

# VENDOR CONTRACT RISK ASSESSMENT

## DataFlow Solutions, Inc. - Master Services Agreement

Assessment Date: January 10, 2026 | Prepared by: Legal Risk Management  
Risk Level: MEDIUM-HIGH (Original) → LOW-MEDIUM (With Proposed Changes)

### EXECUTIVE SUMMARY

This assessment evaluates the legal and business risks associated with the proposed Master Services Agreement with DataFlow Solutions. The original contract presented significant exposure in liability, indemnification, and intellectual property areas. Our proposed redlines address these concerns and bring the agreement to acceptable risk levels.

### RISK MATRIX

Risk Area	Original Risk	Mitigated Risk	Residual Concerns
Liability Exposure	HIGH	MEDIUM	Cap still allows significant exposure in breach scenarios
IP Ownership	HIGH	LOW	Clear ownership; ML prohibition addresses modern concerns
Indemnification	HIGH	LOW	Vendor now bears appropriate data handling risk
Data Security	MEDIUM	LOW	SOC 2 requirement and audit rights provide assurance
Insurance Coverage	MEDIUM	LOW	Increased limits align with exposure
Termination Rights	MEDIUM	LOW	Asymmetric rights favor us appropriately
Regulatory Compliance	MEDIUM	LOW	Explicit CCPA/GDPR obligations

### DETAILED RISK ANALYSIS

#### 1. LIABILITY CAP ANALYSIS

**Original Language:** Mutual cap at 12 months of fees (est. \$480,000/year based on SOW)  
**Concern:** A single data breach could cost \$2-5M in notification, remediation, and regulatory fines. Customer class action settlements in similar cases have exceeded \$10M.  
**Our Position:** 3x cap for vendor (\$1.44M) provides meaningful deterrent while remaining insurable for them.  
**Fallback:** Could accept 2x if they push back hard, but not below that.

#### 2. INTELLECTUAL PROPERTY CONCERNS

**Original Language:** Standard work-for-hire with basic license to vendor tools

**Concern:** No protection against vendor using our data/customizations to train ML models that benefit competitors. No clear assignment of derivative works. License to vendor tools was non-transferable (problematic in M&A;).

**Our Position:** Explicit assignment language, derivative works inclusion, ML training prohibition, transferable license.

**Priority:** DEALBREAKER - Do not sign without these protections.

### **3. INDEMNIFICATION IMBALANCE**

**Original Language:** Mutual indemnification including customer indemnifying vendor for 'Customer Data' claims

**Concern:** If customer data causes harm while in vendor's custody, we should not bear that risk. This is backwards from appropriate risk allocation.

**Our Position:** Expanded vendor obligations (data breach, regulatory); narrowed ours to gross negligence only.

**Priority:** DEALBREAKER - The Customer Data indemnification must be removed.

### **4. DATA SECURITY REQUIREMENTS**

**Original Language:** 'Reasonable security measures' with 48-hour breach notification

**Concern:** 'Reasonable' is subjective and unenforceable. 48 hours may not meet regulatory requirements.

**Our Position:** SOC 2 Type II standard, 24-hour notification, annual audits, customer audit rights.

**Note:** DataFlow claims to be SOC 2 certified already, so this should not be controversial.

## **RECOMMENDATIONS**

1. **Proceed with negotiation** using our redlined version as the starting point.
2. **Hold firm** on liability cap (minimum 2x), IP protections, and indemnification scope.
3. **Concede if necessary** on payment terms, minor insurance adjustments, and confidentiality period.
4. **Walk away** if vendor will not accept IP ownership/ML prohibition or appropriate indemnification.
5. **Document** any deviations from our standard terms in the contract file for future reference.

---

Rachel Kim, Senior Corporate Counsel

Date: January 10, 2026