

Specimen — illustrative example

Solstice Grid Services is a fictional organisation. This document comes from the scenario described on riskwoven.com/examples, and is not an assessment of any real entity. It is advisory output to support your own decisions: not legal advice, not a certification, and not an audit.

Written and reviewed by RiskWoven.com. Written by RiskWoven.com's AI drafting agent and checked by RiskWoven.com's independent review stage before release. The review is automated. It is not a human, legal or audit review.

THIRD-PARTY AI VENDOR REVIEW

Lumen Forecast AI

Hosted load forecasting model

Reviewed 2026-09-16 (UTC) · 2 document types supplied · **4 to escalate**, 4 to review

Recommendation

Do not sign until the 4 escalated terms are changed or formally accepted by the contract owner. Resolve the 4 items marked for review before renewal at the latest. 3 requested documents were not provided, so their subjects remain unreviewed.

Eight findings arise from the review of Lumen Forecast AI's supplied documents. Severity labels reflect the reviewer's assessment of contractual risk exposure based on the supplied documents; no external severity framework was provided. One finding is critical: no audit evidence was provided and the terms contain no audit rights clause, leaving your organisation with no means of verifying Lumen's security controls. Two findings are high severity: Lumen reserves the right to use your aggregated telemetry for model improvement with no opt-out mechanism; and Lumen may add subprocessors on 30 days notice with no right of objection. One further high-severity finding concerns derived data: the supplied terms are silent on whether derivatives embedded in model weights are subject to the stated retention limit, and your organisation may have no means of requiring their removal. Four findings are medium severity: the 12-month post-term retention tail may conflict with data minimisation obligations; subprocessor locations are unconstrained, creating transfer risk despite Canada-based hosting; breach notification covers only personal data, leaving operational data incidents outside the clause; and the terms are silent on broader term change rights and on what remedies the customer would have. Before proceeding, your organisation should obtain Lumen's current subprocessor list and a valid audit report, seek a contractual opt-out from telemetry use for model training, and negotiate an objection right

on subprocessor changes. The supplier contracts should be checked for any deletion-on-request and data return provisions, which the supplied terms do not address.

Not provided — these subjects are unreviewed, not clear

- Independent audit report (SOC 2 Type II, ISO 27001 certificate)
- Subprocessor list
- Security documentation or whitepaper

Findings

Customer data used to train vendor models · High · Escalate

Lumen's AI-specific terms state that Lumen may use aggregated customer telemetry to improve its forecasting models. The terms do not state whether this is opt-in or opt-out, nor do they define what qualifies as aggregated telemetry.

Load forecasting telemetry from your organisation's operations may carry commercially sensitive consumption patterns. Because the terms do not make this opt-out — let alone opt-in — your data could be used to improve a model that also serves your competitors, with no mechanism for you to prevent it. Note: severity labels in this report reflect the reviewer's assessment of contractual risk exposure based on the supplied documents; no external severity framework was provided.

Ask the vendor: Ask for a clause that prohibits training or model improvement on your content unless you opt in, in writing.

Found at: AI-specific terms, sentence 1

Answers to: **ISO/IEC 42001 A.7.3** Document how data used in AI systems is acquired and selected.; **ISO/IEC 42001 A.7.5** Maintain a documented process for tracking the provenance of data used in AI systems across both the data's and the system's life cycles.; **ISO/IEC 27001 A.5.34** Identify and satisfy privacy and PII-protection requirements arising from applicable law, regulation, and contract.; **ISO/IEC 27001 A.5.20** Agree relevant information security requirements with each supplier, scaled to the type of relationship involved.

Derived or de-identified data · High · Escalate

The AI-specific terms permit use of aggregated customer telemetry for model improvement but do not define aggregation thresholds, de-identification standards, or whether Lumen retains derived data beyond the agreement term.

If Lumen embeds your operational patterns into its model weights, those derivatives may not be subject to the 12-month post-term retention limit that applies to raw customer data, as the supplied terms are silent on derivative retention. Your organisation may have no practical means of requiring their removal.

Ask the vendor: Ask for derived and de-identified data to be covered by the same retention and use limits as your content.

Found at: AI-specific terms, sentence 1

Answers to: **ISO/IEC 42001 A.7.5** Maintain a documented process for tracking the provenance of data used in AI systems across both the data's and the system's life cycles.; **ISO/IEC 27001 A.8.10** Delete information held in systems, devices, or any other storage media once it is no longer required.; **ISO/IEC 27001 A.5.34** Identify and satisfy privacy and PII-protection requirements arising from applicable law, regulation, and contract.

Retention of customer content · Medium · Review

Lumen's AI-specific terms state that customer data is retained for the term of the agreement plus 12 months. The terms do not address whether the customer may request earlier deletion, nor what categories of data the retention period covers.

A fixed 12-month tail after contract end means your operational data remains in Lumen's environment after you have moved to another supplier. If your organisation is subject to data minimisation obligations, this automatic retention period may conflict with them and would need to be accepted as a deliberate exception.

Ask the vendor: Ask for a fixed retention period for prompts, uploads, outputs and logs, and deletion on request within a stated time.

Found at: AI-specific terms, sentence 2

Answers to: **ISO/IEC 27001 A.8.10** Delete information held in systems, devices, or any other storage media once it is no longer required.; **ISO/IEC 27001 A.5.33** Protect records against loss, destruction, falsification, unauthorized access, and unauthorized release.; **ISO/IEC 42001 A.7.2** Define, document, and implement data management processes that support AI system development.

