E-Commerce

Compliance in India: Risks, Regulations & Readiness 2026

At a Glance

- Compliance has shifted from reactive to continuous.
- Platform accountability has increased significantly.
- Data governance and consumer protection now intersect.
- Dark patterns and algorithmic transparency are emerging enforcement priorities.
- Compliance increasingly requires coordination between Legal, Product, Operations and Technology.

manucomply

Sector Snapshot

India's e-commerce market is projected to reach USD 325-350 billion by 2030, making it one of the fastest-growing digital markets globally.

Expected to surpass 500 million online shoppers by 2030, driven by rising internet penetration and smartphone adoption.

E-commerce contributes significantly to India's digital economy, supported by UPI, digital payments, and expanding logistics infrastructure.

It includes marketplace platforms, inventory-based models, D2C brands, quick commerce, social commerce, B2B e-commerce and ONDC-enabled platforms.

Why compliance has become more complex

Multiple regulators

Platform accountability

Data protection

Consumer trust

Continuous monitoring

India's e-commerce ecosystem operates within a complex regulatory framework covering:

- Consumer protection
- Data governance and privacy
- Taxation
- Competition law
- Foreign investment (FDI)
- Product safety and quality

Unlike traditional retailers, e-commerce businesses, including marketplace operators, inventory-based platforms, online sellers and D2C brands, must comply with regulations across the entire customer journey, including:

- Seller onboarding and verification
- Product listing and disclosures
- Payment processing
- Customer data management
- Grievance redressal and refunds

Regulatory expectations have evolved significantly. Authorities now focus on:

- Greater transparency in online transactions
- Strengthening consumer trust
- Ensuring fair competition
- Holding platforms accountable , not just sellers, for facilitating compliant transactions

manucomply

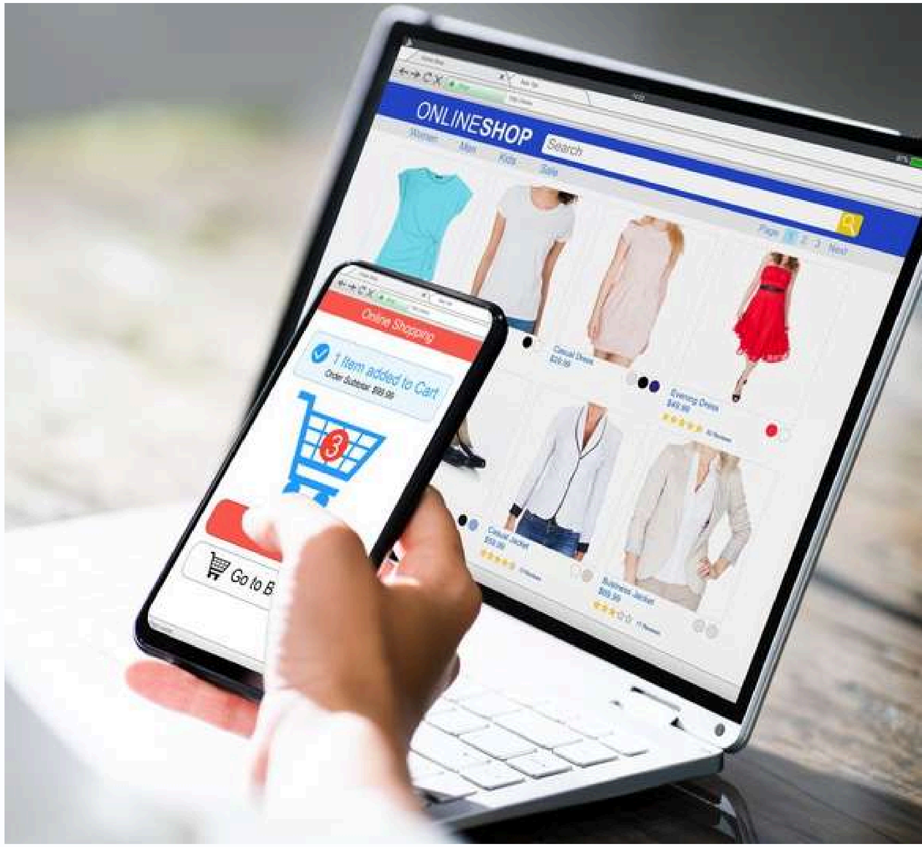
How India's E-Commerce Regulation Evolved

What drove regulation?

- Mobile commerce
- UPI adoption
- Logistics expansion
- Marketplace dominance
- Post-pandemic online shopping boom

What risks emerged?

- Misleading discounts
- Counterfeit products
- Unsafe goods
- Hidden chargesl
- Opaque algorithms
- Data misuse
- Tax leakage
- Weak grievance redressal



Regulatory response

Regulators shifted from treating e-commerce as a technology platform to recognising it as a consumer-facing retail ecosystem requiring continuous compliance.

