CONTRACTS & POLICIES

PCL One Data Processing Addendum

CUSTOMER PERSONAL DATA, PROCESSING AND DATA PROTECTION

Effective Date: 6 October 2025
Classification: Public
Document ID: PCL-CONTRACT-DPA-016

This Data Processing Addendum governs PCL One's processing of Customer Personal Data in connection with subscribed PCL One services. It is incorporated into the applicable Cloud Services Agreement, Ordering Document or other agreement that references it.

Contents

This Addendum should be read together with the applicable PCL One Cloud Services Agreement, Ordering Document, Cloud Service Description and referenced Trust Centre policies.

1. Overview

This Data Processing Addendum (the "Addendum") establishes the baseline data-protection terms that apply when PCL One processes Personal Data on behalf of a Customer in connection with the Services. It is designed to allocate responsibilities between the parties, define PCL One's permitted processing, establish security and incident-management obligations, and document how subprocessors, data-subject requests, transfers, retention and assurance are handled.

POLICY STATUS

This is a public baseline data-processing addendum. Customer-specific processing details, residency restrictions, transfer mechanisms, retention instructions and additional regulatory terms may be documented in the applicable Ordering Document, Service Schedule or jurisdiction-specific schedule.

2. Scope, precedence and roles

2.1 This Addendum applies to PCL One's Processing of Customer Personal Data in connection with the Services identified in the applicable agreement or Ordering Document.

2.2 Unless the applicable agreement expressly states otherwise, this Addendum remains in effect for the period during which PCL One Processes Customer Personal Data on the Customer's behalf, including any agreed transition or deletion period following termination.

2.3 If there is a conflict between this Addendum and the general terms of the Cloud Services Agreement concerning Processing of Customer Personal Data, this Addendum governs to the extent of that conflict. More specific customer terms in an Ordering Document, Service Schedule or jurisdiction-specific schedule govern where expressly stated.

2.4 Where the Customer determines the purposes and means of Processing, the Customer acts as Controller and PCL One acts as Processor. Where the Customer acts as Processor for another Controller, PCL One acts as the Customer's Subprocessor to the extent applicable to the Services.

2.5 Each party is responsible for its own obligations under Applicable Data Protection Law. The Customer is responsible for establishing a lawful basis, providing required notices, obtaining required consents where applicable, and determining whether the Services and configured Processing are appropriate for the Customer's legal and regulatory requirements.

3. Processing instructions and use limitations

3.1 PCL One will Process Customer Personal Data only on documented instructions from the Customer, including instructions reflected in the agreement, Ordering Document, Service Schedule, configured use of the Services, support requests and other written directions accepted by PCL One.

3.2 PCL One may Process Customer Personal Data as necessary to provide, secure, operate, support, maintain, monitor, back up, recover, configure, test and improve the contracted Services for the Customer, and to comply with applicable legal obligations.

3.3 PCL One will not sell Customer Personal Data, use it for unrelated advertising, or use it for generalized profiling unrelated to the contracted Services. Where an AI-assisted capability is enabled, its permitted use, data flow and provider applicability are governed by the subscribed service design and applicable data-protection terms.

3.4 If PCL One reasonably believes a Customer instruction violates Applicable Data Protection Law, PCL One may notify the Customer and suspend the affected Processing to the extent reasonably necessary while the parties work to resolve the issue, unless prohibited by law.

3.5 The Customer will not instruct PCL One to Process Personal Data that is not reasonably required for the subscribed Services or that the Customer is not authorized to provide.

4. Confidentiality and personnel controls

PCL One limits access to Customer Personal Data to personnel and approved service providers who require access for the contracted service, support, security, maintenance or incident-response purpose. Access is subject to confidentiality, authorization and security controls appropriate to the individual's role.

