COMPLIANCE POLICY

Last updated: [01/10/2025]

1. COMMITMENT TO COMPLIANCE

GOVISAN Solutions ("the Company", "we", "our") is committed to the highest level of legal, ethical and regulatory compliance in all our business operations. As a leading company in telecommunications solutions for luxury hospitality and real estate, we recognize our responsibility to comply with applicable laws and regulations in all jurisdictions where we operate.

1.1 Scope of application
This compliance policy applies to:
- All employees, directors and consultants of GOVISAN Solutions
- Business partners, suppliers and contractors
- Subsidiaries and affiliated entities
- All business operations in India, Spain and other countries where we operate

1.2 Fundamental principles
Our compliance program is based on:
- **Integrity**: We act with honesty in all our interactions
- **Transparency**: We maintain open and honest communication with all stakeholders
- **Accountability**: We take responsibility for our actions and decisions
- **Continuous improvement**: We constantly review and improve our processes

2. REGULATORY COMPLIANCE BY JURISDICTION

2.1 India – Local compliance
As a company headquartered in Bengaluru, we comply with:

Data protection laws:
- Digital Personal Data Protection Act (DPDP), 2023[14][16][19]
- Information Technology Act, 2000
- Information Technology (Reasonable Security Practices) Rules, 2011[26]

Commercial regulations:
- Companies Act, 2013
- Foreign Exchange Management Act (FEMA), 1999
- Goods and Services Tax (GST) Act, 2017
- Contract Act, 1872

Sectoral regulations:
- Telecommunications Regulatory Authority of India (TRAI)[26]
- Bureau of Indian Standards (BIS) for telecommunications equipment
- Environmental Impact Assessment requirements

Labor compliance:

- Employees' Provident Funds Act, 1952
- Payment of Wages Act, 1936
- Industrial Disputes Act, 1947
- Sexual Harassment of Women at Workplace Act, 2013

2.2 European Union - GDPR compliance
For our services directed to EU clients:

Data protection:[15][18][21]
- General Data Protection Regulation (GDPR)
- ePrivacy Directive (Cookie Law)
- National data protection laws of each member state

EU representation:
- We have designated an EU representative according to Art. 27 GDPR
- We maintain records of processing activities according to Art. 30 GDPR

International transfers:
- We use approved Standard Contractual Clauses (SCC)
- We implement appropriate technical and organizational measures
- We conduct transfer impact assessments when necessary

2.3 Spain - European office
For our operations in Barcelona:

Local compliance:
- Organic Law on Protection of Personal Data and guarantee of digital rights (LOPDGDD)
- Spanish Civil Code for commercial contracts
- Value Added Tax (VAT) Law
- Capital Companies Law

Registrations and licenses:
- Corresponding commercial registry
- Municipal activity licenses
- Register of processing activities with AEPD

3. COMPREHENSIVE COMPLIANCE PROGRAM

3.1 Organizational structure

Chief Compliance Officer (CCO):
- Reports directly to CEO
- Supervises comprehensive compliance program
- Has authority to investigate potential violations

Compliance Committee:
- Representatives from key areas: Legal, HR, IT, Operations
- Meets quarterly to review policies and procedures
- Reports to Board of Directors semi-annually

Compliance Champions:
- Designated employees in each department

- Act as local point of contact for compliance matters
- Receive quarterly specialized training

3.2 Risk assessments
We conduct comprehensive risk assessments:

Frequency:
- Complete annual assessment
- Ad-hoc assessments for new markets, products or regulations
- Quarterly reviews of emerging risks

Areas assessed:
- Regulatory risks by jurisdiction
- Data protection and cybersecurity risks
- Corruption and bribery risks
- Competition and antitrust risks
- Environmental and sustainability risks

Methodology:
- Identification of inherent risks
- Assessment of existing controls
- Determination of residual risk
- Development of mitigation plans

3.3 Training and awareness

Induction program:
- Mandatory compliance training for all new employees
- Role and responsibility-specific modules
- Knowledge assessment before starting functions

Continuous training:
- Annual update sessions for all staff
- Specialized training for high-risk roles
- Alerts and communications about regulatory changes

Available resources:
- Internal compliance portal with policies and procedures
- Direct consultation line (compliance@govisan.com)
- Quarterly Q&A sessions with legal team

4. SPECIFIC COMPLIANCE POLICIES

4.1 Anti-corruption and anti-bribery

Absolute prohibitions:
- Bribery of public or private officials
- Facilitation payments or "grease payments"
- Inappropriate gifts or excessive entertainment
- Undeclared conflicts of interest

Implemented controls:
- Mandatory due diligence for all business partners
- Prior approval for gifts exceeding $100 USD

- Annual conflict of interest declaration by employees
- Regular audits of expenses and entertainment

Specific procedures:
- Agent and intermediary selection and monitoring process
- Political donation policies (generally prohibited)
- Guidelines for charitable contributions
- Protocols for dealing with government officials

4.2 Data protection and privacy

Fundamental principles:[19][25][28]
- Lawful, fair and transparent processing
- Purpose limitation and data minimization
- Accuracy and storage limitation
- Integrity, confidentiality and accountability

Technical measures:
- Data encryption in transit and at rest
- Role-based access controls
- Pseudonymization where appropriate
- Secure backup and recovery systems

Organizational measures:
- Data Protection Officer (DPO) designation
- Data protection impact assessments (DPIA)
- Data breach response procedures
- Data processing agreements with third parties

4.3 Information security and cybersecurity

Security framework:
- Based on ISO 27001 and NIST Cybersecurity Framework
- Regular vulnerability assessments
- Annual penetration tests by independent third parties
- Cyber incident response plan