Today's regulatory priorities

- Consumer protection
- Market fairness
- Accountability

manucomply

Key Compliance Challenges for E-Commerce Businesses

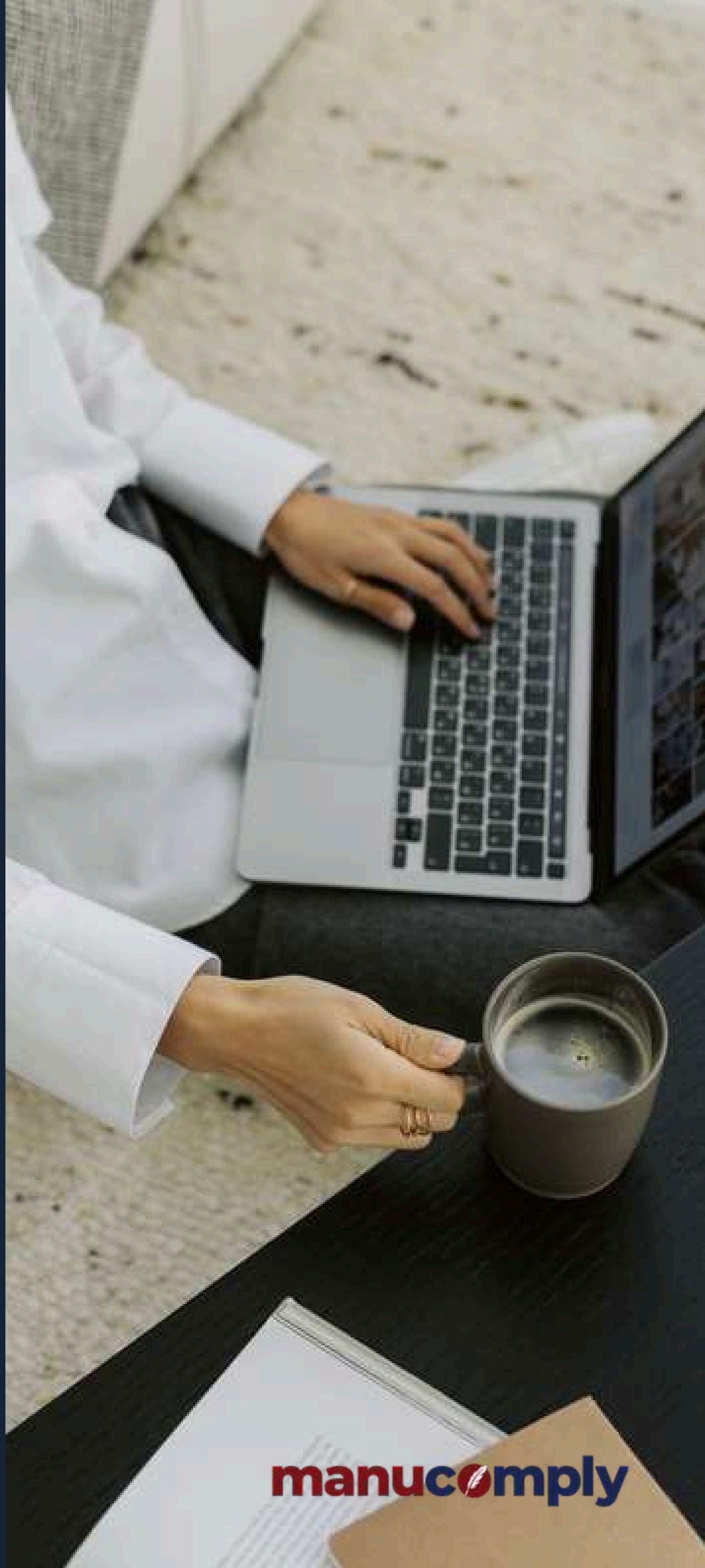
Compliance challenges are more complex than those faced by conventional retailers because they operate at the intersection of technology, logistics, payments, advertising and retail law.

