Building Legal-Ready SaaS Products

Contracts, compliance, and certifications for scaling SaaS internationally

LAWSEL ADVISORY

www.thelawsel.com

Table of Contents

CHAPTER 1

Essential Legal Documents for SaaS

Every SaaS business needs a set of core legal documents. Getting these right from the start avoids costly renegotiations, reduces churn risk with enterprise customers, and demonstrates the maturity that investors and acquirers look for.

Terms of Service (ToS)

Your Terms of Service govern the relationship between your company and your users. Key provisions include:

- Service description and scope
- Account registration and eligibility
- Acceptable use restrictions
- Intellectual property ownership and licensing
- Payment terms, billing cycles, and taxes
- Subscription term, renewal, and cancellation
- Service level commitments (or reference to a separate SLA)
- Limitation of liability
- Indemnification
- Termination and suspension rights
- Governing law and dispute resolution

Avoid copying another company's ToS. Your terms should reflect your specific product, business model, and risk profile.

Privacy Policy

Your privacy policy is both a legal requirement and a trust signal. It should cover:

- What personal data you collect and how
- Why you process it (lawful bases under GDPR, business purposes under CCPA)
- How long you retain it
- Who you share it with (categories of recipients)
- International transfers and safeguards
- Data subject rights and how to exercise them
- Cookie and tracking practices
- How you protect the data (security measures)
- How you handle children's data
- Contact information for privacy inquiries

Write in plain language. Regulators penalise privacy policies that are not understandable to the average user.

Data Processing Agreement (DPA)

If your SaaS product processes personal data on behalf of your customers, you need a DPA. Enterprise customers will require one during procurement.

Many SaaS companies publish a standard DPA on their website that customers can review and sign electronically. This scales better than negotiating individual DPAs with each customer.

Your DPA should be pre-signed and available for download, reducing friction in the sales process.

Acceptable Use Policy (AUP)

An AUP defines what users can and cannot do with your service. Common restrictions include:

- Illegal activity
- Harassment, abuse, or harmful content
- Security violations (hacking, reverse engineering)
- Resource abuse (excessive API calls, crypto mining)
- Resale without authorisation

An AUP gives you the contractual right to suspend or terminate accounts that misuse your service.

CHAPTER 2

Data Processing and Privacy Compliance

As a SaaS provider, you will typically act as a data processor on behalf of your customers (the data controllers). Understanding this relationship is critical to your compliance obligations and contractual commitments.

Controller vs Processor

The distinction matters because it determines your obligations:

As a processor, you:

- Process data only on the controller's documented instructions
- Implement appropriate security measures
- Assist the controller with data subject rights requests
- Notify the controller of data breaches without undue delay
- Delete or return data at the end of the service
- Submit to audits and inspections

However, if you process customer data for your own purposes (e.g., analytics, product improvement, marketing), you become a controller for that processing — with all the obligations that entails.

Be honest about your data practices. Claiming to be a processor while acting as a controller is a compliance risk.

Data Residency and Localisation

Increasingly, customers and regulators require data to be stored in specific locations:

- EU customers often require data to remain within the EEA
- Indian government entities may require data to be stored in India
- Chinese regulations require certain data to undergo security assessment before transfer
- Financial services and healthcare regulators often impose data residency requirements

Build data residency capabilities early. Offering regional data hosting is becoming a competitive requirement for enterprise SaaS.

Security Baseline

At minimum, your SaaS product should implement:

- [ ] Encryption at rest (AES-256) and in transit (TLS 1.2+)
- [ ] Multi-factor authentication for user accounts
- [ ] Role-based access control
- [ ] Audit logging
- [ ] Regular vulnerability scanning and penetration testing
- [ ] Secure software development lifecycle (SSDLC)
- [ ] Incident response plan

- Business continuity and disaster recovery plans
- Employee security awareness training
- Vendor security assessments

CHAPTER 3

SaaS Contract Essentials

Enterprise SaaS contracts are negotiated documents. Understanding the key commercial and legal terms helps you negotiate efficiently and protect your business.

Subscription Terms

Key commercial terms to define:

- Subscription period (monthly, annual, multi-year)
- Auto-renewal mechanism and notice period for non-renewal
- Pricing structure (per seat, usage-based, tiered)
- Price increase provisions and caps
- Payment terms (net 30, net 60) and late payment consequences
- Taxes and who is responsible for them

Be specific about what triggers a new subscription period and how cancellation works. Consumer protection laws in many jurisdictions regulate auto-renewal practices.

