VENDOR CONTRACT REVIEW CHECKLISTS

IT Security Addendum | Data Protection Agreement | AI Governance Provisions

Available at www.tpvrm.net/documents | The Future of Third-Party Risk Management & Data Privacy

These checklists summarize the key contract review and negotiation considerations from Chapter 4 of the book. Use them during contract review to confirm that necessary provisions are included and to identify gaps that may need negotiation or risk acceptance.

Tier guidance: 1 = All tiers. 1-2 = Tier 1 and Tier 2. 1 only = Tier 1 critical vendors only.

PART 1: IT SECURITY ADDENDUM REVIEW CHECKLIST

The IT Security Addendum (ISA) should be included with or integrated into all vendor agreements where the ITC scope assessment has identified access to non-public or regulated information.

Category	Required Provision	Applies to Tier	Status	Gap Notes / Fallback
Access Control	Vendor must implement role-based access control limiting system access to authorized personnel with a legitimate need.	1	[ ] Met [ ] Gap [ ] N/A	
Access Control	Multi-factor authentication (MFA) required for all remote access and privileged accounts accessing organizational data.	1	[ ] Met [ ] Gap [ ] N/A	Non-negotiable for Tier 1
Access Control	Access rights must be reviewed and recertified at least annually; terminated employee access revoked within 24 hours.	1	[ ] Met [ ] Gap [ ] N/A	
Access Control	Privileged access activities must be logged and audit logs retained for a minimum of 12 months.	1-2	[ ] Met [ ] Gap [ ] N/A	
Encryption	Data at rest encrypted using AES-256 or equivalent.	1	[ ] Met [ ] Gap [ ] N/A	
Encryption	Data in transit encrypted using TLS 1.2 or higher.	1	[ ] Met [ ] Gap [ ] N/A	
Encryption	Vendor must notify organization of any changes to encryption standards prior to implementation.	1-2	[ ] Met [ ] Gap [ ] N/A	
Vulnerability Mgmt	Quarterly vulnerability scans for systems handling organizational data; critical findings remediated within 30 days.	1-2	[ ] Met [ ] Gap [ ] N/A	
Vulnerability Mgmt	Annual third-party penetration testing; results and remediation status shared with organization upon request.	1-2	[ ] Met [ ] Gap [ ] N/A	Pentest summary acceptable for Tier 2
Vulnerability Mgmt	Patch management policy with defined SLAs: Critical 14 days, High 30 days, Medium 90 days.	1	[ ] Met [ ] Gap [ ] N/A	Negotiate SLAs for Tier 2
Incident Response	Vendor must notify organization within 72 hours of confirmed or suspected security	1	[ ] Met [ ] Gap [ ] N/A	Non-negotiable

Category	Required Provision	Applies to Tier	Status	Gap Notes / Fallback
	incident affecting organizational data.			
Incident Response	Incident notification must include: nature of incident, data types affected, estimated scope, containment measures, and remediation plan.	1	[ ] Met [ ] Gap [ ] N/A	
Incident Response	Vendor must cooperate with organization's investigation and provide forensic evidence upon written request.	1	[ ] Met [ ] Gap [ ] N/A	
Incident Response	Vendor must maintain a documented Incident Response Plan tested at least annually.	1-2	[ ] Met [ ] Gap [ ] N/A	
Business Continuity	Vendor must maintain a documented Business Continuity Plan covering service disruption scenarios.	1-2	[ ] Met [ ] Gap [ ] N/A	
Business Continuity	Recovery Time Objective (RTO) and Recovery Point Objective (RPO) must be specified for services provided.	1	[ ] Met [ ] Gap [ ] N/A	
Business Continuity	BCP must be tested at least annually; results available to organization upon request.	1	[ ] Met [ ] Gap [ ] N/A	
Subprocessors	Vendor must maintain a current list of subprocessors with access to organizational data.	1-2	[ ] Met [ ] Gap [ ] N/A	
Subprocessors	Prior written approval required before engaging new subprocessors for Tier 1 vendors.	1 only	[ ] Met [ ] Gap [ ] N/A	Advance notification acceptable for Tier 2
Subprocessors	Subprocessors must be bound by equivalent security obligations through contractual flow-down.	1	[ ] Met [ ] Gap [ ] N/A	
Audit Rights	Organization has right to audit vendor security controls, including on-site or virtual walk-through, with reasonable advance notice.	1	[ ] Met [ ] Gap [ ] N/A	Annual audit right minimum
Audit Rights	Vendor must provide current SOC 2 Type II or equivalent third-party assessment report annually.	1-2	[ ] Met [ ] Gap [ ] N/A	
Audit Rights	Vendor must notify organization of material findings in security assessments or regulatory examinations within 30 days.	1-2	[ ] Met [ ] Gap [ ] N/A	
Data Lifecycle	Vendor must return or securely destroy all organizational data within 30 days of contract termination.	1	[ ] Met [ ] Gap [ ] N/A	
Data Lifecycle	Certificate of destruction must be provided upon request.	1-2	[ ] Met [ ] Gap [ ] N/A	
Data Lifecycle	Vendor must maintain documented data retention schedules aligned with organizational policy.	1-2	[ ] Met [ ] Gap [ ] N/A	
Termination	Organization has right to terminate for cause upon material breach, with defined cure period (typically 30 days).	1	[ ] Met [ ] Gap [ ] N/A	