Control area	Baseline requirement
Confidentiality	Personnel with access to Customer Personal Data are subject to confidentiality obligations or equivalent duties appropriate to their role.
Named identities	Administrative and privileged access uses identities attributable to authorized individuals rather than unrestricted shared administrator credentials where the service architecture supports that model.
Least privilege	Access is limited to the role, environment and data scope necessary for the authorized task.

Control area	Baseline requirement
Strong authentication	Administrative access is protected by multi-factor authentication or equivalent strong authentication appropriate to the service architecture.
Time-bound access	Privileged elevation is temporary where supported and is removed or expires after the authorized task or access window.
Logging and review	Administrative activity is logged and material or emergency access is reviewable in accordance with the applicable service controls.

5. Security of processing

5.1 PCL One maintains technical and organizational measures designed to protect the confidentiality, integrity and availability of Customer Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access, taking into account the nature of the Services and the risks of the Processing.

5.2 The baseline measures are summarized in Annex B and supplemented by the PCL One Trust Centre policies applicable to the subscribed service, including policies addressing privileged access, incident response, resilience and recovery, retention and secure disposal, and subprocessors.

5.3 Where the service uses an approved hosting or infrastructure provider, PCL One may rely on physical, environmental and infrastructure controls operated by that provider, while PCL One remains responsible for its contractual obligations to the Customer for the PCL One-managed service.

5.4 The Customer is responsible for security controls under its management, including Customer user administration, Customer-managed identities, networks, endpoints, integrations, access approvals and configuration choices identified as Customer responsibilities in the applicable service design.

SECURITY EVIDENCE

Detailed security architecture, audit extracts, account identifiers, penetration-testing material and similar sensitive evidence are not necessarily public. PCL One may provide appropriate assurance evidence to eligible customers, prospective customers, business partners or regulators through controlled due diligence, subject to confidentiality and report-use restrictions.

6. Personal-data breach and incident support

6.1 PCL One will maintain an incident-response process for Security Incidents affecting Customer Personal Data or the contracted service and will investigate, contain, recover from and document material incidents within PCL One's responsibility.

6.2 For a confirmed Personal Data Breach affecting Customer Personal Data, PCL One will provide a baseline customer notification within 12 hours of confirmation, unless the governing agreement, applicable law or regulator requires a shorter or stricter timeline.

6.3 A preliminary notice may be issued before the full forensic picture is known. Notifications will include information reasonably available at the time, which may include the nature of the incident, affected service or data categories, known or suspected impact, containment and recovery actions, requested Customer actions and the planned update point.

6.4 PCL One will provide information reasonably available to support the Customer's regulator, data-subject, insurance or executive reporting obligations and will remain the Customer-facing escalation point for the contracted service where an underlying hosting or subprocessor incident is involved.

6.5 The Customer will maintain current security and privacy contacts and will provide timely information and access reasonably required to investigate incidents involving Customer-managed identities, networks, integrations or endpoints.

7. Subprocessors and third-party services

7.1 The Customer authorizes PCL One to engage Subprocessors and material third-party service providers where reasonably required to provide the Services, subject to this Addendum and the applicable agreement.

7.2 PCL One will assess relevant security, privacy, confidentiality and service-dependency risks before a provider is used for Customer Processing and will impose written contractual obligations appropriate to the provider's role and the sensitivity of the data involved.

7.3 PCL One will limit provider access to the minimum necessary and will require security and confidentiality controls appropriate to the provider's role. PCL One remains responsible for its contractual obligations to the Customer when Subprocessors are used.

7.4 PCL One will provide advance written notice of a material Subprocessor change before Processing begins where practicable and in accordance with the governing contract. The Customer may raise a reasonable data-protection objection within the process and timeframe stated in the applicable agreement or data-protection terms.

7.5 The public Subprocessor & Third-Party Services Policy identifies providers that may support PCL One services. A Customer-specific schedule, where required, identifies the providers actually applicable to the subscribed service, their purpose and relevant Processing location.