Multi-Regulator Compliance	A single transaction may trigger obligations under consumer law, GST, income tax, data protection, legal metrology, competition law and FDI policy. Businesses often struggle to coordinate compliance across legal, product, operations and technology teams.
Seller Due Diligence	Marketplace operators must verify seller identity, GST registration, product authenticity, return policies and statutory disclosures. Weak onboarding controls can expose platforms to liability for counterfeit or non-compliant products.
Pricing Transparency	Hidden charges, dynamic pricing, misleading discounts and last-minute fee additions are among the most common consumer complaints. Regulators increasingly expect total price disclosure upfront.
Product Authenticity and Safety	Platforms must ensure that listings comply with product-specific laws such as BIS certification, Legal Metrology declarations and sectoral safety standards. Unsafe toys, electronics, wireless devices and cosmetics are frequent enforcement targets.
Data Governance and Cybersecurity	E-commerce businesses collect large volumes of personal data, including addresses, phone numbers, payment details and browsing histories. They must ensure lawful processing, consent management, retention controls and breach response mechanisms.
Tax Reconciliation	GST TCS, seller registration, invoice matching and income-tax withholding under Section 194-O create recurring reconciliation issues. Errors often lead to notices, interest and penalties.
Platform Neutrality and Competition Risk	Algorithms that favour related sellers, private labels or sponsored listings can attract scrutiny under competition law. Deep discounting and exclusive arrangements are also closely monitored.
Foreign Investment Restrictions	Marketplace entities receiving FDI must avoid inventory ownership, price control and preferential vendor treatment. Commercial arrangements that blur the line between marketplace and inventory models can create serious regulatory exposure.

Common Violations

The most frequent compliance failures in India's e-commerce sector are not isolated legal breaches but recurring operational patterns, like:

- Hidden or late-disclosed charges, such as convenience fees added at checkout;
- Misleading discounts, where the original price is inflated or the offer is not genuine;
- Non-disclosure of seller identity, GSTIN or customer care details;
- Sale of non-compliant products, including toys, electronics or packaged goods without mandatory declarations;
- Unauthorised sale of branded goods, especially through third-party sellers;
- Failure to honour refunds or returns for defective or deficient goods;
- Data retention beyond necessity, including storing identity documents after fulfilment;
- Weak consent mechanisms and bundled privacy notices;
- GST/TCS mismatches and delayed filings;
- Preferential ranking or self-preferencing of related sellers or private labels; and
- Dark patterns, such as manipulative user-interface design that nudges consumers into unwanted purchases or subscriptions.



Regulatory framework

Regulators have increasingly moved from complaint-based enforcement to proactive scrutiny. This includes notices, investigations, product takedown directions, consumer advisories, tax audits and competition inquiries. The trend is clear: platforms are expected to exercise active oversight rather than claim passive intermediary status.

These actions demonstrate that marketplaces are expected to monitor listings for statutory compliance, not merely host third-party sellers.

manucomply

Consumer Protection Act, 2019 and Consumer Protection (E-Commerce) Rules, 2020

The Consumer Protection (E-Commerce) Rules, 2020 constitute the primary regulatory framework governing online marketplaces and inventory-based e-commerce entities.

The Rules apply to all e-commerce entities offering goods or services to consumers in India, including foreign e-commerce entities that systematically offer goods or services to consumers in India.

Key Statutory Provisions

Rule 4 – Duties of E-commerce Entities

Every e-commerce entity must:

- Appoint a nodal contact person or senior designated functionary resident in India to ensure compliance with the Consumer Protection Act and the Rules.
- Establish an effective grievance redressal mechanism and appoint a Grievance Officer.
- Acknowledge consumer complaints within 48 hours and redress them within one month from the date of receipt.
- Display on its platform its legal name, principal geographic address, headquarters address, website details, e-mail address and customer care contact details, along with the Grievance Officer's contact information.
- Provide clear information regarding return, refund, exchange, warranty, guarantee, delivery, shipment, payment methods and complaint-handling procedures.
- Ensure that advertisements are consistent with the actual characteristics, access and usage conditions of the goods or services.
- Obtain consumers' explicit and affirmative consent for purchases; consent cannot be inferred through pre-ticked checkboxes or default settings.
- Process refunds in accordance with applicable RBI guidelines or other applicable laws.
- Not impose cancellation charges on consumers unless similar charges are also borne by the e-commerce entity if it cancels the order unilaterally.
- Not manipulate prices to earn unreasonable profit having regard to prevailing market conditions or impose unjustified prices.
- Not discriminate arbitrarily between consumers of the same class.

Rule 5 – Liabilities of Marketplace E-commerce Entities

Marketplace operators are required to:

- display complete details of sellers, including legal name, address, customer care information, GSTIN (where applicable) and ratings;
- disclose ranking parameters used for products;
- identify sponsored or paid listings;
- provide information regarding imported goods, including the country of origin where applicable; and
- maintain records relating to sellers operating on the platform.

Rule 6 – Duties of Sellers

Sellers operating through marketplaces must:

- provide accurate product descriptions;
- honour advertisements and contractual commitments;
- avoid refusing refunds where goods are defective or deficient; and
- ensure that advertisements do not misrepresent product characteristics.

Rule 7 – Inventory-based E-commerce Entities

Inventory-based entities bear direct responsibility for product quality, consumer disclosures and contractual obligations, similar to conventional retailers.

