DATA PRIVACY AND PROTECTION POLICY

JANUARY 2026

POLICY NUMBER: TMG-SEC-016
APPROVAL AUTHORITY: BOARD OF DIRECTORS

THE MAZI GROUP

1. PURPOSE

This Data Privacy and Protection Policy establishes The Mazi Group's commitment to protecting the privacy of personal data collected from customers, employees, partners, and other individuals. We recognize that privacy is a fundamental right and that responsible data handling is essential to maintaining trust with our stakeholders across all brands: Mazi Beauty, Glam Switch, On The Go Mists, and Upvendo.

2. SCOPE

This policy applies to:

- All personal data processed by The Mazi Group and its subsidiaries
- All brands and business units
- All employees, contractors, and third parties who handle personal data
- All processing activities regardless of location
- All data subjects: customers, employees, partners, and website visitors

3. REGULATORY FRAMEWORK

The Mazi Group complies with applicable privacy laws including:

3.1 United States

- California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA)
- Virginia Consumer Data Protection Act (VCDPA)
- Colorado Privacy Act (CPA)
- Other state privacy laws as enacted
- Children's Online Privacy Protection Act (COPPA)
- Health Insurance Portability and Accountability Act (HIPAA) where applicable

3.2 European Union

- General Data Protection Regulation (GDPR)
- ePrivacy Directive
- Member state implementing laws

3.3 Canada

- Personal Information Protection and Electronic Documents Act (PIPEDA)
- Provincial privacy laws (Quebec Law 25, etc.)

3.4 Latin America

- Brazil: Lei Geral de Proteção de Dados (LGPD)
- Mexico: Ley Federal de Protección de Datos Personales
- Other applicable national laws

4. DATA PRIVACY PRINCIPLES

The Mazi Group adheres to the following principles:

4.1 Lawfulness, Fairness, and Transparency

- Process personal data lawfully and fairly
- Be transparent about how we use personal data
- Provide clear privacy notices

4.2 Purpose Limitation

- Collect data for specified, explicit, and legitimate purposes
- Do not process data in ways incompatible with original purposes
- Obtain consent for new purposes when required

4.3 Data Minimization

- Collect only data that is necessary
- Avoid excessive data collection
- Regularly review data holdings

4.4 Accuracy

- Keep personal data accurate and up to date
- Provide mechanisms for individuals to update their data
- Correct inaccurate data promptly

4.5 Storage Limitation

- Retain data only as long as necessary
- Define retention periods for different data categories
- Securely delete data when no longer needed

4.6 Security

- Implement appropriate technical and organizational measures
- Protect against unauthorized access, loss, or destruction
- Regularly assess and improve security measures

4.7 Accountability

- Demonstrate compliance with privacy requirements
- Maintain documentation of processing activities
- Conduct privacy impact assessments

5. TYPES OF PERSONAL DATA

5.1 Customer Data

- Contact information (name, email, phone, address)
- Account credentials
- Purchase history and preferences
- Payment information
- Communication preferences
- Device and usage data

5.2 Brand-Specific Data

Mazi Beauty / On The Go Mists

- Skin type and beauty preferences
- Product reviews and feedback
- Loyalty program data

Glam Switch

- Facial images for AI analysis (with explicit consent)
- Skin analysis results
- Product recommendations history
- Device usage data

Upvendo

- Restaurant business information
- Transaction data
- Employee data (for restaurant clients)
- End consumer order data

5.3 Employee Data

- Employment records
- Payroll and benefits information
- Performance data
- Background check information

5.4 Sensitive Personal Data

Special categories requiring enhanced protection:

- Biometric data (facial images for Glam Switch)
- Health information
- Racial or ethnic origin
- Religious or philosophical beliefs

6. LEGAL BASES FOR PROCESSING

Legal Basis	When Used
Consent	Marketing communications, facial analysis, cookies
Contract	Order fulfillment, account management, service delivery
Legal Obligation	Tax records, regulatory reporting, legal holds

