Data Protection and Privacy Policy

Mergado Marketplaces

Last Reviewed: 5th January 2026
Owner: Mergado Technologies, s.r.o.
Contact: mergado@mergado.com

---

1. Introduction and Scope

This policy defines Mergado Technologies' approach to protecting the confidentiality, integrity, and availability of all information processed within the Mergado Marketplaces extension.

Mergado Marketplaces provides a centralized platform enabling online merchants to manage product listings, inventory, pricing, and orders across multiple e-commerce platforms. This policy describes how personal data and other information are collected, used, stored, protected, shared, and deleted in compliance with applicable data protection laws, including the General Data Protection Regulation (GDPR), and with applicable marketplace platform requirements.

This policy applies to all data processed through our services, including merchant account data, product information, and end customer personal data obtained through API integrations.

---

2. Data Collection and Use

We process only the data that is necessary to provide and operate our services.

2.1 Categories of Data

Depending on service usage, the following data may be processed:

- Merchant account information and authentication credentials
- Product data, inventory levels, and pricing information
- Order data, including buyer names, addresses, contact details, and purchase information
- Performance analytics and sales statistics

- Usage, operational, and system data (e.g., authentication events, API usage, IP addresses)

2.2 Data Collection Methods

Data is collected through:

- Direct input by merchants via the platform
- Automated API synchronization with marketplace platforms (e.g., Amazon, Allegro, Kaufland)
- Import of product data feeds from merchant e-commerce systems via the Mergado application

2.3 Purpose of Processing

Data is used exclusively for:

- Providing, operating, and maintaining the services
- Synchronizing listings, inventory, and pricing across marketplaces
- Enabling merchants to manage orders and fulfilment
- Providing analytics and performance insights required by merchants for their accounts
- Maintaining platform security and preventing fraud
- Complying with legal and regulatory obligations

We do **not** sell or rent personal data and do **not** use personal data for marketing without explicit consent.

---

3. Data Storage and Security

3.1 Storage Infrastructure

- Servers operate in dedicated VLAN and VRF networks protected by enterprise firewalls.
- Databases have no direct internet access; administrative access is permitted only via VPN with mandatory multi-factor authentication (MFA).
- Encrypted daily backups are stored in geographically separated locations.
- Recovery Point Objective (RPO): 24 hours; Recovery Time Objective (RTO): 4 hours.
- We maintain mechanisms to tag and identify the origin of data we store (including marketplace-sourced data) for clear data attribution and segregation of marketplace data.

3.2 Encryption and Key Management

- All PII is encrypted at rest using at least AES-128 (AES-256 used where feasible and for backups).
- All data in transit is encrypted using TLS 1.2 or higher. Message-level encryption is applied where channel termination occurs in untrusted multi-tenant hardware.
- Backups are encrypted using AES-256.
- Runtime encryption keys are stored as protected CI/CD secret variables or managed through a designated key-management mechanism / KMS.
- Encryption keys are never stored in application source code or application databases.
- An audited, offline backup copy of key material is maintained in a secure, encrypted vault with access restricted to a limited number of approved custodians.
- Encryption keys are rotated at least annually and immediately upon suspected compromise. Our KMS covers key lifecycle management (generation, storage, rotation, revocation) consistent with industry best practices.

3.3 Access Controls

- Role-based access control (RBAC) using the principle of least privilege.
- Unique user accounts for all employees.
- Multi-factor authentication (MFA) is required for all production system access.
- Passwords must comply with the organisation's established security requirements, including minimum length and complexity, and are subject to the organisation's password lifecycle policies.
- Database access is restricted to authorised developers and system processes only; merchants can access only their own merchant account data and associated buyer information.
- Access to decrypt buyer PII is limited to explicitly authorised roles, subject to approval workflows and full access logging.
- Access lists (people and services with access to Information) are reviewed at least quarterly. Access rights are revoked within 24 hours of employee termination.

3.4 Network and Endpoint Security

- Network and system security controls are implemented across systems in accordance with organisational security policies.
- Network segmentation isolates databases from application endpoints.
- Access to sensitive systems is limited to authorised, organisation-managed devices and users, in line with applicable security and access control policies.
- Regular security patching and configuration management are enforced.

3.5 Monitoring, Logging and Vulnerability Management

- Centralised logging and monitoring capabilities are implemented to support security monitoring, alerting, and investigation, in accordance with organisational security policies.

- Alerts are generated for indicators of potentially suspicious or unauthorised activity, where appropriate.
- Logs are retained for a minimum of 12 months for security analysis; logs do not contain PII except where necessary to meet legal or regulatory requirements.
- Vulnerability management activities, including scanning and testing, are conducted on a regular basis.
- Identified vulnerabilities are prioritised and remediated based on assessed risk and in line with defined remediation procedures.
- Secure development practices are applied, including code review processes and the use of automated security controls within development and deployment workflows.
- Data Loss Prevention (DLP) controls are implemented to detect and prevent unauthorised movement of information out of protected boundaries.
- A geographically separated secondary backup site is maintained to support timely restoration of PII availability and access in the event of a physical or technical incident.

---

4. Data Retention

Data is retained only for as long as necessary for operational and legal purposes.