Category	Required Provision	Applies to Tier	Status	Gap Notes / Fallback
Termination	Organization has right to terminate for convenience with defined notice period.	1	[ ] Met [ ] Gap [ ] N/A	
Termination	Transition assistance obligations must be specified: minimum 90 days for Tier 1 vendors.	1 only	[ ] Met [ ] Gap [ ] N/A	

PART 2: DATA PROTECTION AGREEMENT (DPA) REVIEW CHECKLIST

A DPA is necessary when the vendor processes personal data on behalf of the organization as a data processor. Under GDPR (Art. 28) and similar regulations, certain provisions are required. This checklist covers GDPR-compliant DPA requirements as a baseline; additional requirements may apply under CCPA, HIPAA, and other relevant regulations.

Category	Required Provision	Applies to Tier	Status	Gap Notes / Fallback
Processing Instructions	DPA must specify that vendor processes personal data only on documented instructions of the organization.	1	[ ] Met [ ] Gap [ ] N/A	GDPR Art. 28(3)(a) - mandatory
Processing Instructions	Scope of permitted processing must be documented: purpose, data types, subject categories, duration, and geographic scope.	1	[ ] Met [ ] Gap [ ] N/A	
Processing Instructions	Vendor must notify organization if it believes an instruction infringes applicable data protection law.	1	[ ] Met [ ] Gap [ ] N/A	GDPR Art. 28(3)(h)
Confidentiality	Vendor must ensure authorized persons processing personal data are bound by appropriate confidentiality obligations.	1	[ ] Met [ ] Gap [ ] N/A	GDPR Art. 28(3)(b)
Security	Vendor must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.	1	[ ] Met [ ] Gap [ ] N/A	GDPR Art. 32
Security	DPA must specify security measures: pseudonymization, encryption, availability/resilience, restoration capabilities, testing.	1	[ ] Met [ ] Gap [ ] N/A	
Data Subject Rights	Vendor must assist organization in responding to data subject requests (access, erasure, portability, objection, correction).	1	[ ] Met [ ] Gap [ ] N/A	GDPR Art. 28(3)(e)
Data Subject Rights	Response assistance must be provided within timeframe allowing organization to meet statutory deadlines.	1	[ ] Met [ ] Gap [ ] N/A	GDPR requires 30-day response
Breach Notification	Vendor must notify organization of personal data breach without undue delay, and in any event within 72 hours of becoming aware.	1	[ ] Met [ ] Gap [ ] N/A	GDPR Art. 33 - mandatory
Breach Notification	Breach notification must include: nature of breach, categories and number of data subjects, categories and number of records, likely consequences, and measures taken.	1	[ ] Met [ ] Gap [ ] N/A	
DPIAs	Vendor must assist organization with Data Protection Impact Assessments (DPIAs) where required by applicable law.	1	[ ] Met [ ] Gap [ ] N/A	GDPR Art. 28(3)(f)
DPIAs	Vendor must notify organization prior to any processing activity likely to result in high risk to data subjects.	1-2	[ ] Met [ ] Gap [ ] N/A	
Subprocessors	DPA must specify whether general or specific authorization model applies for subprocessor engagement.	1	[ ] Met [ ] Gap [ ] N/A	Tier 1: specific authorization preferred

