CONSUMER DATA RIGHTS AND CCPA/GDPR COMPLIANCE

JANUARY 2026

POLICY NUMBER: TMG-SEC-018
APPROVAL AUTHORITY: BOARD OF DIRECTORS

THE MAZI GROUP

1. PURPOSE

This policy establishes The Mazi Group's procedures for honoring consumer data rights under the California Consumer Privacy Act (CCPA), California Privacy Rights Act (CPRA), General Data Protection Regulation (GDPR), and other applicable privacy laws. We are committed to empowering consumers with control over their personal information across all our brands: Mazi Beauty, Glam Switch, On The Go Mists, and Upvendo.

2. SCOPE

This policy applies to:

- All consumer personal information collected by The Mazi Group
- All brands and customer-facing operations
- All employees who handle consumer data requests
- Consumers in jurisdictions with data rights laws
- All channels: websites, apps, retail, customer service

3. APPLICABLE REGULATIONS

3.1 CCPA/CPRA (California)

Applies to California residents when The Mazi Group:

- Has annual gross revenue over $25 million
- Buys, sells, or shares personal information of 100,000+ consumers
- Derives 50%+ of revenue from selling/sharing personal information

3.2 GDPR (European Union)

Applies when:

- Processing data of EU residents
- Offering goods or services to EU residents
- Monitoring behavior of EU residents

3.3 Other State Laws

- Virginia Consumer Data Protection Act (VCDPA)
- Colorado Privacy Act (CPA)

- Connecticut Data Privacy Act (CTDPA)
- Other state laws as enacted

3.4 Canadian Laws

- PIPEDA (federal)
- Quebec Law 25
- Provincial privacy laws

4. CONSUMER RIGHTS

4.1 Right to Know / Access

Consumers can request:

- Categories of personal information collected
- Specific pieces of personal information held
- Sources of personal information
- Purposes for collection and use
- Categories of third parties with whom data is shared
- Categories of information sold or shared (if applicable)

4.2 Right to Delete / Erasure

- Request deletion of personal information
- Subject to legal exceptions (legal obligations, ongoing transactions, security)
- Extends to service providers upon instruction

4.3 Right to Correct

- Request correction of inaccurate personal information
- Provide supporting documentation if needed

4.4 Right to Opt-Out of Sale/Sharing

- Opt out of sale of personal information
- Opt out of sharing for cross-context behavioral advertising
- "Do Not Sell or Share My Personal Information" link required

4.5 Right to Limit Use of Sensitive Personal Information

- Limit use of sensitive personal information to necessary purposes
- "Limit the Use of My Sensitive Personal Information" link required

4.6 Right to Data Portability

- Receive personal information in portable, machine-readable format
- Transfer data to another service provider

4.7 Right to Non-Discrimination

- No discrimination for exercising privacy rights
- Equal service and pricing
- Financial incentives permitted with proper disclosure

5. REQUEST SUBMISSION METHODS

5.1 Available Channels

- Online privacy request form on each brand website
- Email to privacy@mazigroup.us
- Toll-free phone number
- In-app request submission (where applicable)

5.2 Authorized Agents

- Consumers may designate authorized agents
- Written authorization required
- Verify agent authority before processing
- May require consumer verification even with agent

6. IDENTITY VERIFICATION

6.1 Verification Requirements

- Verify identity before fulfilling requests
- Match request information to existing records

- Use reasonable verification methods
- Higher verification for sensitive requests (deletion, specific pieces)

6.2 Verification Methods

- Account login verification
- Email verification
- Knowledge-based questions
- Government ID verification (for high-risk requests)
- Third-party verification services

6.3 Verification Standards

Request Type	Verification Level	Method
Categories of data	Reasonable	2 data points match
Specific pieces	Reasonably high	3 data points match
Deletion	Reasonably high	3 data points match
Correction	Reasonable	2 data points match

7. REQUEST PROCESSING

7.1 Response Timeframes

Regulation	Initial Response	Full Response	Extension
CCPA/CPRA	10 business days	45 calendar days	+45 days with notice
GDPR	Without undue delay	1 month	+2 months with notice
VCDPA/CPA	N/A	45 days	+45 days with notice

7.2 Processing Steps

1. Receive and log request
2. Acknowledge receipt within required timeframe

3. Verify consumer identity
4. Search for and compile personal information
5. Review for exceptions
6. Prepare response
7. Deliver response securely
8. Document completion