Business Liability

Failure to comply may attract proceedings under the Consumer Protection Act, including investigations by the Central Consumer Protection Authority (CCPA), directions to discontinue unfair practices, product recalls, monetary penalties and action against misleading advertisements.

Common Violation Patterns

- Hidden convenience fees or shipping charges added only at checkout;
- Misleading “limited period” or “flash sale” claims;
- Failure to disclose seller identity or grievance contact details;
- Refusal to process refunds for defective goods;
- Misleading product images or exaggerated claims in advertisements.

Business Scenario

An online marketplace advertises a product at a heavily discounted price but adds mandatory convenience charges only at the payment stage. Since the total price is not transparently disclosed upfront, the practice may amount to an unfair trade practice under the Consumer Protection Act and violate the transparency obligations under the E-Commerce Rules.

Digital Personal Data Protection Act, 2023

E-commerce businesses routinely collect names, addresses, payment details, browsing behaviour and purchase histories. The DPDP Act regulates the lawful processing of such digital personal data.

Key Provisions

- **Section 5** – Personal data may only be processed for lawful purposes after valid notice.
- **Section 6** – Consent must be free, specific, informed, unconditional and capable of being withdrawn.
- **Section 8** – Data Fiduciaries must implement reasonable security safeguards, erase personal data when no longer required and notify personal data breaches.
- **Sections 11-13** – Confer rights relating to access, correction, erasure and grievance redressal.

manucomply

Business Liability

Businesses that collect excessive personal information, retain data indefinitely, deploy inadequate cybersecurity measures or fail to respond appropriately to data breaches may face regulatory action once the enforcement framework is fully operational.

Common Violation Patterns

- Collecting identity documents or location data without a clear purpose;
- Bundling consent for marketing, analytics and fulfilment into a single notice;
- Retaining customer data long after order completion;
- Weak access controls over customer databases;
- Failure to provide a simple withdrawal or grievance mechanism.

Business Scenario

An online retailer continues storing customers' identity documents long after order fulfilment without a legitimate business purpose or fails to provide an accessible mechanism for withdrawing consent. Such practices may contravene the data minimisation and consent principles under the DPDP Act.

manucomply

Information Technology Act, 2000

While the DPDP Act governs personal data protection, the Information Technology Act continues to regulate cybersecurity, electronic records and intermediary liability.

Key Provisions

- **Section 43A** – Compensation for failure to implement reasonable security practices resulting in wrongful loss.
- **Section 66** – Computer-related offences and unauthorised access.
- **Section 72A** – Punishes unlawful disclosure of personal information.
- **Section 79** – Grants conditional safe-harbour protection to intermediaries that exercise due diligence.

Business Liability

Failure to implement adequate cybersecurity controls may expose businesses to civil liability, regulatory investigations and reputational harm, particularly following data breaches.

Common Violation Patterns

- Weak password controls and poor access management;
- Failure to secure payment gateways or customer databases;
- Unauthorised sharing of customer information with third parties;
- Inadequate incident response after a breach;
- Failure to remove unlawful listings or counterfeit products after notice.

Business Scenario

If a marketplace suffers a breach because customer data was stored without encryption or access controls, it may face claims for negligence and wrongful loss under Section 43A, apart from reputational damage and consumer complaints.

manucomply

Legal Metrology Act, 2009 and Legal Metrology (Packaged Commodities) Rules, 2011

Product listings on e-commerce platforms must contain the same statutory declarations that are required on physical packaged commodities.

Key Provisions

- **Section 18** of the Legal Metrology Act mandates prescribed declarations on packaged commodities.
- **Rule 6** of the Packaged Commodities Rules requires disclosure of information such as MRP, manufacturer or importer details, country of origin, net quantity and consumer care details.

Business Liability

Platforms that permit listings without mandatory declarations increasingly face regulatory scrutiny.

Common Violation Patterns

- Missing MRP or net quantity disclosures;
- Absence of importer or manufacturer details;
- Failure to disclose country of origin for imported goods;
- Sale of products with incomplete or misleading packaging information;
- Listing products that require certification but do not display it.

Enforcement Example

The CCPA has issued notices to several e-commerce platforms for facilitating the sale of products that lacked mandatory statutory disclosures, including unauthorised wireless communication devices. More recently, enforcement action has also been taken against platforms permitting the sale of toys without mandatory BIS certification, demonstrating that platform operators are expected to exercise reasonable oversight over listings.

Goods and Services Tax (GST)

The GST framework imposes additional obligations on e-commerce operators beyond those applicable to conventional businesses.

Key Provisions

- **Section 24, CGST Act** – Mandatory registration for specified suppliers making taxable supplies through e-commerce operators.
- **Section 52, CGST Act** – E-commerce operators must collect Tax Collected at Source (TCS) on notified supplies and deposit it with the Government.

