Data Liability Assessment

Tier 2 Full Opinion Report

Company:	Nexus Data Solutions	**Date:**	2026-01-14
File:	`customer_records_export.csv`	**Contact:**	legal@nexusdata.example.com
Records:	15,847	**SHA-256:**	`a3b5c7d9e1f2a4b6...`

Risk Assessment Summary

LQ Score

42.5

0 (High Risk) — 100 (Low Risk)

Estimated Liability

$847,250

Regulatory Risk Exposure (USD)

Risk Classification: **HIGH RISK**

Data Domains Detected

Domain	Present	Density
Identification Data	Yes	Moderate
Financial Data	No	—
Health Data	No	—
Location Data	Yes	High
Contact Data	Yes	High
Demographic Data	Yes	Moderate
Sensitive Beliefs	No	—
Credentials	No	—

Linkage Risk Profile

Linkage Category	Status
Demographic Combinations	Detected
Location Combinations	Detected
Health Combinations	Not Detected
Financial Patterns	Not Detected
Professional/Social Context	Detected

Linkage categories represent "toxic pairs and triplets" — combinations of quasi-identifiers that enable re-identification through the mosaic effect, even without direct identifiers.

Key Observations

- High density of contact data detected, representing the primary regulatory exposure in this dataset.
- 3 linkage categories detected, indicating elevated re-identification risk through the mosaic effect.
- Demographic and location data combination creates elevated re-identification risk. See: Linkage Risk.

Methodology Summary

The LQ Legal Risk Engine employs a multi-layer analysis framework:

1. **PII Detection Framework** — Structured detection hierarchy using header analysis, pattern matching, and NLP-based entity recognition to identify 70+ PII types with associated risk weights.
2. **Linkage Risk Analysis** — Evaluation of "toxic pairs" (quasi-identifier combinations) that enable re-identification even without direct identifiers. Based on established privacy research including the Mosaic Effect principle.
3. **Context-Adjusted Risk Calculation** — Base asset risk is amplified by contextual factors including regulatory jurisdiction, organizational profile, infraction history, and intended data use.
4. **Financial Liability Modeling** — Regulatory risk exposure is quantified using a sensitivity model calibrated to breach cost research and regulatory penalty frameworks.

For detailed methodology documentation: https://liabilityquant.com/methodology

Regulatory Compliance Reference

Risk Factor	Relevant Regulatory Frameworks
Direct Identifiers	GDPR Art. 4 (personal data definition), CCPA §1798.140 (personal information), PIPEDA
Sensitive/Special Category Data	GDPR Art. 9 (special categories), HIPAA (PHI), BIPA (biometrics), state genetic privacy laws
Linkage & Re-identification Risk	GDPR Recital 26 (identifiability standard), FTC Act §5 (unfair practices)
Data Processing Activities	GDPR Art. 6 (lawful basis), CCPA §1798.100 (disclosure requirements)
Minor/Child Data	COPPA (under 13), GDPR Art. 8 (child consent), state student privacy laws (FERPA)
Cross-Border Transfers	GDPR Chapter V, adequacy decisions, Standard Contractual Clauses

This mapping is provided as educational context. Consult qualified legal counsel for jurisdiction-specific compliance guidance.

Disclaimers & Limitations

This assessment provides **directional risk quantification** for due diligence, M&A valuations, and cyber insurance underwriting purposes.

- **Not Legal Advice.** This report is a quantitative risk assessment tool. It does not constitute legal advice and should not be relied upon as such. Consult qualified legal counsel for compliance guidance specific to your jurisdiction and circumstances.
- **Methodology Scope.** The LQ engine analyzes structured data files for PII patterns. Limitations include: unstructured text fields may not be fully scanned; contextual PII specific to niche industries may not be detected; obfuscated or encoded identifiers may not be recognized.
- **Liability Estimate.** The financial liability figure is a model-based estimate derived from regulatory risk analysis. Actual penalties depend on specific breach circumstances, regulatory discretion, cooperation efforts, and applicable case law.
- **Data Handling.** Liability Quant does not retain uploaded file contents. Only metadata (file hash, scores, session information) is stored for audit trail purposes per industry best practices.
- **Point-in-Time Assessment.** This report reflects the analyzed file as of the assessment date. Regular re-assessment is recommended as data and regulatory landscapes evolve.
