Tax Ready Bookkeeping

AI Privacy and Data Security Checklist

Tax Ready Bookkeeping | projectbits.com/taxready

Overview

When using AI for bookkeeping, your financial data travels through systems and services. This checklist helps ensure your data remains private, secure, and compliant.

Section 1: Data Classification

What Data Are You Processing?

Data Type	Sensitivity	Example
Transaction details	Medium	Amounts, dates, descriptions
Vendor information	Medium	Names, addresses, contact info
Bank account numbers	High	Account numbers, routing numbers
Tax ID / SSN	Very High	EIN, SSN from W-9s
Financial statements	Medium-High	P&L, Balance Sheet
Employee data	Very High	Payroll, personal info
Customer payment info	Very High	Credit card, bank details

Checklist

- ☐ Inventory all data types processed by AI
- ☐ Classify each by sensitivity level
- ☐ Document where each data type flows
- ☐ Identify highest-risk data

Section 2: AI Service Provider Evaluation

Key Questions to Ask

Data Handling: - [ ] Where is data stored geographically? - [ ] Is data encrypted in transit and at rest? - [ ] Who has access to your data? - [ ] Is your data used to train AI models? - [ ] Can you request data deletion?

Security: - [ ] What security certifications do they have? (SOC 2, ISO 27001, etc.) - [ ] How do they handle security incidents? - [ ] What is their data breach notification policy? - [ ] Do they have cyber liability insurance?

Compliance: - [ ] Do they support your compliance requirements? - [ ] Can they sign a Business Associate Agreement (if needed)? - [ ] What is their data retention policy? - [ ] How do they handle data subject requests?

Provider Assessment

Criteria	Provider 1	Provider 2	Provider 3
Data encryption	Y/N	Y/N	Y/N
Data residency (US)	Y/N	Y/N	Y/N
SOC 2 certified	Y/N	Y/N	Y/N
Data not used for training	Y/N	Y/N	Y/N
Data deletion available	Y/N	Y/N	Y/N
BAA available	Y/N	Y/N	Y/N

Section 3: Data Handling Options

Public Cloud AI Services

Examples: OpenAI API, Google Cloud AI, Amazon Comprehend

Pros: - Easy to use - Cost-effective - Continuous improvement

Cons: - Data leaves your control - May be used for training - Limited visibility

Best For: Non-sensitive data, general categorization

Private/Single-Tenant AI

Examples: Self-hosted models, dedicated instances

Pros: - Data stays in your environment - Not used for training - Full control

Cons: - Higher cost - More maintenance - May be less capable

Best For: Sensitive financial data, regulated industries

Hybrid Approach

Example: Private AI for sensitive data, public for general tasks

Pros: - Balances cost and privacy - Appropriate protection by data type - Flexibility

Cons: - More complex - Multiple systems to manage - Routing logic needed

Best For: Most small businesses

Section 4: Privacy Configuration

Data Minimization

Only send what's needed:

Task	Required Data	Don't Send
Category suggestion	Amount, vendor name, description	Bank account numbers
Vendor matching	Vendor name, address	Tax ID, SSN
Receipt extraction	Receipt image	Personal information visible
Anomaly detection	Transaction patterns	Individual customer details

Checklist

- ☐ Review what data is sent to AI services
- ☐ Remove unnecessary fields before processing
- ☐ Mask sensitive information where possible
- ☐ Use vendor names instead of full records

Section 5: Access Controls

Who Can Access AI-Processed Data?

Role	Access Level	Justification
Owner	Full	Business owner
Controller	Full	Financial oversight
Bookkeeper	Transaction data	Day-to-day processing
AI Service	Processed data only	Service delivery
IT Support	Technical only	System maintenance

Access Control Checklist

- ☐ Define access levels for each role
- ☐ Implement principle of least privilege
- ☐ Review access quarterly
- ☐ Remove access when no longer needed
- ☐ Log all access to sensitive data

Section 6: Audit Trail Requirements

What to Log

Event	Details to Capture
Data sent to AI	Timestamp, data type, purpose

Event	Details to Capture
AI response received	Timestamp, confidence, decision
Human review	Who, when, decision made
Data correction	Original value, new value, reason
Data deletion	What, when, by whom

Checklist

- ☐ Logging enabled for all AI interactions
- ☐ Logs include sufficient detail
- ☐ Logs are retained appropriately (7 years for financial)
- ☐ Logs are protected from tampering
- ☐ Log review process established

Section 7: Incident Response

If a Data Breach Occurs

Immediate Actions (0-4 hours): - [ ] Identify scope of breach - [ ] Contain the breach - [ ] Preserve evidence - [ ] Notify incident response team

Short-Term (24-72 hours): - [ ] Complete investigation - [ ] Assess impact - [ ] Notify affected parties if required - [ ] Notify regulators if required

Long-Term: - [ ] Implement fixes - [ ] Update procedures - [ ] Train staff - [ ] Document lessons learned

Contacts to Have Ready

Contact	Name	Phone	Email
IT/Security			
Legal counsel			
Insurance (cyber)			
AI provider support			
Bank contact			

Section 8: Compliance Considerations

By Industry/Requirement

General Business: - State privacy laws (California CCPA, etc.) - IRS record keeping requirements - Standard data protection practices

Healthcare-Adjacent: - HIPAA if handling PHI - Business Associate Agreements required - Enhanced encryption requirements

Financial Services: - SOX compliance (if applicable) - GLBA requirements - Enhanced audit requirements

Checklist

- ☐ Identify applicable regulations
- ☐ Document compliance requirements
- ☐ Verify AI provider supports requirements
- ☐ Obtain necessary agreements
- ☐ Conduct periodic compliance reviews

Section 9: Employee Training

Training Topics

Topic	Audience	Frequency
Data classification	All staff	Onboarding + annual
AI tool proper use	Bookkeeping team	Onboarding + as needed
Privacy awareness	All staff	Annual
Incident reporting	All staff	Annual
Phishing awareness	All staff	Quarterly

Checklist

- ☐ Training program defined
- ☐ Training materials created
- ☐ Training completion tracked
- ☐ Knowledge verified periodically
- ☐ Training updated as tools change

Section 10: Ongoing Monitoring

Regular Reviews

Review	Frequency	Owner
Access rights	Quarterly	Manager
AI accuracy	Monthly	Bookkeeper
Privacy compliance	Annually	Owner
Vendor security posture	Annually	Owner/IT
Incident log review	Monthly	Manager

Checklist

- ☐ Review schedule established

- ☐ Responsibilities assigned
- ☐ Documentation maintained
- ☐ Issues tracked to resolution
- ☐ Continuous improvement process

Summary: Privacy-First AI Implementation

Before Enabling AI

1. Classify your data
2. Evaluate AI providers
3. Configure data minimization
4. Set up access controls
5. Enable audit logging
6. Train your team

Ongoing

1. Monitor AI interactions
2. Review access quarterly
3. Update training annually
4. Respond to incidents promptly
5. Re-evaluate providers annually

Assessment Completed By:

Date:

Next Review Date:

For more resources: projectbits.com/taxready/ch7

Tax Ready Bookkeeping by Don Lovett | ProjectBits Consulting

Tax Ready(TM) Bookkeeping