THIRD-PARTY DATA SHARING AND PROCESSING AGREEMENTS

JANUARY 2026

POLICY NUMBER: TMG-SEC-019
APPROVAL AUTHORITY: BOARD OF DIRECTORS

THE MAZI GROUP

1. PURPOSE

This policy establishes The Mazi Group's requirements for sharing personal data with third parties and executing appropriate data processing agreements. Proper contractual protections are essential to ensuring that personal data shared with vendors, partners, and service providers is handled in compliance with privacy laws and our commitments to customers across all brands: Mazi Beauty, Glam Switch, On The Go Mists, and Upvendo.

2. SCOPE

This policy applies to:

- All sharing of personal data with third parties
- All vendors, service providers, and partners who process personal data
- All brands and business units
- All types of data sharing arrangements
- All geographic regions

3. THIRD-PARTY CATEGORIES

3.1 Service Providers / Processors

Process data on our behalf under our instructions:

- Cloud hosting providers
- Payment processors
- Email service providers
- Customer service platforms
- Analytics providers
- Shipping and logistics partners
- Contract manufacturers

3.2 Business Partners

Joint or independent processing for mutual benefit:

- Co-marketing partners
- Retail partners

- Affiliate partners
- Technology integration partners

3.3 Third Parties (Independent Controllers)

Receive data and determine their own processing purposes:

- Advertising networks
- Social media platforms
- Data brokers (if applicable)
- Research organizations

4. DATA SHARING PRINCIPLES

- **Necessity:** Share only data necessary for the purpose
- **Purpose Limitation:** Data used only for specified purposes
- **Security:** Appropriate security measures required
- **Accountability:** Third parties accountable for compliance
- **Transparency:** Disclose sharing in privacy notices

5. PRE-SHARING REQUIREMENTS

5.1 Due Diligence

- Assess third-party privacy and security practices
- Review security certifications (SOC 2, ISO 27001)
- Evaluate compliance with applicable laws
- Check for prior data breaches or violations
- Assess data handling capabilities

5.2 Risk Assessment

- Evaluate sensitivity of data to be shared
- Assess volume of data
- Consider geographic locations of processing
- Identify potential risks to data subjects
- Document risk assessment findings

5.3 Approval Requirements

Data Type	Approval Required
Non-sensitive business data	Department Manager
Personal data (standard)	Privacy Team + Legal
Sensitive personal data	DPO + Legal + Executive
Biometric data (Glam Switch)	DPO + Legal + CISO + Executive

6. DATA PROCESSING AGREEMENTS

6.1 When Required

A Data Processing Agreement (DPA) is required when:

- Third party processes personal data on our behalf
- We act as data controller and they act as processor
- Required by GDPR, CCPA, or other applicable laws

6.2 Required DPA Provisions (GDPR Article 28)

- Subject matter and duration of processing
- Nature and purpose of processing
- Type of personal data and categories of data subjects
- Obligations and rights of the controller
- Processing only on documented instructions
- Confidentiality obligations for personnel
- Appropriate security measures
- Sub-processor restrictions and requirements
- Assistance with data subject rights
- Assistance with security and breach notification
- Deletion or return of data upon termination
- Audit rights

6.3 Additional DPA Provisions

- Data breach notification timeframes (24-72 hours)
- Insurance requirements
- Indemnification provisions
- Limitation on data use
- Prohibition on selling data
- Compliance certification requirements

7. SERVICE PROVIDER AGREEMENTS (CCPA)

7.1 Required Provisions

- Prohibition on selling or sharing personal information
- Prohibition on retaining, using, or disclosing data outside the business relationship
- Prohibition on combining data with other sources (with exceptions)
- Compliance certification
- Right to take reasonable steps to ensure compliance
- Notification if unable to meet obligations

7.2 Contractor Agreements

For CPRA "contractors":

- Written contract with required terms
- Certification of understanding and compliance
- Grant of right to monitor compliance

8. INTERNATIONAL DATA TRANSFERS

8.1 Transfer Mechanisms

For transfers outside EEA/UK:

- Standard Contractual Clauses (SCCs) - EU approved
- UK International Data Transfer Agreement/Addendum
- Adequacy decisions (where available)

- Binding Corporate Rules (if applicable)
- Derogations (limited circumstances)

8.2 Transfer Impact Assessment

- Assess laws of destination country
- Evaluate risks to data subjects
- Identify supplementary measures needed
- Document assessment and decision

