

TRUST CENTRE

End-of-Service, Data Portability & Transition Policy

CUSTOMER DATA EXPORT, ORDERLY TRANSITION, ACCESS WIND-DOWN AND SECURE DISPOSAL

Effective Date: 6 October 2025

Classification: Public

Document ID: PCL-TRUST-EXIT-018

This document is intended for public distribution. Customer-specific export formats, transition periods, migration services, retention schedules, fees and post-termination assistance are governed by the applicable Agreement, Ordering Document, Service Schedule, Statement of Work or other contracted service terms.

Contents

This policy should be read together with the PCL One Cloud Services Agreement, Cloud Service Description, Data Processing Addendum, Data Retention, Backup & Secure Disposal Policy, Professional Services Terms, applicable Ordering Document and customer-specific Service Schedule or Statement of Work.

01	Overview
02	Scope and contractual relationship
03	Exit and portability principles
04	Customer data ownership and control
05	Supported export mechanisms and formats
06	Exit planning and transition window
07	Transition assistance and professional services
08	Integrations and third-party dependencies
09	Access wind-down and service continuity
10	Export validation and customer acceptance
11	Retention, legal holds and backups
12	Secure disposal and destruction confirmation
13	Customer responsibilities
14	Exceptions and customer-specific terms
15	Assurance and evidence
16	Related documents
17	Statement of changes

1. Overview

PCL One supports an orderly end-of-service process so that Customers can retrieve Customer Data, transition business processes and integrations, and complete secure disposal activities in accordance with the applicable contract. This policy establishes the public baseline for data portability and service transition when a subscription, Order or applicable service ends.

Public baseline

Customer Data remains under the Customer's ownership or control as stated in the applicable Agreement. Customers may use supported export mechanisms during the service term, and an agreed export or transition period applies at contract end before remaining Customer Data is securely deleted or rendered inaccessible, subject to legal holds and documented backup cycles.

2. Scope and contractual relationship

This policy applies to PCL One-managed cloud services where it is incorporated into the applicable Agreement, Order, Service Schedule or Service Specifications. It addresses the operational treatment of Customer Data and service access at expiry, termination or other agreed end of service.

- The applicable Agreement and Order determine the legal basis, effective date and consequences of expiry or termination.
- The Service Description, Service Schedule or Statement of Work may define service-specific export formats, transition periods, migration activities, dependencies and fees.
- The Data Processing Addendum and Data Retention, Backup & Secure Disposal Policy govern personal-data return, retention, legal holds, backup expiration and secure disposal.
- Where mandatory law or a negotiated customer term is stricter or more specific, that term controls for the affected service.

3. Exit and portability principles

Principle	Public baseline
Orderly transition	PCL One coordinates end-of-service activities so that access, exports, integrations and disposal can be managed in a controlled sequence.
Customer control	The Customer decides what supported data exports it requires and is responsible for validating exported information before final disposal.
Portability	PCL One uses supported machine-readable or service-supported export mechanisms appropriate to the subscribed service.
Security	Exports, transition access and disposal remain subject to authentication, authorization, encryption and other applicable security controls.
No indefinite retention	End-of-service processing does not create indefinite retention. Remaining data is disposed of after the agreed transition period, subject to documented exceptions.
Contract specificity	Timing, formats, assistance and any associated fees may differ by service and are defined in the applicable customer terms.

4. Customer data ownership and control

Ending a service does not transfer ownership of Customer Data to PCL One. Customer Data remains subject to the ownership and control provisions of the applicable Agreement and to applicable data-protection law.

- PCL One does not claim ownership of Customer Data merely because it is hosted or processed within the Services.
- Customer administrators should identify the records, reports, attachments, audit information and configuration data that must be exported before service access ends.
- Data created or maintained outside the PCL One service, including Customer-managed exports and third-party repositories, remains governed by the controls of the receiving environment.

5. Supported export mechanisms and formats

Customers may use supported export capabilities during the subscription term and, where applicable, during the agreed transition window. Available mechanisms depend on the service, data type and contracted configuration.

Export category	Typical treatment
Business records	Supported reporting, bulk export or structured data extract mechanisms available within the subscribed service.
Documents and attachments	Service-supported download or packaged export where the applicable service maintains customer-uploaded documents.
Audit and operational records	Supported reports or exports where such records are customer-accessible under the applicable service design.
Configuration and reference data	Export or documentation where supported and appropriate to the service.
APIs and integrations	Documented APIs or integration interfaces may be used for ongoing extraction where included in the subscribed service.