Business Liability

Common compliance failures include:

- Delayed GST return filing;
- Incorrect TCS reconciliation;
- Invoice mismatches; and
- Inaccurate reporting of supplies.

These issues often result in notices, interest liabilities and reconciliation disputes.

Business Scenario

If an e-commerce operator facilitates taxable supplies by multiple sellers but fails to reconcile TCS deductions with the actual value of supplies, the mismatch may trigger notices from tax authorities and create avoidable interest exposure.

Common Violation Patterns

- Sellers operating without mandatory GST registration;
- Mismatch between platform records and seller invoices;
- Incorrect classification of supplies;
- Failure to reconcile TCS with seller statements;
- Delayed deposit of collected tax.

manucomply

Income-tax Act, 1961

The Finance Act, 2020 introduced Section 194-O, requiring e-commerce operators to deduct 1% TDS at source on payments made to resident sellers facilitated through their digital platforms.

Business Liability

Incorrect deduction, delayed deposit or reporting failures may expose operators to interest, penalties and disallowance consequences under the Income-tax Act.

Common Violation Patterns

- Failure to deduct TDS on seller payouts;
- Incorrect PAN mapping;
- Delayed deposit of deducted tax;
- Mismatch between platform statements and seller returns;
- Confusion over whether a transaction falls within the scope of Section 194-O.

Business Scenario

If a marketplace pays a resident seller without deducting TDS under Section 194-O, the operator may be liable for interest and penalty consequences, even if the omission was caused by a system error.

manucomply

Competition Act, 2002

As digital marketplaces continue to grow, competition law has become central to platform governance.

Key Provisions

- **Section 3** – Prohibits anti-competitive agreements.
- **Section 4** – Prohibits abuse of dominant position.
- **Section 19** – Empowers the Competition Commission of India (CCI) to investigate anti-competitive conduct.

Practical Compliance Risks

Regulators have examined:

- Preferential treatment of related sellers;
- Exclusive product launches;
- Algorithmic self-preferencing;
- Deep discounting; and
- Discriminatory ranking of sellers. .

Common Violation Patterns

- Ranking related sellers above independent sellers without disclosure;
- Using platform data to advantage private labels;
- Exclusive tie-ups that reduce consumer choice;
- Opaque discounting arrangements with selected vendors;
- Algorithmic bias in search results or product visibility.

Landmark Regulatory Development

The CCI's investigations involving Amazon and Flipkart highlighted concerns regarding preferential listings, exclusive arrangements and platform neutrality, reinforcing the importance of transparent marketplace governance.

Business Scenario

If a marketplace gives higher visibility to its own private label products while suppressing competing sellers without transparent ranking criteria, the conduct may raise concerns under Sections 3 and 4 of the Competition Act.

FEMA and India's Foreign Direct Investment (FDI) Policy

Foreign investment in e-commerce is governed through FEMA and the Consolidated FDI Policy.

Marketplace entities receiving FDI are prohibited from:

- Owning inventory sold through the platform;
- Directly or indirectly influencing sale prices;
- Providing preferential treatment to selected vendors; or
- Operating in a manner that effectively converts a marketplace model into an inventory-based business.

Given continuing regulatory scrutiny, businesses must periodically review their vendor arrangements, ownership structures and commercial practices to ensure alignment with FDI conditions.

Common Violation Patterns

- Concentration of sales with a few related vendors;
- Indirect price control through incentives or rebates;
- Inventory ownership through affiliated entities;
- Vendor arrangements that resemble exclusive distribution;
- Operational control that blurs the marketplace/inventory distinction.

Business Scenario

If a foreign-funded marketplace effectively controls pricing and inventory through related entities, regulators may treat the arrangement as inconsistent with the marketplace model permitted under India's FDI policy.

Case-laws

Case Name	Compliance Lesson	Business Takeaway
Amazon v. Amway MANU/DE/0311/2020	Platforms can be liable for facilitated sales	E-commerce platforms cannot assume blanket immunity as intermediaries where they play an active role in facilitating sales. Businesses should conduct robust seller due diligence, establish effective notice-and-takedown mechanisms for infringing products, and implement systems to prevent the sale of unauthorised or counterfeit goods.
Delhi Vyapar Mahasangh v. Amazon & Flipkart MANU/CO/0001/2020	Marketplace neutrality	Marketplace operators should ensure fair and transparent platform governance. Preferential treatment to select sellers, exclusive arrangements, discriminatory algorithms and deep discounting may attract scrutiny under the Competition Act. Businesses should document objective seller-ranking criteria and maintain neutrality in marketplace operations.
Flipkart v. CCI MANU/KA/3124/2021	Competition law oversight	The Karnataka High Court reaffirmed the CCI's authority to investigate alleged anti-competitive practices in digital marketplaces. E-commerce entities should periodically review pricing policies, commercial agreements, exclusive partnerships and platform algorithms to ensure continued compliance with competition law.

