistics Partner)

Purpose: Delivery of orders to buyers

Shared Data:

- Delivery address (Delivery Location)



- Name/username
- Phone number (emergency contact only)
- Email address (emergency contact only)

Legal Basis: Business purpose (service provision on behalf of Cultioo)

Contractual Safeguards: Delvoo acts as a Service Provider under CCPA/CPRA with a written contract obligating Delvoo to:

- Use data exclusively for delivery purposes
- Not use data for own commercial purposes
- Not resell or share data
- Implement appropriate security measures
- Treat data confidentially

Compliance Rationale: The sharing with Delvoo is necessary and proportional to the service provided and is not classified as "sale" or "sharing" under CCPA/CPRA.

b) Stripe Inc. (Payment Processor)

Purpose: Secure processing of all payment transactions

Shared Data:

- Payment data (complete credit card or bank account information)
- Transaction details
- Name and email address

Special Note: Stripe acts as an independent controller, not as a Service Provider of Cultioo.

Legal Basis: Contract performance (necessary for payment processing)

Disclaimer: Cultioo assumes no responsibility for data processing by Stripe. Users are subject to Stripe's separate privacy policy:
<https://stripe.com/privacy>

c) IT and Infrastructure Service Providers

Purpose:

- Cloud hosting and server management
- Database administration
- IT security and monitoring
- Backup and disaster recovery
- Analytics services

Shared Data: All categories of personal information stored in the app (depending on service provider)

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., Google Analytics, Mixpanel)
- Email delivery services
- Customer support platforms

14.3 Disclosure Due to Legal Obligations

Cultioo is obligated to disclose personal information upon lawful request to the following entities:

- **Law Enforcement Agencies:** In response to court orders, subpoenas, or statutory requirements
- **Government Agencies:** To fulfill regulatory obligations
- **Tax and Financial Authorities:** To comply with tax-related retention requirements

Legal Basis: Compliance with legal obligations

Transparency Commitment: Cultioo will notify users of such requests where legally permissible.

14.4 Disclosure in Corporate Transactions

In the event of a merger, acquisition, restructuring, or sale of assets, personal information may be transferred as part of the transaction to the successor entity.

- **Obligation:** The successor will be obligated to continue to comply with this Privacy Policy.
- **Notification:** Users will be informed in advance of such a transaction.

14.5 Aggregated and Anonymized Data

Cultioo may share aggregated, anonymized, or pseudonymized data that cannot be traced back to individual users for the following purposes:

- Market research
- Industry analysis
- Public reports
- Academic research

Important: This data is not considered personal information and is not subject to the restrictions of this Privacy Policy.

15. Sale and Sharing of Personal Information

15.1 No Sale or Sharing (CCPA/CPRA Statement)

Cultioo does NOT sell or share your personal information.

Based on current business practices, Cultioo expressly confirms:

- Cultioo does not sell personal information (including sensitive personal information) as defined by CCPA/CPRA.



- Cultioo does not share personal information for purposes of cross-context behavioral advertising.

15.2 Definitions

"Sale" means under CCPA/CPRA: The selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration.

"Sharing" means under CCPA/CPRA: The sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration.

15.3 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 on the website and in the app.
- You will have the right to opt-out of the sale or sharing.

16. Your Privacy Rights

Depending on your state of residence, consumers in the United States have specific statutory rights regarding their personal information. Cultioo is committed to facilitating the exercise of these rights through transparent and accessible mechanisms.

16.1 Applicable Laws

The following rights apply particularly to residents of:

- **California:** CCPA/CPRA
- **Virginia:** VCDPA
- **Colorado:** CPA
- **Connecticut:** CTDPA
- **Utah:** UCPA

Cultioo grants these rights to all U.S. users, regardless of state of residence, to ensure a uniformly high privacy standard.

16.2 Right to Know / Right to Access

You have the right to request that Cultioo disclose:

- Which categories of personal information were collected about you
- From which sources the personal information originated
- For which business or commercial purposes the data was collected or disclosed
- To which categories of third parties the personal information was disclosed
- The specific personal information that Cultioo has collected about you

Time Period: The disclosure relates to the preceding 12 months.

Frequency: You can exercise this right up to twice within 12 months free of charge.