7.3 Response Delivery

- Deliver through secure channel
- Use consumer's preferred method when possible
- Portable format for data portability requests
- Do not require account creation to receive response

8. EXCEPTIONS AND LIMITATIONS

8.1 CCPA/CPRA Exceptions

- Complete a transaction or provide requested service
- Security and fraud prevention
- Debug and repair errors
- Exercise free speech rights
- Comply with legal obligations
- Internal uses aligned with consumer expectations
- Scientific, historical, or statistical research

8.2 GDPR Exceptions

- Legal claims establishment, exercise, or defense
- Compliance with legal obligations
- Public interest tasks
- Archiving in public interest
- Scientific or historical research

8.3 Documenting Exceptions

- Document basis for any exception applied
- Inform consumer of exception and reason
- Apply exceptions narrowly

9. SERVICE PROVIDER REQUIREMENTS

9.1 Forwarding Requests

- Forward deletion requests to service providers
- Instruct service providers to delete
- Confirm service provider compliance

9.2 Contractual Requirements

- Contracts require service providers to honor requests
- Prohibit retention beyond business purpose
- Require notification of inability to comply

10. OPT-OUT MECHANISMS

10.1 Do Not Sell/Share

- Clear and conspicuous link on homepage
- Easy-to-use opt-out mechanism
- No account required to opt out
- Honor opt-out for at least 12 months

10.2 Global Privacy Control

- Honor Global Privacy Control (GPC) signals
- Treat GPC as valid opt-out request
- Apply to browser/device making request

10.3 Opt-Out Preference Signals

- Recognize and honor opt-out preference signals

- Process signals as valid opt-out requests
- Document signal processing

11. SENSITIVE PERSONAL INFORMATION

11.1 Categories (CPRA)

- Social Security, driver's license, passport numbers
- Account credentials (username + password)
- Precise geolocation
- Racial or ethnic origin
- Religious or philosophical beliefs
- Union membership
- Genetic data
- Biometric data (including facial images for Glam Switch)
- Health information
- Sex life or sexual orientation

11.2 Use Limitations

- Use only for purposes disclosed at collection
- Honor requests to limit use
- Provide "Limit Use" link on website

12. SPECIAL CONSIDERATIONS BY BRAND

12.1 Glam Switch

- Facial images are biometric/sensitive data
- Explicit consent required for collection
- Clear disclosure of AI analysis purposes
- Easy deletion of facial data
- No sale or sharing of biometric data

12.2 Upvendo

- B2B and B2C data considerations
- Restaurant customer vs. end consumer data
- Clear data controller/processor relationships
- Support restaurant clients in honoring requests

13. RECORD KEEPING

- Log all consumer requests received
- Document verification steps
- Record response and completion date
- Maintain records for 24 months (CCPA requirement)
- Track metrics for annual reporting

14. TRAINING

- Train customer service on handling requests
- Train privacy team on processing procedures
- Annual refresher training
- Update training for regulatory changes

15. METRICS AND REPORTING

15.1 CCPA Metrics (if required)

- Number of requests received by type
- Number of requests complied with (full/partial)
- Number of requests denied
- Median response time

15.2 Internal Reporting

- Monthly request volume reports
- Response time tracking
- Exception usage analysis

- Process improvement recommendations

16. RELATED POLICIES

This policy should be read in conjunction with:

- TMG-SEC-016: Data Privacy and Protection Policy
- TMG-SEC-019: Third-Party Data Sharing and Processing Agreements
- TMG-SEC-020: Incident Response and Data Breach Notification
- TMG-SEC-038: AI Ethics and Responsible AI Use Policy

17. POLICY REVIEW

This policy shall be:

- Reviewed annually by the DPO and Legal
- Updated for regulatory changes
- Approved by executive leadership
- Communicated to relevant teams

18. DEFINITIONS

- **Consumer:** Natural person who is a resident of a jurisdiction with privacy rights.
- **Personal Information:** Information that identifies, relates to, or could be linked to a consumer.
- **Sale:** Disclosing personal information for monetary or valuable consideration.
- **Sharing:** Disclosing for cross-context behavioral advertising (CPRA).
- **Service Provider:** Entity processing data on behalf of a business under contract.

For questions about this policy, contact:
Privacy Department
privacy@mazigroup.us