8. Data-subject and regulatory assistance

8.1 Taking into account the nature of the Processing and the functionality available in the Services, PCL One will provide reasonable assistance to the Customer in responding to requests from individuals to exercise rights under Applicable Data Protection Law where the Customer cannot reasonably fulfill the request using available service functionality.

8.2 If PCL One receives a request from an individual relating to Customer Personal Data for which the Customer is responsible, PCL One may direct the individual to the Customer unless Applicable Data Protection Law requires PCL One to respond directly.

8.3 PCL One will provide reasonable information and cooperation for Customer privacy-impact assessments, data-protection impact assessments, regulator consultations or similar compliance activities where required by Applicable Data Protection Law and relevant to the contracted Services. Additional work outside normal service operations may be subject to an agreed scope and fees where permitted by law and contract.

8.4 The Customer remains responsible for decisions regarding legal basis, response to data-subject requests, records classification, statutory retention, required notices and regulator submissions unless the parties expressly agree otherwise.

9. International transfers and data residency

9.1 The hosting region, data-residency model and any contractual localization requirement for the subscribed service are identified in the applicable Ordering Document, Service Schedule or service design.

9.2 PCL One will not intentionally relocate Customer Personal Data outside an expressly contracted residency model except where authorized by the Customer, permitted by the applicable agreement, required for an approved service-provider arrangement, or required by law, in each case subject to applicable data-protection obligations.

9.3 Where Applicable Data Protection Law requires a recognized transfer mechanism for a transfer of Customer Personal Data, the parties will apply the mechanism identified in the applicable transfer schedule, Ordering Document or jurisdiction-specific terms. Such mechanism may include standard contractual clauses, an approved certification or other legally recognized safeguard, as applicable.

9.4 For a Canada-only municipal deployment, production customer data, backups and recovery copies remain within the approved Canadian residency model where that baseline is adopted by the applicable Order, subject to any documented Customer-approved exception.

10. Retention, return and secure deletion

10.1 Customer-specific retention requirements are governed by the applicable agreement, Service Schedule, records schedule, Customer instructions and Applicable Data Protection Law. PCL One does not impose one universal business-record retention period across all Customer data categories.

10.2 The Customer may use supported export mechanisms during the service term. At termination or expiry, PCL One will provide the agreed export and transition period identified in the applicable service terms.

10.3 After the agreed transition period, PCL One will delete or render inaccessible remaining Customer Personal Data in the active service, subject to legal retention requirements, active holds and documented backup-cycle limitations. Residual backup copies expire through the applicable backup rotation unless law requires continued preservation.

10.4 A documented legal hold, investigation hold, records-freeze instruction or statutory requirement may suspend routine deletion only for affected data. Once the hold is released, the normal retention and disposal process resumes.

10.5 Where requested or contractually required, PCL One may provide a secure-data-destruction confirmation identifying the relevant scope and completion date of disposal.

11. Audit, assurance and compliance evidence

11.1 PCL One will maintain records reasonably necessary to demonstrate operation of the controls described in this Addendum and applicable Trust Centre policies.

11.2 Where available and applicable to the subscribed service, PCL One may provide independent assurance reports, certifications, audit summaries or other evidence through controlled due diligence. Detailed reports may be subject to confidentiality, report-use and eligibility restrictions.

11.3 If Applicable Data Protection Law requires additional audit information that is not reasonably addressed by available assurance evidence, the parties will cooperate in good faith on a reasonable audit process that protects other customers, PCL One confidential information, security architecture and service continuity.

11.4 Customer audits must be proportionate to the Processing risk and, unless prohibited by law, coordinated in advance, performed during reasonable business hours, limited to relevant controls, and conducted in a manner that does not compromise security or service operations.

12. Government and legal access requests

12.1 PCL One may be required by law, court order, subpoena, regulator instruction or other binding legal process to preserve or disclose Customer Personal Data.