Legitimate Interest	Fraud prevention, security, product improvement
Vital Interest	Emergency situations affecting health or safety

7. INDIVIDUAL RIGHTS

We respect and facilitate the following rights:

7.1 Right to Access

- Individuals can request copies of their personal data
- Respond within legally required timeframes
- Provide data in portable format when requested

7.2 Right to Rectification

- Correct inaccurate personal data
- Complete incomplete data

7.3 Right to Erasure

- Delete personal data when legally required
- Honor "right to be forgotten" requests
- Document exceptions (legal holds, regulatory requirements)

7.4 Right to Restrict Processing

- Limit processing in certain circumstances
- Mark data as restricted

7.5 Right to Data Portability

- Provide data in machine-readable format
- Transfer data to another controller when requested

7.6 Right to Object

- Honor objections to direct marketing
- Consider objections to legitimate interest processing

7.7 Rights Related to Automated Decision-Making

- Inform individuals about automated decisions
- Provide human review when requested
- Explain logic involved in automated processing

8. CONSENT MANAGEMENT

- Obtain clear, affirmative consent when required
- Document consent with timestamp and scope
- Make withdrawal of consent easy
- Do not bundle consent with other terms
- Obtain parental consent for children under applicable age

9. PRIVACY NOTICES

- Provide clear, accessible privacy notices
- Include all required disclosures
- Update notices when practices change
- Maintain notices for each brand and service
- Provide notices in appropriate languages

10. DATA SECURITY

- Implement security measures per TMG-SEC-017
- Encrypt personal data in transit and at rest
- Control access based on need-to-know
- Monitor for unauthorized access
- Conduct regular security assessments

11. DATA RETENTION

- Retain data only as long as necessary
- Follow retention schedules per TMG-SEC-005
- Securely delete or anonymize data after retention period

- Document retention decisions

12. THIRD-PARTY DATA SHARING

- Share data only with authorized third parties
- Execute data processing agreements
- Verify third-party privacy and security practices
- Disclose sharing in privacy notices
- See TMG-SEC-019 for detailed requirements

13. INTERNATIONAL DATA TRANSFERS

- Use approved transfer mechanisms (SCCs, adequacy decisions)
- Conduct transfer impact assessments
- Implement supplementary measures when needed
- Document transfer justifications

14. PRIVACY BY DESIGN

- Incorporate privacy into product and system design
- Conduct privacy impact assessments for new processing
- Minimize data collection by default
- Build in privacy controls

15. DATA BREACH RESPONSE

- Report suspected breaches immediately
- Follow incident response procedures (TMG-SEC-020)
- Notify regulators within required timeframes
- Notify affected individuals when required
- Document all breaches and responses

16. ROLES AND RESPONSIBILITIES

16.1 Data Protection Officer (DPO)

- Oversee privacy compliance program
- Advise on privacy matters
- Serve as contact for regulators and data subjects
- Monitor compliance and training

16.2 All Employees

- Handle personal data responsibly
- Complete privacy training
- Report privacy concerns
- Follow data handling procedures

17. TRAINING

- Privacy awareness training for all employees
- Role-specific training for data handlers
- Annual refresher training
- Training on new regulations and requirements

18. RELATED POLICIES

This policy should be read in conjunction with:

- TMG-SEC-005: Records Management and Document Retention Policy
- TMG-SEC-017: Cybersecurity and IT Security Policy
- TMG-SEC-018: Consumer Data Rights and CCPA/GDPR Compliance
- 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

19. POLICY REVIEW

This policy shall be:

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

20. DEFINITIONS

- **Personal Data:** Information relating to an identified or identifiable individual.
- **Processing:** Any operation performed on personal data.
- **Data Subject:** Individual whose personal data is processed.
- **Controller:** Entity that determines purposes and means of processing.
- **Processor:** Entity that processes data on behalf of a controller.

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