

TRUST CENTRE

Data Residency & Location Policy

DATA LOCATION, RESIDENCY, CROSS-BORDER PROCESSING AND SERVICE PROVIDER GOVERNANCE**Effective Date:** 6 October 2025**Classification:** Public**Document ID:** PCL-TRUST-RES-008

This document is intended for public distribution. Detailed infrastructure diagrams, exact provider configuration, internal access paths, customer-specific data-flow maps, operational logs and other sensitive implementation evidence are restricted and may be provided separately to eligible customers, auditors or regulators subject to appropriate access and confidentiality restrictions.

Contents

This policy should be read together with the PCL One Data Processing Addendum, Cloud Hosting & Delivery Policy, Cloud Service Description, Subprocessor & Third-Party Services Policy, Data Retention, Backup & Secure Disposal Policy, Privileged Support & Emergency Access Policy and the applicable customer agreement or Ordering Document.

01	Overview
02	Scope and applicability
03	Residency principles
04	Service regions and contracted residency model
05	Canada-only municipal deployments
06	Production, backups and disaster recovery
07	Non-production and testing data
08	Support and administrative access
09	Subprocessors and third-party services
10	Operational metadata and service telemetry
11	Integrations, exports and customer-directed transfers
12	Cross-border transfers and legal requirements
13	Changes to location or providers
14	Customer responsibilities
15	Assurance, exceptions and related documents
16	Statement of changes

1. Overview

PCL One provides cloud services using approved hosting and service-provider architectures selected for the subscribed service. Where a customer agreement includes a data-residency or localization requirement, PCL One configures and operates the service according to the residency model identified in the applicable Ordering Document, Service Schedule or approved service design.

Public baseline

Where the applicable Order adopts the PCL One Canada-only municipal residency model, production Customer Data, backups and recovery copies remain within the approved Canadian residency model, subject to the documented service architecture and any expressly approved customer-specific exception.

2. Scope and applicability

This policy applies to PCL One-managed cloud services and the handling of Customer Data across production hosting, backup, recovery, non-production environments, support operations and third-party service relationships where PCL One controls or governs processing location.

- Customer-managed systems, endpoints, local exports and customer-selected third-party integrations remain subject to the customer's own location and transfer decisions unless expressly included in the subscribed service.
- A service-specific or customer-specific residency term in an agreement, Order, Service Schedule, DPA or approved technical design takes precedence over this public baseline where it is more specific.
- This policy distinguishes Customer Data from operational metadata, account information and provider telemetry because different technical and contractual rules may apply to those categories.

3. Residency principles

- Document the approved residency model before production configuration when a contractual location requirement applies.
- Keep Customer Data within the contracted residency model unless the Customer authorizes another location, the applicable agreement permits it, or applicable law requires otherwise.
- Use geographically separate locations within the approved residency model for redundancy, backup and recovery when the service architecture requires it.
- Limit location changes to controlled, assessed changes that consider security, privacy, continuity and contractual obligations.
- Maintain provider and subprocessor governance so the location and purpose of material processing can be identified when required.
- Use data minimization, masking or synthetic data where feasible to reduce unnecessary movement of production information.

4. Service regions and contracted residency model

The applicable Order or Service Schedule identifies the hosting region or residency model when a regional commitment applies. A residency commitment may cover one or more data categories depending on the subscribed service and contract.

Data or processing category	Public baseline
Production Customer Data	Stored and processed within the approved residency model identified for the subscribed service where a contractual residency requirement applies.
Backups and recovery copies	Remain within the approved residency model when the contracted service includes a regional or country-specific commitment.
Non-production copies of Customer Data	Handled according to the same residency restriction unless the data is appropriately masked, synthetic, anonymized or otherwise excluded by the applicable service design.
Operational metadata and service telemetry	Governed by the service architecture, provider arrangements and applicable contract; customer-specific localization requirements are documented where they extend to these categories.

Data or processing category	Public baseline
Customer-directed exports or integrations	Transferred to the destination selected or configured by the Customer and thereafter subject to the Customer or receiving provider controls.

5. Canada-only municipal deployments

PCL One supports a Canada-only municipal residency model for subscribed services where that model is adopted by the applicable Order. Under that model, production Customer Data, backup copies and disaster-recovery copies remain within the approved Canadian residency architecture.

- Production and recovery capability may use geographically separate Canadian locations to support resilience and recovery objectives.
- PCL One does not intentionally relocate Customer Data outside the contracted Canadian residency model except where expressly authorized by the Customer, permitted by the governing agreement or required by law.
- Where a customer-specific commitment also restricts the geographic location of support access, that access restriction is documented and applied through the applicable service design or support arrangement.
- Exact cloud regions, service components and provider locations may be recorded in customer-specific technical documentation when required for regulatory or procurement purposes.

6. Production, backups and disaster recovery

Residency controls apply across the lifecycle of covered Customer Data. Backup and recovery architecture is designed so that regional resilience does not silently defeat an agreed localization requirement.

- Backup copies containing Customer Data are encrypted and access-controlled in accordance with PCL One security and backup policies.
- Recovery copies are maintained in locations consistent with the approved residency model for the subscribed service.
- RTO and RPO commitments govern recovery objectives; they do not by themselves authorize transfer of Customer Data outside an agreed residency model.
- Retention and deletion of backup data are governed by the Data Retention, Backup & Secure Disposal Policy and any customer-specific schedule.

7. Non-production and testing data

PCL One seeks to minimize the use of identifiable production Customer Data in development, quality assurance and testing activities. Where production-derived data is required for an approved operational purpose, access, masking, residency and retention controls are applied according to the sensitivity of the data and the applicable service commitment.