Subprocessors and supply chain · High · Escalate

Lumen's AI-specific terms state that Lumen may engage subprocessors with 30 days notice. The terms do not grant the customer a right to object, and no subprocessor list was supplied.

Because no subprocessor list was provided, your organisation cannot assess who currently processes your load forecasting data or where. The 30-day notice period is informational

only if there is no corresponding right to object, meaning Lumen can expand its subprocessor chain without your agreement.

Ask the vendor: Ask for the current subprocessor list, advance notice of changes, and a right to object.

Found at: AI-specific terms, sentence 3

Answers to: **ISO/IEC 27001 A.5.21** Define and implement processes for managing information security risk across the ICT products and services supply chain.; **ISO/IEC 27001 A.5.19** Define and implement processes for managing the information security risks that come with using suppliers' products or services.; **ISO/IEC 27001 A.5.22** Monitor, review, and evaluate suppliers' security practices and service delivery on an ongoing basis, and manage changes to them.

Processing locations and transfers · Medium · Review

Lumen's data processing terms state that data is hosted in Canada. The terms do not address whether subprocessors may process data in other jurisdictions, nor whether Lumen may change the hosting location.

Canada is confirmed as the primary hosting location, but because the subprocessor list was not provided and the terms do not restrict subprocessor locations, data could flow to jurisdictions with different adequacy status without your organisation being informed in advance.

Ask the vendor: Ask for the processing and storage locations in the contract, and notice before either changes.

Found at: Data processing terms, sentence 1

Answers to: **ISO/IEC 27001 A.5.14** Put transfer rules, procedures, or agreements in place covering every type of information transfer — internal to the organization and between the organization and outside parties.; **ISO/IEC 27001 A.5.34** Identify and satisfy privacy and PII-protection requirements arising from applicable law, regulation, and contract.; **ISO/IEC 27001 A.5.23** Establish processes for acquiring, using, managing, and exiting cloud services that satisfy the organization's information security requirements.

Unilateral change of terms · Medium · Review

Lumen's AI-specific terms permit engagement of new subprocessors on 30 days notice with no stated right of objection or exit. The supplied terms do not address Lumen's right to change other terms, model behaviour, or hosting locations.

The absence of an objection right on subprocessor changes, combined with silence on broader term changes, means Lumen can materially alter the conditions under which your

data is processed. The supplied terms do not address what remedies or exit rights the customer would have in such circumstances.

Ask the vendor: Ask for advance written notice of material changes and a right to terminate without penalty if you do not accept them.

Found at: AI-specific terms, sentence 3

Answers to: **ISO/IEC 27001 A.5.20** Agree relevant information security requirements with each supplier, scaled to the type of relationship involved.; **ISO/IEC 27001 A.5.22** Monitor, review, and evaluate suppliers' security practices and service delivery on an ongoing basis, and manage changes to them.; **ISO/IEC 27001 A.5.23** Establish processes for acquiring, using, managing, and exiting cloud services that satisfy the organization's information security requirements.

Incident and breach notification · Medium · Review

Lumen's data processing terms state that Lumen notifies the customer of a personal data breach without undue delay. The terms do not specify a maximum notification period, define what constitutes a breach, or address notification of security incidents that do not involve personal data.

Load forecasting data may include operational data that is not personal data. A breach of that data would not trigger the notification clause as written, leaving your organisation without contractual visibility of incidents affecting its operational information.

Ask the vendor: Ask for notice of any incident affecting your data within a fixed number of hours, with no conditions that delay the clock.

Found at: Data processing terms, sentence 2

Answers to: **ISO/IEC 27001 A.5.24** Plan and prepare for information security incidents by defining, establishing, and communicating incident management processes along with the associated roles and responsibilities.; **ISO/IEC 27001 A.5.25** Assess information security events and decide which ones qualify as information security incidents.; **ISO/IEC 27001 A.5.26** Respond to information security incidents following the documented procedures.; **ISO/IEC 27001 A.5.20** Agree relevant information security requirements with each supplier, scaled to the type of relationship involved.

Audit evidence and assurance · Critical · Escalate

No independent audit report, SOC 2 Type II report, or ISO 27001 certificate was provided. The supplied terms do not include an audit rights clause or an obligation on Lumen to provide assurance evidence on request.

Without audit evidence, your organisation cannot assess whether Lumen's controls over your load forecasting data meet any baseline standard. The absence of both third-party assurance documents and a contractual audit rights clause represents a significant gap in

vendor oversight. Note: severity labels in this report reflect the reviewer's assessment of contractual risk exposure based on the supplied documents; no external severity framework was provided.

Ask the vendor: Ask for a current independent assurance report (for example SOC 2 Type II or an ISO/IEC 27001 certificate) or a right to audit.

Found at: Not addressed in supplied documents

Answers to: **ISO/IEC 27001 A.5.22** Monitor, review, and evaluate suppliers' security practices and service delivery on an ongoing basis, and manage changes to them.; **ISO/IEC 27001 A.5.19** Define and implement processes for managing the information security risks that come with using suppliers' products or services.; **ISO/IEC 42001 A.10.3** Maintain a process confirming that AI-related services, products, and materials sourced from suppliers are consistent with the organization's own responsible-AI approach before they're adopted.

Documents supplied: Data processing agreement or terms; AI-specific terms (model training, inference, retention)

Written and reviewed by RiskWoven.com. Written by RiskWoven.com's AI drafting agent and checked by RiskWoven.com's independent review stage before release. The review is automated. It is not a human, legal or audit review. Produced from the documents you supplied. It reports what those documents commit the vendor to. It is not legal advice and it does not clear the vendor.

Questions about anything in this review: hello@riskwoven.com