Regulatory Readiness Playbook for SaaS Companies

Market entry checklists and compliance frameworks for global SaaS expansion

LAWSEL ADVISORY

www.thelawsel.com

Table of Contents

01 Market Entry Compliance Checklist

02 Data Localisation Requirements

03 Consumer Protection Compliance

04 Security Compliance Framework Selection

05 Regulatory Change Monitoring

06 Go-Live Compliance Checklist

CHAPTER 1

Market Entry Compliance Checklist

European Union

- [ ] Appoint an EU representative if you have no EU establishment (GDPR Art. 27)
- [ ] Register with a lead supervisory authority (based on main establishment)
- [ ] Implement GDPR-compliant privacy notices and cookie consent
- [ ] Ensure data processing agreements with all EU processors
- [ ] Implement cross-border transfer mechanisms for data leaving the EEA
- [ ] Comply with the Consumer Rights Directive (14-day cooling-off period for B2C)
- [ ] Ensure auto-renewal practices meet EU consumer protection standards
- [ ] Comply with the European Accessibility Act (effective June 2025)
- [ ] Register for VAT if exceeding thresholds (or use the One Stop Shop)
- [ ] Assess sector-specific regulations (fintech: PSD2, EMD; healthtech: MDR; edtech: CEFR)

India

- [ ] Appoint a Data Protection Officer if classified as a Significant Data Fiduciary under DPDPA
- [ ] Implement consent-based data collection with clear, specific notice
- [ ] Provide data subject rights mechanisms (access, correction, erasure)
- [ ] Assess data localisation requirements (government and financial sector data)
- [ ] Register with CERT-In for cybersecurity incident reporting (6-hour notification requirement)
- [ ] Comply with Information Technology Act and IT Rules
- [ ] Assess whether SEBI, RBI, or IRDAI regulations apply (financial services)
- [ ] Register for GST if providing services in India
- [ ] Consider FDI restrictions and approval requirements for your sector

United States

- [ ] Identify applicable state privacy laws (CCPA/CPRA, Virginia CDPA, Colorado CPA, Connecticut DPA, Utah CPA, and others)
- [ ] Implement 'Do Not Sell/Share My Personal Information' mechanisms where required
- [ ] Comply with CAN-SPAM for email marketing and TCPA for calls/texts
- [ ] Assess FTC enforcement risk (Section 5 unfair/deceptive practices)
- [ ] Comply with COPPA if collecting data from children under 13
- [ ] Assess sector-specific requirements (HIPAA for health, GLBA for financial, FERPA for education)
- [ ] Register to collect state sales tax (varies by state and SaaS taxability)
- [ ] Assess state-level auto-renewal and subscription requirements

United Kingdom

- Appoint a UK representative if you have no UK establishment (UK GDPR Art. 27)
- Register with the ICO if processing personal data (annual fee based on turnover)
- Comply with UK GDPR and Data Protection Act 2018
- Implement UK-specific standard contractual clauses (UK International Data Transfer Agreement)
- Comply with the Consumer Rights Act 2015 for B2C
- Register for UK VAT if exceeding thresholds
- Assess Online Safety Act obligations if providing user-generated content features

UAE and Singapore

UAE:

- Assess whether DIFC or ADGM free zone data protection laws apply (separate from federal PDPL)
- Comply with federal PDPL requirements
- Assess data localisation requirements for government and regulated sector data
- Register for VAT (5%)
- Assess commercial licensing requirements (mainland or free zone)

Singapore:

- Comply with PDPA (consent obligations, Do Not Call registry)
- Mandatory breach notification to PDPC within 3 days (for notifiable breaches)
- Assess data transfer provisions (comparable protection standard)
- Register for GST if exceeding $1 million threshold
- Assess licensing requirements under the Payment Services Act (if applicable)

CHAPTER 2

Data Localisation Requirements

Requirements by Jurisdiction

Full Localisation (data must remain in-country):

- China: personal information exceeding volume thresholds; critical information infrastructure operator data
- Russia: personal data of Russian citizens must be stored on servers in Russia
- Vietnam: certain categories of data require local storage
- Indonesia: public sector data; certain electronic system operator data

Conditional Transfer (transfers permitted with safeguards):

- EU/EEA: adequacy decision, SCCs, BCRs, or derogations
- UK: UK adequacy regulations, UK IDTA, or derogations
- India: permitted except to countries specifically restricted by the government
- Brazil: adequacy, SCCs, BCRs, consent, or other LGPD mechanisms
- South Korea: consent or adequate safeguards

Sector-Specific Localisation:

- Financial services: many jurisdictions require transaction data to be accessible locally (India RBI, EU varies by member state)
- Healthcare: patient data often subject to stricter localisation (US HIPAA does not require localisation but creates practical barriers; EU varies)
- Government: most jurisdictions require government data to remain in-country

Architecture Considerations

- [ ] Design for multi-region deployment from the start
- [ ] Implement data residency selection in onboarding flows
- [ ] Ensure metadata and logs are also localised (not just primary data)
- [ ] Consider CDN and edge processing locations
- [ ] Document data flows including sub-processor locations
- [ ] Build tooling for data migration between regions (for customer mobility)
- [ ] Account for disaster recovery and backup locations

CHAPTER 3

Consumer Protection Compliance

Auto-Renewal Requirements

United States (California):