Access policies:
- Mandatory multi-factor authentication
- Quarterly access permission reviews
- Principle of least privilege
- Continuous monitoring of privileged activities

Vendor management:
- Security assessments for all IT providers
- Mandatory cybersecurity contractual clauses
- Continuous third-party risk monitoring
- Secure termination procedures

4.4 Competition and antitrust

Specific commitments:
- Not participate in price-fixing agreements
- Not divide markets or customers with competitors

- Not exchange competitively sensitive information
- Respect third-party intellectual property

Operational policies:
- Guidelines for competitor interactions
- Procedures for participating in industry associations
- Merger and acquisition protocols
- Specific training for sales and marketing teams

5. MONITORING AND AUDITING

5.1 Continuous monitoring system

Key performance metrics:
- Number of reported and resolved violations
- Average incident resolution time
- Percentage of employees trained in compliance
- Regulatory audit results

Technology tools:
- Integrated compliance management system
- Automatic alerts for risk activities
- Executive dashboard with real-time metrics
- Automated reports for regulatory authorities

5.2 Internal audit program

Frequency and scope:
- Complete annual compliance program audit
- Quarterly thematic audits by risk area
- Semi-annual follow-up on previous recommendations

Methodology:
- Review of policies and procedures
- Testing of implemented controls
- Interviews with key personnel
- Review of documentation and records

Reports:
- Executive reports for senior management
- Detailed reports for operational management
- Corrective action plans with specific timelines

5.3 External audits

Regulatory audits:
- Full cooperation with government inspectors
- Proactive preparation for scheduled audits
- Complete and organized documentation
- Follow-up on regulatory recommendations

Third-party audits:
- Annual ISO certifications (27001, 9001, 14001)
- Compliance audits by enterprise clients

- Due diligence reviews for strategic partners
- Sustainability and ESG assessments

6. REPORTING AND ESCALATION PROCEDURES

6.1 Reporting channels

Compliance hotline:
- Email: compliance@govisan.com
- Phone: [Specific 24/7 number]
- Secure web system for anonymous reports
- Physical mailbox in main offices

Reporter guarantees:
- Strict confidentiality of identity
- Prohibition of retaliation against good faith reporters
- Impartial investigation of all reports
- Communication of results when appropriate

6.2 Investigation process

Process stages:
1. **Receipt and registration** (24 hours)
2. **Initial assessment** (72 hours)
3. **Detailed investigation** (15-30 days)
4. **Determination and corrective measures** (7 additional days)
5. **Follow-up and closure** (30-60 days)

Investigation principles:
- Presumption of innocence until proven otherwise
- Right to be heard and present evidence
- Proportionality between offense and sanction
- Complete documentation of process

6.3 Corrective and disciplinary measures

Sanction scale:
- Counseling and additional training
- Verbal or written warning
- Temporary suspension with or without pay
- Employment contract termination
- Civil or criminal legal action

Factors considered:
- Severity of violation
- Intentionality of act
- Employee's previous history
- Cooperation during investigation
- Impact on company and stakeholders

7. CONTINUOUS IMPROVEMENT

7.1 Periodic program review

Annual evaluation:
- Effectiveness of implemented controls
- Policy adequacy to current regulations
- Operational procedure efficiency
- Employee satisfaction with program

Benchmarking:
- Comparison with industry best practices
- Participation in sectoral working groups
- Consultations with external experts
- Adoption of international standards

7.2 Compliance innovation

Emerging technologies:
- Artificial intelligence for anomaly detection
- Blockchain for transaction traceability
- Compliance process automation
- Predictive analytics for risk management

Advanced methodologies:
- Design thinking applied to compliance
- Gamification for training
- Microlearning for continuous education
- Behavioral insights for cultural change

8. COMMUNICATION AND CULTURE

8.1 Program communication

Internal channels:
- Employee portal with compliance resources
- Quarterly newsletters with updates
- Semi-annual town halls with leadership
- Specific departmental sessions

External communication:
- Code of ethics published on website
- Compliance statements in proposals
- Annual sustainability reports
- Participation in sectoral conferences

8.2 Compliance culture

Organizational values:
- Compliance as everyone's responsibility
- "Speak up" culture for reporting concerns
- Recognition of ethical behavior
- Visible leadership by example

Cultural indicators:
- Annual ethical culture surveys
- Training engagement metrics
- Number of proactive compliance consultations

- Client and partner feedback on ethical behavior

9. CONTACTS AND RESOURCES

9.1 Compliance team

Chief Compliance Officer:
Email: cco@govisan.com
Location: Bengaluru, India

European Compliance:
Email: eu-compliance@govisan.com
Location: Barcelona, Spain

Data Protection Officer:
Email: privacy@govisan.com
Available: 24/7 for critical incidents

9.2 External resources

Legal advisory:
- Main firm in India: [Name and contact]
- European advisory: [Name and contact]
- Jurisdiction specialists as needed

Main regulatory bodies:
- **India:** Ministry of Electronics and IT, Data Protection Board
- **Spain:** Spanish Data Protection Agency (AEPD)
- **EU:** European Data Protection Board (EDPB)

10. FINAL PROVISIONS

10.1 Validity and updates
This policy comes into effect on [Date] and will be reviewed annually or when significant regulatory changes require it.

10.2 Authority and approval
This policy has been approved by the Board of Directors of GOVISAN Solutions and is binding for the entire organization.

10.3 Languages
This policy is available in English, Spanish and Hindi. In case of discrepancies, the English version prevails.

Approved by: Board of Directors
Approval date: [Date]
Next review: [Date + 1 year]
Version: 1.0