

DATA PRIVACY & CONFIDENTIALITY POLICY

BLUE MOON MTC LTDA

Corporate Governance & Compliance Pack 2026

Document ID	BM-COMP-005
Version	1.0
Effective Date	01 October 2026
Document Owner	Management - BLUE MOON MTC LTDA
Approved By	Managing Director / Sole Shareholder
Review Cycle	Annual, or earlier upon material privacy, legal, contractual or business change

1. Purpose

BLUE MOON MTC LTDA ("BLUE MOON" or "the Company") is committed to protecting personal data and confidential information entrusted to it by employees, applicants, customers, suppliers, business partners and other stakeholders.

This Policy establishes principles and minimum requirements for lawful personal-data processing and for the protection of confidential business and technical information. It complements BLUE MOON's Information Security Policy and other controlled governance documents.

2. Scope

This Policy applies to BLUE MOON management, employees, contractors and other persons acting on behalf of the Company, and to personal data or confidential information processed through Company systems, devices, cloud services, files, communications or authorized customer environments.

Customer-specific contractual, privacy and confidentiality requirements must also be followed when applicable.

3. Privacy Roles and Responsibilities

BLUE MOON may act as a controller of personal data when it determines the purposes and essential elements of processing, such as for its own corporate, recruitment, personnel, supplier or business-contact activities.

BLUE MOON may act as a processor/operator when it processes personal data on behalf of a customer and according to that customer's documented instructions and applicable contract. In that role, BLUE MOON will not independently use customer personal data for unrelated purposes.

The role applicable to a particular processing activity depends on the factual and contractual circumstances and must not be assumed solely from the name of the service.

4. Privacy Principles

Personal-data processing must follow applicable legal and contractual principles, including legitimate and specific purpose, adequacy, necessity and data minimization, transparency where required, security, prevention, non-discrimination and accountability.

BLUE MOON will seek to process only the personal data reasonably necessary for the authorized purpose and will avoid unnecessary duplication or retention.

5. Categories of Protected Information

Protected information under this Policy may include personal data, sensitive personal data, confidential business information and security-sensitive technical information.

- Personal data includes information relating to an identified or identifiable natural person.
- Sensitive personal data receives heightened protection where applicable law classifies it as such.

- Confidential business information may include contracts, pricing, financial information, commercial plans, internal records and non-public customer information.
- Security-sensitive technical information may include network diagrams, IP addressing, firewall and access-control configurations, VPN parameters, credentials, certificates, security logs, vulnerability information, change records, technical evidence and incident information.

6. Lawful and Authorized Processing

BLUE MOON will process personal data only when there is an appropriate legal, contractual or otherwise authorized basis for the activity. Personal data must not be collected or used merely because it is technically accessible.

When acting for a customer, BLUE MOON personnel must limit processing to the authorized service scope and customer instructions. If an instruction appears to conflict with applicable law or contractual security requirements, it must be escalated to BLUE MOON management before proceeding where reasonably possible.

7. Data Minimization and Purpose Limitation

Collection, access, extraction, copying and retention of personal data must be limited to what is necessary for the relevant business or technical purpose.

Technical troubleshooting, firewall analysis, logging and security work may expose BLUE MOON personnel to identifiers or other personal data contained in logs and systems. Such access does not authorize unrelated use, profiling, disclosure or retention.

8. Confidentiality Obligations

Confidential information obtained through BLUE MOON business must be used only for legitimate authorized purposes and disclosed only to persons with a valid need to know.

Confidentiality obligations continue after completion of an engagement or termination of access where required by contract, law or the nature of the information.

Personnel must not use customer information for personal benefit, competitive advantage, public demonstrations, training examples, social media, portfolios or marketing unless the information has been lawfully authorized for that use.

9. Access Control

Access to personal data and confidential information must be based on role, business need and least privilege. Access must be removed or adjusted when responsibilities change or the information is no longer required.

Privileged customer access must follow BM-COMP-004 Information Security Policy and the customer's applicable access-control requirements.

10. Sharing and Disclosure

Personal data or confidential information may be shared only when there is a legitimate and authorized purpose and appropriate safeguards are in place.

Before disclosing customer information to a subcontractor, service provider or other third party, BLUE MOON must verify that the disclosure is permitted and that appropriate confidentiality, privacy and security obligations apply.

Information must not be sent to personal email accounts, unauthorized cloud storage, consumer messaging services or other unapproved channels when such use would conflict with Company or customer requirements.

11. Cross-Border and Cloud Processing

Where personal data is stored, accessed or transferred across jurisdictions, BLUE MOON will consider applicable legal and contractual requirements governing international transfer and data location.

Cloud and software services used for protected information must be evaluated proportionately to the sensitivity of the information and the Company's role in the processing.

12. Data Subject Rights

When BLUE MOON acts as controller, requests from individuals concerning their personal data will be handled in accordance with applicable law and verified appropriately before disclosure or action.