12.2 Unless legally prohibited, PCL One will notify the Customer of a binding request directed to PCL One for Customer Personal Data and will use reasonable efforts to direct the requesting authority to the Customer where appropriate.

12.3 To the extent PCL One is required to respond directly, PCL One will assess the request in accordance with applicable law and will seek to disclose only the Customer Personal Data legally required for the response.

12.4 PCL One may preserve data subject to a lawful preservation requirement or legal hold even where routine deletion would otherwise apply. The affected data will remain subject to appropriate access restrictions and will be deleted when the preservation obligation ends, subject to the normal backup cycle.

13. Agreement relationship and liability

13.1 This Addendum forms part of the agreement governing the Services. Except as expressly modified by this Addendum, the remaining terms of the governing agreement continue to apply.

13.2 Liability arising from this Addendum is subject to the limitations, exclusions and remedies in the governing agreement unless Applicable Data Protection Law requires otherwise or the applicable Ordering Document expressly states a different treatment.

13.3 No provision of this Addendum limits an individual's rights or a regulator's authority where such limitation is prohibited by Applicable Data Protection Law.

14. Definitions

Term	Meaning
Applicable Data Protection Law	Data privacy, data protection, breach-notification or related laws and regulations that apply to the relevant Processing of Customer Personal Data under the Services.
Controller	The entity that determines the purposes and means of Processing Personal Data, or the equivalent role under Applicable Data Protection Law.
Customer Personal Data	Personal Data contained in Customer Data that PCL One Processes on the Customer's behalf in connection with the Services.
Personal Data	Information relating to an identified or identifiable individual, or equivalent protected personal information under Applicable Data Protection Law.
Personal Data Breach	A confirmed breach of security resulting in unauthorized access to, acquisition of, use of, disclosure of, alteration of, loss of, destruction of or unavailability of Customer Personal Data, to the extent treated as a personal-data breach under Applicable Data Protection Law.
Process / Processing	Any operation performed on Personal Data, including collection, storage, use, retrieval, disclosure, transmission, alteration, deletion or destruction.
Processor	The entity that Processes Personal Data on behalf of a Controller, or the equivalent role under Applicable Data Protection Law.
Subprocessor	A third party engaged by PCL One to Process Customer Personal Data on PCL One's behalf in connection with the contracted Services.

Annex A

Description of processing

The following description applies as a baseline. The applicable Ordering Document, Service Schedule, implementation design or Customer-specific data inventory may provide more specific processing details for a subscribed service.

Processing attribute	Baseline description
Subject matter	Provision, operation, support, security, maintenance, backup, recovery, configuration, implementation and administration of the subscribed PCL One Services.
Duration	For the service term and any agreed transition, support, legal-hold or backup-expiration period during which PCL One retains Customer Personal Data.
Nature of processing	Collection, receipt, organization, storage, hosting, retrieval, consultation, use, transmission, integration, reporting, backup, recovery, support access, deletion and other operations necessary to provide the subscribed Services.
Purpose	To provide and support the Services in accordance with the Customer's documented instructions, the governing agreement and applicable service specifications.
Frequency	Continuous or recurring for active service operations, with event-driven processing for transactions, integrations, support, backup, recovery and incident response.

Categories of data subjects

- Customer employees, workers, contractors, applicants, managers, retirees and other workforce participants where HCM, payroll or related functions are used.
- Customer residents, ratepayers, utility account holders, taxpayers, vendors, suppliers, customers, contacts or other persons whose data the Customer enters into the subscribed service.
- Customer administrators, users, support contacts, authorized approvers and other individuals who interact with or administer the service.
- Other individuals whose Personal Data is included in Customer Data at the Customer's direction.