8.3 Supplementary Measures

- Technical measures (encryption, pseudonymization)
- Organizational measures (access controls, policies)
- Contractual measures (additional commitments)

9. SUB-PROCESSOR MANAGEMENT

9.1 Sub-Processor Requirements

- Prior authorization for sub-processors (general or specific)
- Written agreements with sub-processors
- Same data protection obligations as primary processor
- Processor remains liable for sub-processor compliance

9.2 Sub-Processor Notification

- Maintain list of approved sub-processors
- Notify of new sub-processors (for general authorization)
- Provide opportunity to object
- Document sub-processor changes

10. SPECIFIC SHARING SCENARIOS

10.1 Cloud Services

- DPA required with cloud providers

- Verify data center locations
- Ensure appropriate security certifications
- Address data residency requirements

10.2 Marketing and Advertising

- Disclose sharing in privacy notice
- Honor opt-out requests
- Contractual restrictions on data use
- Comply with "sale" and "sharing" definitions

10.3 Payment Processing

- PCI DSS compliant processors only
- Minimize data shared
- Strong contractual protections
- Regular compliance verification

10.4 AI and Analytics (Glam Switch)

- Special protections for biometric data
- Clear purpose limitations
- Prohibition on model training without consent
- Data minimization requirements

10.5 Upvendo Restaurant Clients

- Clear controller/processor relationship
- DPA with restaurant clients as controllers
- Support for client compliance obligations
- End consumer data handling procedures

11. AGREEMENT TEMPLATES

11.1 Standard Templates

- Data Processing Agreement (GDPR compliant)

- Service Provider Agreement (CCPA compliant)
- Standard Contractual Clauses (controller-to-processor)
- Standard Contractual Clauses (controller-to-controller)
- UK International Data Transfer Addendum

11.2 Template Usage

- Use approved templates for all agreements
- Legal review required for modifications
- Document deviations from standard terms
- Update templates for regulatory changes

12. ONGOING MANAGEMENT

12.1 Agreement Tracking

- Maintain register of all data sharing agreements
- Track agreement terms and expiration dates
- Monitor compliance obligations
- Schedule periodic reviews

12.2 Compliance Monitoring

- Regular assessment of third-party compliance
- Request compliance certifications annually
- Conduct audits for high-risk processors
- Address compliance issues promptly

12.3 Incident Response

- Require prompt breach notification from third parties
- Coordinate incident response
- Document third-party incidents
- Assess need for regulatory notification

13. TERMINATION

13.1 Data Return/Deletion

- Require return or deletion of data upon termination
- Specify timeframe for data deletion
- Obtain certification of deletion
- Address data in backups

13.2 Transition Planning

- Plan for data migration if needed
- Ensure continuity of data protection
- Verify new provider compliance before transfer

14. ROLES AND RESPONSIBILITIES

14.1 Privacy Team

- Review and approve data sharing arrangements
- Maintain agreement templates
- Track data sharing agreements
- Conduct third-party assessments

14.2 Legal

- Negotiate and finalize agreements
- Review non-standard terms
- Advise on legal requirements
- Update templates for legal changes

14.3 Business Units

- Identify data sharing needs
- Initiate third-party engagement process
- Monitor day-to-day third-party performance
- Report compliance concerns

14.4 Security

- Assess third-party security practices
- Review security certifications
- Participate in security audits
- Respond to security incidents

15. RELATED POLICIES

This policy should be read in conjunction with:

- TMG-SEC-014: Vendor and Supplier Management Policy
- TMG-SEC-016: Data Privacy and Protection Policy
- TMG-SEC-017: Cybersecurity and IT Security Policy
- TMG-SEC-018: Consumer Data Rights and CCPA/GDPR Compliance
- TMG-SEC-020: Incident Response and Data Breach Notification

16. POLICY REVIEW

This policy shall be:

- Reviewed annually by Privacy and Legal teams
- Updated for regulatory changes
- Approved by the DPO and Chief Legal Officer
- Communicated to relevant teams

17. DEFINITIONS

- **Controller:** Entity that determines purposes and means of processing.
- **Processor:** Entity that processes data on behalf of a controller.
- **Sub-processor:** Processor engaged by another processor.
- **DPA:** Data Processing Agreement.
- **SCCs:** Standard Contractual Clauses approved by the European Commission.
- **Service Provider:** CCPA term for entity processing data on behalf of a business.

For questions about this policy, contact:

Privacy Department

privacy@mazigroup.us