16.3 Right to Delete

You have the right to request deletion of your personal information that Cultioo has collected about you.

Self-Service Deletion:

1. Navigate to account settings
2. Select "Delete Account"



3. Confirm by entering your password

After confirmation, all data associated with your account is finally and irrevocably removed from the database. Data recovery is not possible.

Exceptions to Right to Delete: Cultioo may deny deletion if data retention is necessary for:

- Completing the transaction for which the data was collected
- Detecting security incidents, protecting against fraudulent or illegal activities
- Debugging to identify and fix errors
- Exercising free speech rights
- Complying with legal obligations (e.g., tax retention periods)
- Internal uses reasonably aligned with consumer expectations
- Asserting or defending legal claims

16.4 Right to Correct

You have the right to request correction of inaccurate personal information that Cultioo has stored about you.

Self-Service Correction:

- Navigate to account settings ("My Account")
- Modify the desired information
- Save the changes

Correctable Data: Name/username, Email address, Phone number, Delivery address(es), Profile picture.

If you need assistance with corrections, contact us using the contact details in Section 21.

16.5 Right to Limit Use of Sensitive Personal Information

You have the right to direct Cultioo to limit the use of your sensitive personal information (SPI) to what is necessary to provide the requested services.

Cultioo's SPI Practices:

a) Precise Location Data:

- Location data is stored exclusively locally on your device.
- It is not transmitted to Cultioo servers.
- Control: You can restrict or revoke location access at any time via your device settings.

b) Financial Account Information:

- Cultioo stores only the last four digits of your payment methods.
- Complete financial data is managed exclusively by Stripe.

c) Message Contents:

- Stored exclusively to enable communication between buyer and seller.
- Access is restricted to sender and recipient.

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

You have the right to opt-out of the sale or sharing of your personal information.

Current Status: Cultioo currently does not sell or share personal information under CCPA/CPRA. Therefore, an opt-out is not currently required.

Future Commitment: Should Cultioo introduce practices in the future that constitute sale or sharing:

- A clearly visible link "Do Not Sell or Share My Personal Information" will be provided.
- You can opt-out at any time without it affecting service quality.

Universal Opt-Out Mechanisms (UOOMs): Cultioo commits to respecting Universal Opt-Out Mechanisms such as Global Privacy Control (GPC).

16.7 Right to Data Portability

You have the right to receive the personal information concerning you in a structured, commonly used, and machine-readable format.

Contact us using the contact details in Section 21 to request a copy of your data in a portable format. Data will be provided in a common format (e.g., JSON, CSV).

16.8 Right to Opt-Out of Automated Decision-Making

Cultioo currently does not use fully automated decision-making systems that have legal or similarly significant effects on users (e.g., fully automated credit decisions).

If such systems are implemented in the future, you will be informed and have the right to object to such processing.

16.9 Right to Non-Discrimination

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

This specifically means:

- You will not be denied service



- You will not be charged different prices or rates
- You will not be provided a different level or quality of goods or services
- You will not be treated differently

Exception: Cultioo may offer you a different price, rate, or quality if that difference is reasonably related to the value your data provides to Cultioo.

16.10 Exercising Your Rights

Submitting a Request: You can exercise your privacy rights through the following channels:

- **Online Request Portal:** cultioo.com
- **Email:** privacy@cultioo.com
- **Mailing Address:** Cultioo Inc., Attn: Privacy Rights Department, 8 The Green, Ste A, Dover 19901, United States

Verification Process: To protect the security of your data, Cultioo must verify your identity before fulfilling your request:

1. **Matching:** We match the information you provide with the data stored in our records.
2. **Additional Verification:** For sensitive requests (e.g., deletion, access to specific data), additional verification steps may be required.
3. **Authorized Agent:** You can authorize a representative to submit a request on your behalf (written authorization required).

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.

Free of Charge: Exercising your privacy rights is free of charge. Cultioo does not charge fees for processing your requests (at reasonable frequency).