- Present auto-renewal terms clearly and conspicuously before purchase
- Obtain affirmative consent to the auto-renewal terms
- Provide an acknowledgement with the auto-renewal terms and cancellation policy
- Provide an easy mechanism to cancel (online cancellation must be as easy as sign-up — 'click to cancel' rule)

European Union:

- Clearly disclose the subscription term and renewal mechanism before purchase
- Provide a 14-day cooling-off period for new subscriptions (Consumer Rights Directive)
- Ensure cancellation is as easy as sign-up
- Provide confirmation of cancellation

United Kingdom:

- Similar to EU requirements under the Consumer Rights Act 2015
- Provide clear renewal notices before each renewal
- Unfair terms may be struck down under the Consumer Rights Act

Refund Obligations

- EU: full refund within 14 days of cancellation during cooling-off period
- UK: similar to EU under the Consumer Contracts Regulations
- California: refund of unused portion upon cancellation (for automatic renewals)
- Australia: strong consumer guarantees under the Australian Consumer Law — refunds required if service is not fit for purpose

Best practice: clearly state your refund policy in your terms of service. Even where not legally required, offering a money-back guarantee can reduce consumer complaints and chargeback disputes.

CHAPTER 4

Security Compliance Framework Selection

Framework Comparison

SOC 2:

- Best for: US market, SaaS companies, enterprise sales
- Timeline: Type I (3–6 months), Type II (6–12 months additional)
- Cost: $20,000–$100,000+
- Maintenance: annual audit
- Key benefit: most requested by US enterprise buyers

ISO 27001:

- Best for: international markets, EU/Asia enterprise sales
- Timeline: 6–12 months for initial certification
- Cost: $30,000–$150,000+
- Maintenance: annual surveillance audits, full recertification every 3 years
- Key benefit: internationally recognised, preferred in EU and Asia

CSA STAR:

- Best for: cloud-native companies, demonstrating cloud-specific controls
- Timeline: depends on level (self-assessment to third-party audit)
- Cost: varies widely (self-assessment is low cost)
- Key benefit: cloud-specific, complements SOC 2 and ISO 27001

HIPAA (Health):

- Required for: handling Protected Health Information in the US
- No formal certification; requires ongoing compliance programme

PCI DSS (Payments):

- Required for: handling payment card data
- Level depends on transaction volume

Recommended Approach

Year 1: SOC 2 Type I + basic security policies
Year 2: SOC 2 Type II + ISO 27001 (if targeting international markets)
Year 3+: Maintain SOC 2 Type II and ISO 27001; add sector-specific frameworks as needed

- Select an auditor/certification body early
- Implement a GRC (Governance, Risk, Compliance) tool to manage evidence
- Assign a compliance owner
- Budget for annual maintenance, not just initial certification

CHAPTER 5

Regulatory Change Monitoring

Monitoring Process

- [ ] Assign a regulatory monitoring owner (legal/compliance team)
- [ ] Subscribe to regulatory newsletters and alerts for each jurisdiction you operate in
- [ ] Monitor key sources:
  - EU: European Commission, EDPB, national DPAs
  - US: FTC, state attorney general offices, NIST
  - UK: ICO, DSIT, CMA
  - India: MeitY, Data Protection Board, SEBI, RBI
  - Singapore: PDPC, MAS
- [ ] Conduct quarterly regulatory review meetings
- [ ] Maintain a regulatory change log (date, regulation, jurisdiction, impact, action required, deadline)
- [ ] Assess impact of each change on your product, contracts, and operations
- [ ] Assign action items with deadlines and owners
- [ ] Report material changes to leadership and the Board

CHAPTER 6

Go-Live Compliance Checklist

Pre-Launch Final Checks

Privacy:

- ☐ Privacy policy published and accessible from all pages
- ☐ Cookie consent mechanism implemented and tested
- ☐ Data subject rights request mechanism operational
- ☐ DPA available for enterprise customers
- ☐ Records of processing activities up to date
- ☐ Cross-border transfer mechanisms in place

Security:

- ☐ Penetration test completed and findings remediated
- ☐ Vulnerability scanning operational
- ☐ Encryption at rest and in transit verified
- ☐ Access controls and authentication tested
- ☐ Incident response plan documented and tested
- ☐ Security certifications current (or audit scheduled)

Consumer Protection:

- ☐ Terms of service published and accepted at sign-up
- ☐ Pricing displayed clearly with taxes
- ☐ Auto-renewal terms disclosed and consented to
- ☐ Cancellation mechanism functional and accessible
- ☐ Refund policy clearly stated

Sector-Specific:

- ☐ Required licences and registrations obtained
- ☐ Sector-specific compliance requirements met
- ☐ Regulatory filings completed (if applicable)

Contracts:

- ☐ Customer agreements reviewed for the target market
- ☐ Vendor contracts include appropriate data protection terms
- ☐ Employee contracts comply with local employment law

Tax:

- ☐ VAT/GST/sales tax registration completed where required
- ☐ Tax collection and remittance configured in billing system

Ready to discuss your compliance needs?

Book a free 30-minute consultation to explore how LawSel Advisory can support your business.

BOOK A CONSULTATION

calendly.com/rini-thelawsel/30min

GET IN TOUCH

rini@thelawsel.com
www.thelawsel.com