Case Name	Compliance Lesson	Business Takeaway
Christian Louboutin v. Nakul Bajaj MANU/DE/4019/2018	IP protection	Online marketplaces that actively promote, advertise or facilitate sales may lose the protection available to passive intermediaries under the IT Act. Businesses should implement robust intellectual property protection measures, verify seller authenticity, promptly remove infringing listings and maintain an effective IP complaint redressal mechanism.
Kent RO v. Amit Kotak MANU/DE/0551/2017	Notice-and-takedown obligations	E-commerce platforms are expected to act responsibly once notified of intellectual property violations. Businesses should establish documented notice-and-takedown procedures, respond promptly to infringement complaints and maintain records demonstrating due diligence to minimise legal exposure.
CCPA – Non-Compliant Products	Product compliance	Platforms are increasingly expected to verify that products offered through their marketplaces comply with applicable regulatory requirements. Businesses should conduct pre-listing compliance checks, verify mandatory licences and certifications (such as BIS, FSSAI or CDSCO approvals), ensure statutory declarations are displayed, and promptly remove non-compliant products upon detection or regulatory direction.
CCPA – Dark Patterns	Fair consumer interfaces	Consumer interface design is now a key area of regulatory focus. Businesses should avoid deceptive user-interface practices such as false urgency, disguised advertisements, basket sneaking, subscription traps and hidden charges. Online platforms should ensure that consumers are provided with clear, informed and transparent choices throughout the purchasing journey.

Emerging Compliance Priorities

Regulatory expectations continue to evolve beyond statutory compliance. Authorities have increasingly focused on deceptive user-interface practices (“dark patterns”), unsafe product listings, misleading advertisements and marketplace accountability. Businesses are therefore expected to adopt compliance-by-design practices, undertake periodic legal audits of product listings, strengthen seller due diligence and integrate legal, technology and operational teams into a unified compliance framework.

Emerging Risk Areas

- Dark patterns in checkout and subscription flows;
- Influencer marketing without proper disclosure;
- AI-driven recommendations that distort consumer choice;
- Cross-border sales and customs compliance;
- Counterfeit detection and takedown systems;
- Product recall readiness and incident response;
- Stronger audit trails for seller onboarding and delisting decisions.

A platform that repeatedly promotes a “free trial” but makes cancellation difficult may attract scrutiny not only under consumer law but also under emerging dark-pattern enforcement standards.

For e-commerce businesses in India, compliance is no longer a back-office function. It is a core business capability that affects consumer trust, platform reputation, tax efficiency, investor confidence and regulatory continuity. The most resilient businesses are those that treat compliance as a design principle embedded into product architecture, seller onboarding, pricing logic, data governance and grievance redressal from the outset.

Comprehensive Compliance Checklist for E-Commerce Businesses Operating in India

A. Business Registration & Statutory Setup

- Determine the appropriate business structure (Proprietorship/Partnership/LLP/Private Limited Company) and complete incorporation/registration.
- Obtain PAN and TAN of the business entity.
- Obtain GST registration, where applicable, including compliance with registration requirements for e-commerce operators and notified suppliers under the CGST Act, 2017.
- Register under the Shops & Establishments Act, if applicable.
- Obtain relevant trade licences and local municipal approvals.
- Register as an MSME (Udyam Registration), where eligible.
- Obtain trademark registration for the business name, logo and key brands.
- Identify whether the business operates as a Marketplace Model or Inventory-Based Model and document the applicable regulatory obligations.

B. Consumer Protection & E-Commerce Rules Compliance

- Appoint a nodal contact person or senior designated functionary resident in India.
- Appoint a Grievance Officer and establish an effective grievance redressal mechanism.
- Acknowledge consumer complaints within 48 hours and resolve them within one month.
- Display the legal name, registered office address, customer care details, website and Grievance Officer details on the platform.
- Clearly publish return, refund, cancellation, exchange, warranty, guarantee, delivery and payment policies.
- Obtain explicit consumer consent before placing orders (no pre-ticked boxes or implied consent).
- Ensure refunds are processed within the prescribed timelines.
- Do not impose unilateral cancellation charges on consumers unless similar charges are borne by the platform.
- Avoid unfair trade practices, misleading advertisements, deceptive pricing and arbitrary discrimination between consumers.
- Ensure advertisements accurately represent the goods or services offered.
- Display registered office address, principal geographic address (where applicable), e-mail address and customer care contact details as required under the E-Commerce Rules.
- Ensure compliance with the Consumer Protection (E-Commerce) Rules, 2020 for both marketplace and inventory-based models.