17. Retention Period

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

17.1 Retention Period by Category

Data Category	Retention Period	Justification
Account Data (name, email, username, address, phone)	Until account deletion by user	Necessary for service provision and account management
Transaction Data (purchase history, order details)	7 years from transaction date	IRS requirements for tax records; potential disputes
Message History (messenger)	Until account deletion or upon specific request	Enabling continuous communication between transaction parties
Payment Data (last 4 digits)	Until account deletion or removal by user	Display and management of payment methods
Payment Data (complete, at Stripe)	According to Stripe policies	Outside Cultioo's control; see Stripe Privacy Policy
Usage and Technical Data (logs, IP addresses, device IDs)	12-24 months	Security, troubleshooting, analysis
Location Data (local)	Device only; no server storage	Localized services; complete user control
Legally Required Retention	Varies by data type and requirement	Compliance with legal, tax, or regulatory obligations

17.2 Deletion After Purpose Fulfillment

After expiration of the retention period or upon your request (right to delete), your data will be securely deleted or anonymized, unless legal retention obligations prevent deletion.

17.3 Secure Deletion Protocols

Cultioo uses secure deletion methods that prevent data recovery and ensure protection of your privacy.

18. Privacy of Minors

18.1 Children's Online Privacy Protection Act (COPPA)

The Cultioo App is directed to a general adult audience and is not specifically designed or intended for children under 13 years of age.

Commitment: Cultioo does not knowingly collect personal information from children under 13 years of age without verifiable parental consent.

18.2 Actions Upon Knowledge

If Cultioo obtains actual knowledge that it has collected personal information from a child under 13 without parental consent, we will:

- Immediately notify the parent or guardian
- Seek verifiable parental consent
- Promptly delete the child's information if consent is not obtained within a reasonable timeframe



18.3 Parental Notice

Parents or guardians are encouraged to contact us if they believe their child has provided personal information to Cultioo without their consent.

18.4 Age Verification

Users are required to affirm they meet the minimum age requirements to use the service upon registration.

18.5 State-Specific Requirements for Minors (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 minors are set to the highest level.

Parental Rights: Parents or legal guardians of minors may exercise privacy rights on behalf of their children by contacting us with appropriate verification.

19. Do Not Track and Tracking Technologies

19.1 Use of Cookies and Tracking Technologies

The Cultioo App may use cookies and similar tracking technologies to ensure functionality and improve user experience.

19.2 Types of Tracking Technologies

Type	Purpose	Legal Basis	Duration
Essential Cookies	Enable basic functions (e.g., login, shopping cart)	Contract performance (necessary for service provision)	Until session end or up to 12 months
Analytics Cookies	Analyze usage to improve the app	Consent or legitimate interest	Up to 12 months
Functional Cookies	Remember user preferences and settings	Consent or legitimate interest	Up to 12 months

19.3 Cookie Control

You can adjust your cookie settings at any time via app settings or your device. Disabling certain cookies may limit app functionality.

19.4 Do Not Track (DNT) Signals

Current Position: Cultioo currently does not honor traditional Do Not Track (DNT) browser signals, as there is no uniform industry standard for responding to such signals.

Transparency: We disclose that third-party tracking may occur through integrated service providers (e.g., analytics platforms).

19.5 Global Privacy Control (GPC)

Commitment to Honor GPC: In compliance with CCPA/CPRA and other state laws, Cultioo commits to recognizing and honoring the Global Privacy Control (GPC) signal as a valid opt-out request for:

- Sale of personal information
- Sharing for cross-context behavioral advertising

Implementation: When we detect a GPC signal from your browser or device, we will treat it as a request to opt-out on that browser/device.

19.6 Third-Party Trackers

The Cultioo App may integrate third-party services that use their own tracking technologies:

Examples:

- Google Analytics (analytics)
- Firebase (crash reporting, analytics)
- Social media plugins (if applicable)

Control: These third parties have their own privacy policies. You can manage third-party tracking through device privacy settings, browser settings, and third-party opt-out tools (e.g., Network Advertising Initiative opt-out page).

19.7 Advertising and Marketing

Current Status: Cultioo does not currently display third-party advertising within the app.

Future Disclosure: If third-party advertising is introduced, 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, 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 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

You can also submit your requests through our online portal:

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

21.4 Mailing Address

Cultioo Inc.

Attn: Privacy Rights / Legal & Compliance Department

privacy@cultioo.com

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

© 2026 Cultioo Inc. All Rights Reserved.