Limitation of Liability

Liability provisions are among the most heavily negotiated SaaS contract terms:

- General liability cap: typically 12 months of fees paid or payable
- Uncapped carve-outs: certain obligations should not be subject to the cap (e.g., IP indemnification, confidentiality breaches, wilful misconduct)
- Exclusion of consequential damages: standard in vendor-form agreements but often resisted by enterprise buyers
- Data breach liability: increasingly carved out of general caps, with higher or uncapped limits

Understand your risk exposure. If your service processes sensitive data or supports critical business processes, your liability provisions need to reflect that.

Intellectual Property

IP provisions should clearly address:

- Ownership: the vendor retains ownership of the service, including any improvements. The customer retains ownership of their data.
- Licence grant: the vendor grants a limited, non-exclusive licence to use the service during the subscription term.
- Customer data: the vendor receives a limited licence to process customer data solely to provide the service.
- Feedback: if the customer provides suggestions or feedback, clarify whether the vendor can use it.
- IP indemnification: the vendor typically indemnifies the customer against third-party IP infringement claims related to the service.

CHAPTER 4

Security and Compliance Certifications

Enterprise customers and regulated industries require evidence of your security posture. The right certifications reduce sales friction and demonstrate maturity.

SOC 2

SOC 2 is the most commonly requested certification for SaaS companies:

- Type I: Assesses the design of controls at a point in time. Faster and cheaper to obtain. Good as a starting point.
- Type II: Assesses the operating effectiveness of controls over a period (typically 6–12 months). Required by most enterprise buyers.
- Trust Service Criteria: Security (always required), Availability, Processing Integrity, Confidentiality, Privacy (select based on your service).

Timeline: 3–6 months for Type I, 6–12 months for Type II. Cost: $20,000–$100,000+ depending on scope and auditor.

ISO 27001

ISO 27001 is the international standard for information security management systems (ISMS):

- Preferred by European and Asian enterprise customers
- Requires establishing, implementing, maintaining, and continually improving an ISMS
- Covers 93 controls across organisational, people, physical, and technological categories
- Certification valid for 3 years with annual surveillance audits

Timeline: 6–12 months. Cost: $30,000–$150,000+ depending on organisation size and scope.

When You Need What

Stage 1 — Seed/Series A:

- Focus on foundational security practices
- SOC 2 Type I is sufficient for early enterprise deals

Stage 2 — Series B and scaling:

- SOC 2 Type II becomes essential
- Consider ISO 27001 if targeting European or Asian markets

Stage 3 — Growth and regulated industries:

- Maintain SOC 2 Type II and ISO 27001
- Add sector-specific certifications as needed (HIPAA, PCI DSS, FedRAMP)
- Consider CSA STAR for cloud-specific assurance

CHAPTER 5

Scaling Internationally

International expansion introduces legal complexity across data protection, consumer protection, employment, taxation, and sector-specific regulation. Planning ahead avoids expensive surprises.

Data Localisation Requirements

Before entering a new market, assess whether data can leave the jurisdiction:

- EU/EEA: Data can be transferred with appropriate safeguards (SCCs, adequacy)
- India: Transfers permitted except to restricted countries; government data may require local storage
- China: Security assessment required for transfers exceeding volume thresholds
- Russia: Personal data of Russian citizens must be stored on servers in Russia
- Indonesia: Certain public sector data must be stored locally
- Vietnam: Data localisation requirements for specific categories

If your architecture does not support regional data hosting, start planning before you need it.

Consumer Protection

SaaS products sold to consumers or small businesses face consumer protection requirements:

- Auto-renewal disclosure: many jurisdictions (California, EU, UK) require clear disclosure and easy cancellation
- Right to cancel: EU consumers have a 14-day cooling-off period for online purchases
- Refund obligations: vary by jurisdiction
- Unfair contract terms: many jurisdictions can strike down terms that create a significant imbalance
- Accessibility: the EU European Accessibility Act (effective June 2025) requires digital products and services to be accessible

Design your subscription flow, cancellation process, and terms with these requirements in mind.

Pre-Launch Legal Checklist

Before launching in a new market:

- [ ] Identify applicable data protection law and appoint a local representative if required
- [ ] Update privacy policy and cookie notices for local requirements
- [ ] Implement appropriate cross-border transfer mechanisms
- [ ] Review consumer protection requirements (auto-renewal, cancellation, refunds)
- [ ] Assess whether sector-specific licences or registrations are required
- [ ] Review employment law if hiring locally
- [ ] Assess tax obligations (VAT/GST registration, withholding tax)
- [ ] Update terms of service for local governing law and dispute resolution
- [ ] Ensure marketing practices comply with local advertising and electronic marketing laws

- Consider local language requirements for contracts and notices

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