TRUST CENTRE

Subprocessor & Third-Party Services Policy

SUPPLY-CHAIN TRANSPARENCY AND SERVICE-PROVIDER GOVERNANCE

Effective Date: 6 October 2025

Classification: Public

This document is intended for public distribution. Supporting assurance evidence may be subject to separate access and confidentiality restrictions.

Contents

This policy should be read together with the applicable customer agreement, order, service schedule and data-protection terms.

1. Overview

This policy explains how PCL One identifies, assesses, contracts with and discloses third-party service providers that may process customer data in support of PCL One services. The public register below is intentionally scoped: a customer-specific subprocessor schedule should identify only providers that actually process customer data for the subscribed service.

> **POLICY STATUS**
> This is a public baseline policy. Service-specific commitments are governed by the applicable agreement, order, service schedule and data-protection terms.

2. Scope and applicability

Applies to subprocessors and material third-party service providers used in the delivery of PCL One cloud services.

Covers provider due diligence, contractual safeguards, access limitations, change notification and customer-specific disclosure.

Provider applicability may vary by product, architecture, customer geography and enabled features.

Relationship to customer agreements

The governing agreement and data-protection terms control any customer-specific notice period, objection process or additional provider restrictions. The public register should not be read as confirmation that every listed provider processes data for every customer.

3. Definitions

Term	Meaning
Subprocessor	A third party engaged by PCL One to process customer personal data on PCL One's behalf in connection with the contracted service.
Third-Party Service Provider	A supplier or service provider that supports delivery or operation of a PCL One service. Not every provider is necessarily a subprocessor for every customer.
Material Change	The addition or replacement of a provider in a role that materially changes how customer data is processed, stored or accessed.
Customer-Specific Schedule	The record identifying providers actually applicable to a particular subscribed service, including purpose and processing location where relevant.

4. Public service-provider register

Provider	Service purpose	Customer-data treatment	Applicability
Microsoft Azure	Cloud infrastructure, networking, storage, backup and recovery services for the municipal cloud baseline.	Customer data may be hosted or processed where Azure is selected. Canada-only municipal deployments use approved Canadian regions documented for the service.	Applicable where selected for hosting.
MongoDB	Database technology or managed database service used by selected PCL One architectures.	Applies only where included in the subscribed service design. Processing scope and location are documented for the service.	Conditional - architecture dependent.

Provider	Service purpose	Customer-data treatment	Applicability
OpenAI	AI service provider for specifically approved AI-assisted capabilities where enabled.	Used only for approved use cases. Customer data is not used to train generalized or shared models through the contracted PCL One service. AI capabilities may be restricted or disabled according to service design.	Conditional - feature dependent.

The register above identifies services that may support PCL One's cloud environment. Before production use, the customer-specific schedule should confirm the providers that actually process customer data for the subscribed service, their purpose and relevant processing location.

5. Provider governance and change notification

Security, privacy, confidentiality and service-dependency risks are assessed before a provider is used for customer processing.

Written contractual obligations are flowed down to the provider appropriate to its role and the sensitivity of the data involved.

Provider access to customer data is limited to the minimum necessary, role-controlled and logged where access is required.

PCL One remains responsible for its contractual obligations to the customer when subprocessors are used.

PCL One provides advance written notice of a material subprocessor change before processing begins where practicable and in accordance with the governing contract.

A customer may raise a reasonable data-protection objection under the process defined in the applicable data-protection terms; PCL One will work in good faith to mitigate the concern or identify a practical alternative where feasible.

Customer-specific register content

Field	Recorded information
Provider	Legal or service-provider name.
Purpose	Service function performed.
Data categories	Types of customer data processed, where applicable.
Location	Approved processing/storage region or jurisdiction where relevant.
Access model	Whether provider personnel may access customer data and under what controls.
Change date	Date added, changed or removed from the customer schedule.

6. Customer responsibilities

Review material subprocessor notices and raise any permitted objection within the timeframe stated in the applicable data-protection terms.

Identify customer-specific residency, industry or regulatory constraints before service design is finalized.

Avoid treating the public register as the complete list for a specific service; use the customer-specific schedule for contractual applicability.

7. Exceptions and exclusions

Providers that do not process customer data may fall outside the definition of subprocessor even if they support PCL One business operations.

Provider names, products or legal entities may change through normal supplier reorganization or service evolution; material changes are handled under the applicable notification process.

A provider may be excluded, disabled or replaced for a particular customer where the service architecture and contract support that configuration.

8. Assurance and evidence

PCL One maintains records supporting the operation of this policy. Detailed security evidence is not necessarily public and may be provided to eligible customers, prospective customers, business partners or regulators through controlled due diligence, subject to applicable report-use and confidentiality restrictions.

Customer-specific subprocessor schedule.

Provider due-diligence and risk-assessment records.

Applicable contractual security, confidentiality and privacy clauses.

Material-change notification records.

Relevant provider assurance reports or certifications where available and subject to confidentiality.

PCL One maintains a SOC 2 Type 2 report covering controls relevant to Security, Confidentiality and Availability within the scope of that report. The full report is restricted-use assurance evidence and is not incorporated into this public policy by publication.

9. Statement of changes

Effective date	Summary
6 October 2025	Initial publication of this policy.