Category	Required Provision	Applies to Tier	Status	Gap Notes / Fallback
Subprocessors	Vendor must impose equivalent data protection obligations on subprocessors by contract.	1	[ ] Met [ ] Gap [ ] N/A	GDPR Art. 28(4) - mandatory
Subprocessors	Vendor remains fully liable for subprocessor compliance with DPA obligations.	1	[ ] Met [ ] Gap [ ] N/A	GDPR Art. 28(4)
Subprocessors	DPA must include or reference current subprocessor list with processing locations.	1-2	[ ] Met [ ] Gap [ ] N/A	
Cross-Border Transfers	DPA must identify all countries or regions where personal data will be processed or stored.	1	[ ] Met [ ] Gap [ ] N/A	
Cross-Border Transfers	For EU data transferred outside EEA: valid transfer mechanism documented (SCCs, adequacy decision, BCRs, etc.).	1	[ ] Met [ ] Gap [ ] N/A	GDPR Chapter V - mandatory for EU data
Cross-Border Transfers	Standard Contractual Clauses (SCCs) must reference 2021 EU SCCs (not the superseded 2010 versions).	1	[ ] Met [ ] Gap [ ] N/A	
Audit Rights	DPA must grant organization right to conduct audits or inspections of vendor's data processing activities.	1	[ ] Met [ ] Gap [ ] N/A	GDPR Art. 28(3)(h) - mandatory
Audit Rights	Vendor must make available all information necessary to demonstrate compliance with GDPR Art. 28 obligations.	1	[ ] Met [ ] Gap [ ] N/A	
Data Deletion	DPA must require return or deletion of all personal data at choice of organization at contract end.	1	[ ] Met [ ] Gap [ ] N/A	GDPR Art. 28(3)(g) - mandatory
Data Deletion	Vendor must confirm in writing when deletion is complete, with method of deletion documented.	1	[ ] Met [ ] Gap [ ] N/A	

PART 3: AI GOVERNANCE CONTRACT PROVISIONS CHECKLIST

Use this checklist when the vendor offers AI-enabled services or will process organizational data through AI systems. These provisions supplement the ISA and DPA.

Category	Required Provision	Applies to Tier	Status	Gap Notes / Fallback
Data Use	Explicit prohibition on using organizational data to train or fine-tune AI models without prior written consent.	1	[ ] Met [ ] Gap [ ] N/A	Non-negotiable
Data Use	Vendor must document all AI systems that process organizational data, including training data sources and model architectures.	1	[ ] Met [ ] Gap [ ] N/A	
Transparency	Vendor must provide model documentation (model card or equivalent) describing AI system purpose, capabilities, and limitations.	1	[ ] Met [ ] Gap [ ] N/A	
Transparency	Vendor must disclose when AI-generated outputs are used in service delivery and the basis for those outputs.	1-2	[ ] Met [ ] Gap [ ] N/A	
Accuracy & Bias	Vendor must conduct and document bias and fairness assessments prior to deployment and at defined intervals.	1	[ ] Met [ ] Gap [ ] N/A	
Accuracy & Bias	Vendor must notify organization of material changes to AI model performance, accuracy, or fairness characteristics.	1	[ ] Met [ ] Gap [ ] N/A	Material = >10% change in key metrics or introduction of new bias patterns
Human Oversight	Vendor must support organization's right to human review of AI-driven decisions affecting the organization or its customers.	1	[ ] Met [ ] Gap [ ] N/A	Required for high-risk AI under EU AI Act
Human Oversight	Vendor must document the human oversight mechanisms in place for high-risk AI systems.	1 only	[ ] Met [ ] Gap [ ] N/A	
Monitoring	Vendor must monitor AI systems in production for performance drift, degradation, and fairness metric changes.	1	[ ] Met [ ] Gap [ ] N/A	
Monitoring	Vendor must notify organization of AI system incidents (material accuracy degradation, bias discoveries, regulatory findings) within 30 days.	1	[ ] Met [ ] Gap [ ] N/A	
Regulatory	Vendor must cooperate with organization's compliance obligations under applicable AI regulations (EU AI Act, NIST AI RMF, OMB M-24-10, etc.).	1	[ ] Met [ ] Gap [ ] N/A	
Regulatory	Vendor must provide documentation required for organization's fundamental rights impact assessments or AI use case inventories.	1	[ ] Met [ ] Gap [ ] N/A	

CONTRACT REVIEW SIGN-OFF

Vendor Name	
Contract / Agreement Reference	
Review Date	
Reviewed By (TPRM)	
Reviewed By (Legal)	
Open Gaps Requiring Risk Acceptance	
Overall Contract Approval Status	[ ] Approved [ ] Approved with Risk Acceptance [ ] Requires Renegotiation [ ] Rejected