C. Marketplace Compliance (Applicable to Marketplace E-Commerce Entities)

- Conduct seller KYC and due diligence before onboarding sellers.
- Obtain written undertakings from sellers regarding compliance with applicable laws and accuracy of product information.
- Display seller details including legal name, address, customer care details and GSTIN (where applicable).
- Display seller return, refund, warranty and shipping policies.
- Clearly identify sponsored or paid listings.
- Disclose the main ranking parameters determining product visibility.
- Maintain records of all sellers operating on the platform.
- Establish systems to detect and remove counterfeit, prohibited or illegal products.
- Prevent sellers from posting fake reviews or falsely representing themselves as consumers.
- Display importer details and country of origin wherever required under applicable laws.

D. Product Listing & Consumer Information Compliance

- Ensure product descriptions, specifications and images are accurate and not misleading.
- Display mandatory declarations under the Legal Metrology (Packaged Commodities) Rules, including:
  - MRP;
  - manufacturer/importer details;
  - country of origin (where applicable);
  - net quantity;
  - consumer care details; and
  - expiry/manufacturing details, wherever required.
- Verify mandatory certifications before listing regulated products (e.g., BIS, FSSAI, CDSCO, AGMARK, Hallmark).
- Remove prohibited, unsafe or recalled products promptly.
- Establish a product recall and customer notification mechanism.

E. Data Privacy & Cybersecurity Compliance

- ✓ Publish a Privacy Policy, Terms of Use and Cookie Policy.
- ✓ Obtain valid consent before collecting or processing personal data.
- ✓ Collect only data necessary for specified business purposes.
- ✓ Maintain appropriate security safeguards for customer data.
- ✓ Implement encryption, access controls and secure authentication mechanisms.
- ✓ Maintain a documented data retention and deletion policy.
- ✓ Establish procedures for reporting and responding to personal data breaches.
- ✓ Conduct periodic cybersecurity audits and vulnerability assessments.
- ✓ Secure payment gateways and comply with RBI and payment security requirements.

F. Tax & Financial Compliance

- ✓ Obtain GST registration, where applicable.
- ✓ Collect and deposit Tax Collected at Source (TCS) under Section 52 of the CGST Act, wherever applicable.
- ✓ Reconcile GST returns with seller transactions and platform records.
- ✓ Deduct TDS under Section 194-O of the Income-tax Act on eligible seller payments.
- ✓ Deposit TDS within prescribed timelines and file periodic TDS returns.
- ✓ Maintain proper books of accounts and financial records.
- ✓ Conduct statutory audit and tax audit, wherever applicable.

G. Competition Law & Fair Marketplace Practices

- Avoid preferential treatment of related sellers or private labels.
- Ensure pricing practices do not distort market competition.
- Review exclusive arrangements for Competition Act compliance.
- Maintain transparent seller ranking and recommendation mechanisms.
- Periodically review algorithms for discriminatory or anti-competitive outcomes.
- Maintain documentation supporting objective ranking and recommendation criteria.

H. Foreign Investment (FDI) Compliance (Applicable to Foreign-Funded Marketplace Entities)

- Ensure compliance with the Consolidated FDI Policy and FEMA.
- Operate strictly as a marketplace where applicable.
- Do not own or control inventory sold on the platform.
- Do not directly or indirectly influence product prices.
- Avoid preferential treatment to selected vendors.
- Periodically review vendor relationships and commercial arrangements for FDI compliance.

I. Consumer Grievance & Customer Support

- Maintain a dedicated customer support mechanism.
- Issue complaint/ticket numbers for every consumer grievance.
- Maintain grievance registers and complaint resolution records.
- Maintain records demonstrating timely complaint acknowledgement and resolution
- Track complaint resolution timelines.
- Establish escalation mechanisms for unresolved complaints.
- Periodically analyse complaint trends and implement corrective measures.

J. Advertising, Marketing & Platform Governance

- Ensure advertisements are truthful, substantiated and compliant with the Consumer Protection Act.
- Comply with the Guidelines for Prevention of Misleading Advertisements and Endorsements.
- Ensure influencer advertisements comply with ASCI's Influencer Advertising Guidelines.
- Avoid false urgency, misleading discounts or deceptive "limited stock" claims.
- Clearly disclose sponsored products and paid promotions.
- Ensure promotional campaigns accurately reflect actual offers and availability.

Checklist

manucomply

K. Employment & Labour Compliance

- Issue appointment letters and employment contracts to employees.
- Maintain attendance, wage and leave records.
- Comply with Minimum Wages, Payment of Wages and Payment of Bonus requirements.
- Register under EPF and ESI, where applicable.
- Constitute an Internal Committee under the POSH Act (where 10 or more employees are employed).
- Implement a POSH Policy and conduct employee awareness programmes.
- Comply with Maternity Benefit, Gratuity and other applicable labour laws.