When BLUE MOON acts as processor/operator for a customer, requests relating to customer-controlled data will normally be referred to or handled under the instructions of the relevant customer, unless applicable law requires otherwise.

13. Retention and Disposal

Personal data and confidential information must not be retained longer than necessary for legitimate business, legal, contractual, security or evidentiary purposes.

At the end of the applicable retention period or engagement, information must be securely deleted, destroyed, returned or anonymized as appropriate and subject to legal or contractual requirements.

Copies created temporarily for troubleshooting or technical analysis must be removed when no longer required, unless retention is specifically authorized.

14. Security Safeguards

BLUE MOON will apply technical and administrative safeguards proportionate to the nature of the information, processing context and risk. Applicable measures may include access controls, multi-factor authentication, encryption, secure configuration, endpoint protection, logging, backup, secure transfer and controlled deletion.

Detailed security requirements are established in BM-COMP-004 Information Security Policy and supporting security procedures.

15. Personal Data and Security Incidents

Suspected unauthorized access, loss, disclosure, alteration or other compromise involving personal data or confidential information must be reported promptly to BLUE MOON management and handled under the applicable incident-management process.

When BLUE MOON acts as processor/operator and becomes aware of a personal-data incident affecting customer-controlled data, it will inform the relevant controller without undue delay and provide reasonably available information necessary for the controller's assessment and response, subject to applicable contract and law.

When BLUE MOON acts as controller, management will assess whether notification to affected individuals, the Brazilian National Data Protection Authority (ANPD), customers or other parties is legally or contractually required. Applicable statutory deadlines must be observed.

16. Customer Technical Data

Customer technical information may be highly sensitive even when it does not constitute personal data. BLUE MOON therefore protects non-public network, firewall, security and infrastructure information under confidentiality and information-security controls regardless of whether privacy law applies.

Customer technical data must not be reused across customers or included in public materials without appropriate authorization and removal of protected information.

17. Recruitment and Personnel Data

Personal data collected from job applicants, employees and contractors must be limited to legitimate recruitment, engagement, administration, compliance and business purposes.

Access to CVs, contact information, identification records, compensation or other personnel information must be restricted to authorized persons and retained only as required for the relevant purpose and applicable obligations.

18. Suppliers and Service Providers

Where a supplier or service provider processes personal data or confidential information for BLUE MOON, the Company will apply proportionate due diligence and contractual requirements based on the nature and risk of the processing.

Third parties must not receive broader access than necessary for the contracted service.

19. Privacy by Design and Change

New systems, services or material changes involving personal data should consider privacy and security requirements during planning rather than only after implementation.

Where processing may present elevated privacy risk, BLUE MOON management will evaluate whether additional assessment, safeguards, contractual controls or a formal impact assessment are appropriate or legally required.

20. Records and Accountability

BLUE MOON will maintain records and evidence proportionate to its processing activities and obligations. Relevant documentation may include privacy notices, contractual terms, processing records, incident records, access evidence, retention decisions and third-party safeguards.

Documentation must accurately reflect actual practices and must not claim controls, certifications or processes that are not implemented.

21. Privacy Contact and Escalation

Privacy questions, data-subject requests, customer privacy matters and suspected privacy incidents must be directed through BLUE MOON's official business contact channels for management review and routing.

BLUE MOON will designate or update specific privacy responsibilities and contact information as required by applicable law, regulation, Company scale or customer commitments.

22. Training and Awareness

Personnel with access to personal data or confidential customer information must understand their confidentiality, privacy and security responsibilities. Awareness and role-specific guidance will be provided proportionate to access and risk.

23. Non-Compliance

Unauthorized access, disclosure, copying, retention or misuse of personal data or confidential information may result in access restriction, corrective action, contractual or disciplinary measures, customer notification or other action appropriate to the circumstances.

24. Responsibility and Governance

Overall responsibility for this Policy rests with BLUE MOON management. The Managing Director is accountable for approving the Policy, assigning privacy responsibilities, reviewing material privacy risks and incidents, and ensuring that privacy controls remain proportionate to the Company's activities and obligations.

Technical and administrative personnel are responsible for handling protected information only within authorized scope and for promptly escalating privacy or confidentiality concerns.

25. Related Controlled Documents

This Policy forms part of BLUE MOON's Corporate Governance & Compliance framework and should be read together with:

- BM-COMP-001 Code of Business Conduct & Ethics.
- BM-COMP-004 Information Security Policy.
- Incident Response & Security Incident Management Procedure.
- Access Control & Privileged Access Standard.
- Supplier & Subcontractor Standards.
- Business Continuity & Disaster Recovery Plan.

26. Review Cycle

This Policy will be reviewed at least annually and earlier following a material privacy incident, significant change in processing activities, applicable legal or regulatory change, material customer requirement or other relevant change in business risk.

27. Approval

This Policy becomes effective upon approval by BLUE MOON MTC LTDA management and remains in force until superseded by a later approved version.

Approved by:

LUCIANO IZAIAS MAGALHAES TYE

Managing Director / Sole Shareholder

BLUE MOON MTC LTDA