- **End customer personal data (buyer PII):** Buyer personal data obtained through marketplace integrations is retained only as necessary for the legitimate purposes described in Section 2. For **Amazon**-sourced buyer PII specifically, Mergado will retain such PII for **no longer than 30 days after order delivery**, unless retention beyond that period is legally required.
- **Merchant account data:** Retained for the duration of the business relationship and deleted within 90 days of account closure, subject to legal obligations.
- **Product/inventory data:** Deleted within 30 days of account closure unless otherwise required to meet legal obligations.
- **Audit logs:** Retained for at least 12 months for security analysis and incident investigation.

Where platforms other than Amazon impose specific retention limits or deletion requirements, we will apply those platform-specific requirements to the data sourced from those platforms.

---

5. Data Sharing and Disclosure

We share data only when necessary and under strict controls:

- **With merchants:** Each merchant is provided with buyer information solely in relation to that merchant’s own orders and only to the extent necessary to perform the

merchant's obligations and functions. Merchants may optionally integrate our extension with their e-commerce platform for the purpose of managing orders within that platform.

- **With marketplace platforms:** Data is shared as required for platform functionality and in accordance with marketplace terms and policies. We will comply with marketplace requests for deletion or data handling.
- **With service providers:** Limited to infrastructure, hosting, security, and support providers that operate under written contracts requiring confidentiality, data protection obligations and appropriate safeguards (including Standard Contractual Clauses where transfers outside the EEA occur).
- **Legal requirements:** When required by law, court order, or regulatory authority. We will not speak on behalf of a marketplace or represent a marketplace to regulators unless expressly authorised in writing by the marketplace.
- **Internal access:** Personal data access is restricted to authorised employees on a strict need-to-know basis, enforced through RBAC and logged access approvals.

---

6. Incident Response

We maintain a documented Incident Response Plan (reviewed at least every six months and after major infrastructure changes) that defines roles, responsibilities, escalation paths and procedures for handling security incidents, including unauthorised access, data leaks and system compromises.

- Security events are detected through continuous monitoring, SIEM alerting and logging.
- Upon identification of an incident we perform immediate containment and remediation, conduct a root cause investigation, implement corrective actions, maintain chain of custody for investigative evidence, and document all actions taken.
- Where a personal data breach is confirmed, we will notify affected merchants and relevant supervisory authorities as required by applicable law and contractual obligations. Where a marketplace partner is affected (for example, Amazon), we will notify the marketplace in accordance with their requirements and timelines. Specifically for Amazon, we will notify Amazon security at **security@amazon.com within 24 hours** of detecting a Security Incident that involves Amazon Information, and we will cooperate with Amazon's investigation, provide remediation evidence upon request, and follow any further Amazon instructions.

The Incident Response Plan is available at:
https://www.mergado.com/sites/default/files/perm/document/incident_response_plan.pdf

---

7. Data Subject Rights

Under GDPR and applicable laws, individuals have the right to:

- Access personal data we hold about them
- Rectify inaccurate or incomplete personal data
- Request erasure (subject to legal retention requirements and platform obligations)
- Restrict processing where applicable
- Receive data in a machinereadable format (data portability)
- Object to processing based on legitimate interests

Requests should be submitted to **mergado@mergado.com**. Requests are verified and processed within **30 calendar days**, with extensions when legally permitted.

---

8. Data Deletion

Secure deletion procedures:

- Active database records are permanently deleted from all systems in accordance with documented sanitisation procedures.
- Encrypted data is removed from backups at the next backup rotation, or earlier where required to comply with legal or platform deletion obligations; backup retention and rotation schedules are documented and enforced.
- Encryption keys are destroyed or revoked in the KMS when associated data is permanently deleted in accordance with our key lifecycle procedures.
- API credentials and keys are revoked and purged immediately upon account closure or when no longer required.
- We will comply with platform deletion notices and certify secure destruction when requested.

---

9. Employee Responsibilities

All employees are required to:

- Sign confidentiality and acceptable-use agreements containing contractual confidentiality obligations for PII and marketplace data.
- Complete regular data protection, secure coding and security awareness training (annually at minimum).
- Refrain from copying data to personal devices or removable media.
- Report security incidents immediately through defined escalation channels.
- Comply with access logging, approval and monitoring requirements.

---

10. Compliance and Audits

We comply with:

- General Data Protection Regulation (GDPR) and applicable national data protection laws
- Marketplace platform requirements
- Industry security best practices

We maintain:

- Documented data handling and privacy policies and Records of Processing Activities (where applicable)
- Data Protection Impact Assessments (DPIAs) where required
- Regular internal audits and cooperation with external or marketplace-led audits.

---

11. Policy Updates

This policy is reviewed at least annually and updated when legal requirements, processing activities, or platform requirements change. Any updates are communicated to relevant employees and, where required by contract or law, to clients and partners.

---

12. Contact Information

If you have questions about this Privacy Policy or our data protection practices, or if you wish to report a security incident, please contact:

Mergado Technologies, s.r.o.
Pavlovská 12
623 00 Brno
Czech Republic

Email: mergado@mergado.com
Website: www.mergado.com