L. Records & Documentation

- Maintain seller onboarding and KYC records.
- Maintain transaction logs and payment records.
- Maintain GST, TDS and financial records.
- Maintain complaint and grievance records.
- Maintain cybersecurity audit reports.
- Maintain privacy and consent records.
- Maintain contracts with sellers, logistics partners and payment service providers.
- Maintain internal compliance audit reports.
- Preserve records in accordance with applicable statutory retention requirements.

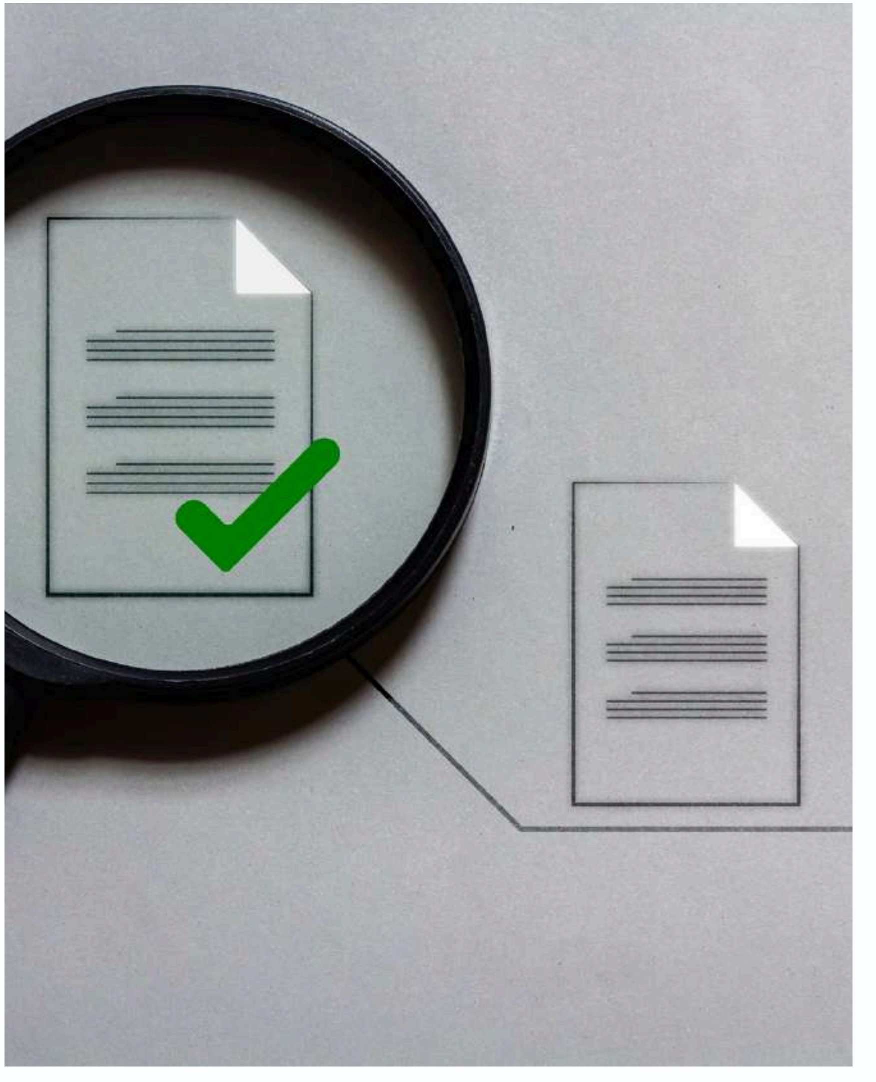
M. Periodic Compliance Review & Governance

- Conduct periodic legal and compliance audits.
- Review platform policies following legislative or regulatory changes.
- Train employees on consumer protection, data privacy and cybersecurity obligations.
- Conduct periodic seller compliance reviews.
- Monitor regulatory developments issued by the CCPA, MeitY, DPIIT,
- RBI, GST authorities, Income Tax Department and the Competition Commission of India.
- Establish an internal compliance calendar to monitor licence renewals, statutory filings, tax compliances and regulatory reporting.
- Implement a Compliance-by-Design framework integrating legal, operational and technology teams into platform governance.

Compliance Is No Longer a Function. It's a Business Capability.

The organisations that will lead India's digital economy are not those that simply comply with regulations, but those that embed compliance into every stage of the business - from product design and seller onboarding to customer experience and governance.

Reactive Compliance	Compliance by Design
Spreadsheets	Centralised compliance platform
Manual tracking	Automated monitoring
Periodic audits	Continuous compliance
Siloed legal teams	Cross-functional ownership
Regulatory response	Proactive risk management
Compliance as a cost	Compliance as a competitive advantage



Build a Future-Ready Compliance Function with

manucomply

www.manucomply.com