Categories of Customer Personal Data

Category	Examples where applicable
Identity and contact data	Name, address, telephone number, email address, internal identifiers and business contact details.
Workforce and employment data	Employment status, position, department, compensation, payroll, tax, benefits, time, leave, performance, recruitment and training information.
Financial and transaction data	Payment details, banking information, account balances, invoices, transactions, taxation, utility, procurement and related financial records.
Government or regulated identifiers	Tax identifiers, employee identifiers, permit or account identifiers and other regulated identifiers where configured by the Customer.
Authentication and audit data	User identifiers, role assignments, access events, audit records, security logs and support-case information.
Documents and attachments	Files, forms, images, correspondence and metadata uploaded or generated through subscribed workflows.
Special or sensitive data	Health, benefits, disability, union, demographic, background, financial or other sensitive information only where the Customer uses service features that require such Processing and Applicable Data Protection Law permits it.

Annex B

Technical and organizational measures

PCL One applies measures appropriate to the subscribed architecture and the risks of Processing. Service-specific implementation details may differ, and sensitive configuration evidence is provided through controlled due diligence rather than public disclosure.

Control domain	Baseline measures
Governance and accountability	Documented security, privacy, incident, resilience, access and data-lifecycle policies; assigned operational ownership; risk-based control review and supporting records.
Identity and privileged access	Named administrative identities where supported; least privilege; role-based access; strong authentication; approval; time-bound elevation; logging and review of material or emergency access.
Data protection	Access controls, data minimization, service-specific encryption and secure communications, segregation appropriate to the architecture, and restrictions on unnecessary use or disclosure.
Hosting and infrastructure	Approved hosting and service providers; provider due diligence; contractual safeguards; controlled provider access; customer-specific residency and architecture documentation where required.
Logging and monitoring	Operational and security logging for PCL One-managed components, service-health monitoring, review of material administrative activity and incident evidence preservation.
Backup and recovery	Automated protected backups appropriate to the subscribed service; documented recovery windows; restore testing; controlled recovery procedures; service-specific RTO/RPO where contracted.
Incident management	Detection and triage, containment, investigation, evidence preservation, customer notification, recovery, corrective actions and post-incident follow-through for material incidents.
Subprocessor governance	Security/privacy risk assessment, written contractual safeguards, minimum-necessary access, applicability tracking and material-change notification under the governing terms.
Retention and disposal	Customer-approved or contracted retention schedules, legal-hold handling, controlled export/transition, secure deletion or rendering inaccessible, and backup expiration through the documented cycle.
Business continuity	Documented resilience and recovery processes, periodic recovery exercises, recovery runbooks and corrective-action tracking for in-scope services.

ASSURANCE

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 Addendum by publication.

Annex C

Transfer and jurisdiction-specific terms

This Annex provides the baseline mechanism for adding jurisdiction-specific privacy and transfer terms without changing the body of the Addendum for every Customer. The applicable Order or Customer-specific schedule identifies which additional terms apply.

Topic	Baseline treatment
Data residency	The applicable Order or Service Schedule identifies any contracted hosting or residency restriction for Customer Personal Data.
Cross-border transfers	Where a transfer mechanism is legally required, the parties apply the mechanism identified in the applicable transfer schedule or jurisdiction-specific terms.
Standard contractual clauses	If required for the applicable transfer, the relevant clauses or approved addendum may be incorporated by reference or attached to the Customer-specific schedule, with the parties' roles and service information populated as required.
Local privacy terms	Additional controller/processor, consumer privacy, public-sector, health, employment or sector-specific terms may be included where required by Applicable Data Protection Law or the Customer's procurement terms.
Conflict	Jurisdiction-specific terms control only to the extent necessary to satisfy the applicable legal requirement and otherwise leave this Addendum unchanged.

Nothing in this Annex should be read as a representation that every transfer mechanism or jurisdiction-specific term applies to every Customer. Applicability depends on the Customer, subscribed service, Processing location, data subjects and Applicable Data Protection Law.

15. Statement of changes

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

This Addendum is intended to operate as part of the PCL One contract framework. Service-specific or customer-specific obligations are governed by the applicable agreement, Ordering Document, Service Schedule and incorporated policies.