# Quick-Start Data Compliance Checklist for SMBs

Essential steps to help small and medium-sized businesses meet basic data protection and privacy obligations.

## 1. Understand What Data You Collect

☐ Identify all types of personal data you collect (e.g., name, email, IP addresses)

☐ List all data sources (websites, apps, contact forms, third-party tools)

☐ Categorize sensitive data (e.g., health info, financial data)

## 2. Map Data Flows

☐ Document how data flows through your systems (collection, storage, processing)

☐ Identify who has access to the data internally and externally

☐ Note where data is stored (on-premise, cloud providers, geographic locations)

## 3. Review and Update Privacy Policies

☐ Ensure your privacy policy is clear, accessible, and up to date

☐ Include details on what data is collected, why, how it’s used, and user rights

☐ Tailor the policy to relevant laws (e.g., GDPR, CCPA)

## 4. Establish Legal Basis for Data Use

☐ Confirm you have a legal basis to collect/process data (e.g., consent, contract, legitimate interest)

☐ Obtain and log user consent where required

☐ Provide users with opt-in/opt-out options for marketing communications

## 5. Implement Data Protection Measures

☐ Use encryption for data at rest and in transit

☐ Secure devices and systems with firewalls, antivirus, and strong passwords

☐ Regularly update software and perform vulnerability checks

## 6. Set Up Internal Policies and Training

☐ Create a data protection policy for staff

☐ Train employees on handling personal data securely

☐ Limit access to data based on job roles (least privilege principle)

## 7. Manage Third-Party Vendors

☐ Vet vendors for data security and compliance practices

☐ Sign Data Processing Agreements (DPAs) with third-party processors

☐ Review third-party compliance with standards (e.g., ISO, SOC 2)

## 8. Enable User Rights

☐ Make it easy for users to access, correct, or delete their data

☐ Set up processes to respond to user data requests within legal timeframes

☐ Track and log all user requests and responses

## 9. Plan for Data Breaches

☐ Create a data breach response plan

☐ Assign roles and responsibilities for breach management

☐ Know your notification obligations under GDPR/CCPA

## 10. Conduct Regular Reviews

☐ Schedule annual or bi-annual audits of your data practices

☐ Update documentation, privacy notices, and training as needed

☐ Stay informed about changes in data privacy regulations

## 🧰 Suggested Tools for SMBs

|  |  |
| --- | --- |
| Function | Tools |
| Security | Bitwarden, 1Password, Malwarebytes |
| Data Mapping | Lucidchart, Excel, Vizio |
| Policy Management | Termly, iubenda, TrustArc |
| Training | Cybersecurity Awareness Training (e.g., KnowBe4) |