- Synthetic, masked or de-identified test data is preferred where it can meet the testing objective.
- Non-production environments that contain Customer Data are included in the applicable residency restriction when required by the customer agreement or service design.
- Copies created for troubleshooting or migration are limited to the minimum necessary data and removed when the approved purpose is complete, subject to legal or contractual retention requirements.

8. Support and administrative access

Data residency and personnel access location are related but distinct controls. PCL One manages privileged support access under named identities, MFA, least privilege, approval, logging and time-bound elevation where supported.

Access-location commitments

Where the governing customer agreement requires Customer Data to be accessed only from a specified country or region, PCL One applies that restriction to the applicable support model. Otherwise, authorized remote administrative access is governed by the contracted service design, DPA and Privileged Support & Emergency Access Policy.

9. Subprocessors and third-party services

PCL One may rely on approved infrastructure, database, AI, communications or other service providers to deliver portions of the subscribed service. Provider use is governed through due diligence, contractual safeguards, security review and the PCL One subprocessor governance process.

- The public Subprocessor & Third-Party Services Policy identifies providers that may support PCL One services; a customer-specific schedule may identify the providers actually applicable to a subscribed service.
- Where residency is contractually restricted, PCL One selects and configures providers so covered Customer Data is processed consistently with the agreed model, subject to documented exceptions.
- A provider's corporate location does not by itself determine the storage location of Customer Data; the relevant service region, processing configuration and data flow are considered together.

10. Operational metadata and service telemetry

Cloud services generate operational records such as authentication events, service health data, security alerts, usage metrics, support records and configuration telemetry. These records are managed according to their purpose, sensitivity, contractual treatment and the capabilities of the relevant platform.

- PCL One minimizes inclusion of Customer Data in operational telemetry where feasible.
- Customer-specific requirements that extend localization obligations to defined metadata or logs are documented in the applicable Order, DPA, Service Schedule or technical design.
- Security and diagnostic information may be retained separately from primary application data when required for monitoring, incident response, forensic investigation or service reliability.

11. Integrations, exports and customer-directed transfers

A Customer may configure integrations, exports, APIs, file transfers or downstream applications that move information to systems outside the PCL One-managed service boundary. Such customer-directed movement is not treated as a PCL One relocation of the hosting environment.

- The Customer is responsible for approving destinations, credentials, recipients and legal transfer conditions for customer-controlled integrations.
- PCL One uses encrypted transport for supported outbound connections where PCL One controls the connection and the receiving endpoint supports secure transport.
- Where PCL One implements an integration as part of professional services, the agreed data flow and destination are documented during design and configuration.

12. Cross-border transfers and legal requirements

PCL One does not intentionally transfer Customer Personal Data outside an expressly contracted residency model except where the Customer authorizes the transfer, the applicable agreement permits it, an approved service-provider arrangement requires it, or applicable law requires it. Where data-protection law requires a transfer mechanism or additional safeguards, those requirements are addressed through the DPA or applicable transfer schedule.

- Government or law-enforcement requests are handled according to applicable law and contractual obligations.
- Where legally permitted, PCL One seeks to direct requests for Customer Data to the Customer when the Customer is the appropriate responding party.
- Emergency or legally compelled processing does not create a standing authorization to change the contracted residency model.

13. Changes to location or providers

Material changes to hosting architecture, service providers or processing locations are assessed before production use for security, privacy, resilience, contractual and residency impact.

- PCL One uses change-management controls for material provider or architecture changes.
- Where the applicable agreement requires notice, approval or a defined objection process for subprocessor or location changes, PCL One follows that process.
- Policy or architecture updates will not be used to silently remove a customer-specific residency commitment documented in a current Order or Service Schedule.

14. Customer responsibilities

- Identify residency, localization, access-location and regulatory requirements before production deployment and keep those requirements current.
- Classify the information placed into the service and determine whether the subscribed service and residency model are appropriate for that information.
- Review customer-controlled integrations, exports, support attachments and downstream destinations for cross-border transfer implications.

- Maintain lawful authority to provide Customer Data to PCL One and instruct processing under the applicable agreement and DPA.
- Notify PCL One before materially changing a requirement that affects service region, provider selection, recovery design or support model.

15. Assurance, exceptions and related documents

PCL One maintains evidence supporting the operation of relevant hosting, access, backup, provider and change-management controls. Detailed architecture diagrams, customer-specific data-flow maps, provider configurations and audit evidence are restricted because they may contain sensitive security or customer information.

Document	Relationship
PCL One Data Processing Addendum	Processing instructions, data-protection roles, subprocessors, international transfers and Customer Personal Data.
PCL One Cloud Hosting & Delivery Policy	Hosting, service regions, platform operations, backup, recovery and change management.
PCL One Cloud Service Description	Subscribed service scope, environments, regions, boundaries and service-specific objectives.
PCL One Subprocessor & Third-Party Services Policy	Provider register, governance and service-specific applicability.
PCL One Privileged Support & Emergency Access Policy	Support access, privileged administration and emergency access controls.
PCL One Data Retention, Backup & Secure Disposal Policy	Retention, backup, recovery copies, termination handling and secure disposal.

Exceptions

Any exception to a contracted residency or access-location commitment requires documented approval under the applicable contractual and governance process. A technical workaround or operational convenience does not by itself override an agreed residency restriction.

16. Statement of changes

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

This public policy describes PCL One's baseline approach. The applicable Cloud Services Agreement, Ordering Document, Service Schedule, Data Processing Addendum and customer-specific technical design govern where they contain more specific commitments.