How to Use the Checklist

Review each section to ensure your start-up addresses key compliance areas. Each checklist provides actionable steps to meet South African regulatory standards and support sustainable business practices. While it's a general guide, it's recommended to seek further clarification on specific requirements from relevant legal or compliance advisors.

Service Provider Compliance and Management Checklist	
1. Due Diligence and Selection	
Background Check	
☐ Verify the service provider's business credentials (e.g., registration, reputation, and financial stability).	Explain
☐ Check for any history of regulatory violations or litigation.	Explain
Experience and Expertise	
☐ Assess the provider's industry experience, especially in relation to the specific services required.	Explain
☐ Review case studies, references, or testimonials from other clients.	Explain
Licensing and Certification	
☐ Ensure the provider holds all relevant licenses and certifications (e.g., ISO certifications, data protection compliance).	Explain
☐ Confirm compliance with local and international regulations applicable to the service.	Explain
2. Data Protection and Privacy Compliance	
Privacy Policies and Compliance	
☐ Review the provider's privacy policies to ensure alignment with your data protection obligations (e.g., POPIA, GDPR).	Explain
☐ Confirm they implement data minimization principles and collect only necessary information.	Explain
Data Processing Agreement (DPA)	

Disclaimer

This checklist is for informational purposes only and should not be construed as legal advice. It does not guarantee compliance with applicable laws or serve as a substitute for professional legal or compliance consultation. Start-ups should engage qualified professionals to address specific legal requirements and ensure full compliance.

☐ Sign a DPA that specifies data processing roles, responsibilities, and compliance requirements.	Explain
☐ Ensure the DPA includes data retention, deletion, and incident notification terms.	Explain
Data Security Measures	
☐ Verify that the provider uses encryption, access controls, and other security measures to protect personal and sensitive data.	Explain
☐ Ensure multi-factor authentication (MFA) and secure storage practices are in place.	Explain
3. Service Level Agreement (SLA)	
Performance Metrics and Standards	
☐ Establish clear performance metrics, including response times, uptime, and resolution times.	Explain
☐ Include consequences for not meeting performance standards (e.g., penalties, corrective action requirements).	Explain
Quality Control and Reporting	
☐ Define quality control measures, such as regular progress reports, audits, or reviews.	Explain
☐ Request periodic reports and updates on key metrics and service delivery.	Explain
4. Security and Risk Management	
Security Policies and Controls	
☐ Ensure the provider has a documented security policy, covering network, physical, and application security.	Explain
☐ Verify compliance with security frameworks (e.g., ISO 27001, NIST).	Explain
Incident Response and Breach Notification	

Disclaimer

This checklist is for informational purposes only and should not be construed as legal advice. It does not guarantee compliance with applicable laws or serve as a substitute for professional legal or compliance consultation. Start-ups should engage qualified professionals to address specific legal requirements and ensure full compliance.

☐ Confirm that the provider has an incident response plan and will notify you promptly in the event of a data breach.	Explain
☐ Specify breach notification timelines and reporting responsibilities in the SLA.	Explain
Risk Assessments and Vulnerability Testing	
☐ Require the provider to perform regular risk assessments and vulnerability testing.	Explain
☐ Request summaries of findings and any mitigation actions taken for critical vulnerabilities.	Explain
5. Compliance and Regulatory Obligations	
Compliance with Local Laws and Standards	
☐ Verify that the provider complies with all local and industry-specific regulations applicable to their services (e.g., POPIA, GDPR, HIPAA).	Explain
Regulatory Reporting Obligations	
☐ Specify any regulatory reporting obligations that the provider must fulfill (e.g., reporting data breaches to the Information Regulator).	Explain
Audit Rights	
☐ Include provisions allowing for periodic audits or inspections to ensure compliance with contractual and regulatory requirements.	Explain
6. Confidentiality and Intellectual Property Protection	
Confidentiality Agreements	
☐ Ensure that the service provider signs a confidentiality agreement covering all proprietary and sensitive information.	Explain
Intellectual Property (IP) Ownership	
☐ Clearly define IP rights for work produced, specifying that your company retains ownership of any materials created on its behalf.	Explain
Non-Disclosure Obligations	
☐ Include non-disclosure obligations in the contract to protect sensitive business	Explain

Disclaimer

This checklist is for informational purposes only and should not be construed as legal advice. It does not guarantee compliance with applicable laws or serve as a substitute for professional legal or compliance consultation. Start-ups should engage qualified professionals to address specific legal requirements and ensure full compliance.

information from being shared with third parties.	
7. Payment and Financial Terms	
Fee Structure and Payment Terms	
☐ Define the fee structure, including fixed fees, hourly rates, or milestone-based payments.	Explain
☐ Specify payment terms, including due dates and penalties for late payments.	Explain
Invoicing and Payment Schedule	
☐ Establish a clear invoicing schedule with itemized billing, if applicable.	Explain
☐ Include details on currency, payment methods, and any applicable taxes or fees.	Explain
8. Operational and Business Continuity	
Disaster Recovery and Continuity Plans	
☐ Confirm the provider has a documented disaster recovery and business continuity plan.	Explain
☐ Include terms requiring continuity of services in case of unexpected events or disruptions.	Explain
Backups and Redundancy	
☐ Ensure the provider regularly backs up critical data and has redundancy plans in place.	Explain
☐ Specify backup frequencies and recovery time objectives (RTO) in the SLA.	Explain
9. Employee Screening and Training	
Background Checks	
☐ Confirm that the provider performs background checks on employees who will access sensitive data.	Explain
Training Programs	
☐ Ensure the provider trains their employees on data protection, security, and compliance requirements relevant to your business.	Explain
Confidentiality Agreements for Employees	
☐ Verify that all employees handling your data have signed confidentiality agreements.	Explain
10. Termination and Exit Management	

Disclaimer

This checklist is for informational purposes only and should not be construed as legal advice. It does not guarantee compliance with applicable laws or serve as a substitute for professional legal or compliance consultation. Start-ups should engage qualified professionals to address specific legal requirements and ensure full compliance.

Termination Clauses	
☐ Define conditions under which the contract can be terminated, including performance issues or compliance failures.	Explain
Data Transfer and Deletion	
☐ Specify that upon termination, the provider must securely transfer data back to you and delete any residual data within a set timeframe.	Explain
Transition Support	
☐ Include terms for transition support to a new provider or internal team if the agreement ends.	Explain

Disclaimer

This checklist is for informational purposes only and should not be construed as legal advice. It does not guarantee compliance with applicable laws or serve as a substitute for professional legal or compliance consultation. Start-ups should engage qualified professionals to address specific legal requirements and ensure full compliance.