Formats may include commonly used machine-readable or document formats such as CSV, XLSX, JSON, XML, PDF or other service-supported formats. This policy does not guarantee that every data category is available in every format.

6. Exit planning and transition window

The transition window is the period during which the Customer completes required exports and other agreed exit activities before final disposal. The length of that period is governed by the applicable service terms rather than a single universal public duration.

- PCL One and the Customer should confirm the planned service-end date, authorized transition contacts and material export dependencies.
- Customer access during a transition window remains subject to the applicable contract, security controls and any lawful suspension rights.
- The Customer should initiate large or complex exports early enough to allow verification and correction before the transition window closes.
- If the parties agree to extend access or provide additional transition services, the arrangement should be documented in the applicable Order, Service Schedule or Statement of Work.

7. Transition assistance and professional services

Standard service exports are distinct from project-based migration or transition assistance. Where requested, PCL One may provide additional professional services to support data mapping, extraction, reconciliation, integration cutover, knowledge transfer or coordination with a successor provider.

- Additional transition assistance is scoped through a Statement of Work or other written agreement where it is not included in the existing service.
- The SOW may define deliverables, Customer dependencies, acceptance criteria, schedule, fees and third-party responsibilities.
- PCL One does not assume responsibility for configuring, operating or validating a successor platform unless that work is expressly included in the agreed scope.

8. Integrations and third-party dependencies

Ending a PCL One service may affect integrations, identity connections, payment services, data feeds and other third-party dependencies. The parties should coordinate the sequence for disabling or redirecting those connections.

- The Customer is responsible for Customer-managed endpoints, credentials, certificates, identity-provider changes and receiving systems.
- PCL One will disable or retire PCL One-managed integration components in accordance with the applicable exit plan and security requirements.
- Third-party providers may have separate termination, retention or export obligations that are governed by their own contracts or by the applicable Customer agreement.

9. Access wind-down and service continuity

Service access is reduced or discontinued in a controlled manner consistent with the effective end date and agreed transition plan. PCL One may preserve limited administrative access where necessary to complete authorized export, security, billing, legal-hold or disposal activities.

Access is not a retention guarantee

A transition window provides time to complete agreed exit activities; it does not create indefinite production access or an indefinite right to retain data after the contracted service has ended.

10. Export validation and customer acceptance

The Customer is responsible for confirming that required exports have been completed and are usable before final disposal. PCL One will reasonably address export issues within the scope of the supported mechanism or agreed transition services.

- Validate file completeness, readability and expected record counts where those controls are relevant to the export.
- Confirm that required attachments, reports, audit information and reference data have been captured where supported.
- Retain copies in a Customer-controlled environment in accordance with the Customer's own records and security requirements.
- Raise material export issues promptly during the transition period so they can be investigated before access ends.

11. Retention, legal holds and backups

End-of-service disposal remains subject to approved retention schedules, legal holds, investigations, statutory preservation requirements and documented backup cycles.

Data state	End-of-service treatment
Active production data	Deleted or rendered inaccessible after the agreed transition period unless an applicable retention exception requires continued preservation.
Backups	Residual copies expire through the documented backup rotation and are not used to create indefinite business-record retention.
Legal-hold data	Routine deletion is suspended only for affected data until the hold or preservation requirement is released.
Migration or staging data	Removed or de-identified when no longer required for migration, validation or acceptance, subject to legal or contractual needs.

12. Secure disposal and destruction confirmation

After the agreed transition period, remaining Customer Data in the active service is securely deleted or rendered inaccessible in accordance with the Data Retention, Backup & Secure Disposal Policy, subject to applicable legal-retention requirements and backup-cycle limitations.

- PCL One applies disposal controls appropriate to the applicable service, storage technology and data state.
- Residual backup copies expire through the applicable backup rotation unless law or a documented hold requires preservation.
- Where requested or contractually required, PCL One may provide a secure-data-destruction confirmation or certificate identifying the relevant scope and completion date.

13. Customer responsibilities

A successful exit depends on timely Customer decisions and participation. The Customer is responsible for the controls and actions that remain within its administrative or business process.

- Designate authorized exit, security, privacy and technical contacts.
- Identify required exports and any regulatory or records-retention constraints that affect the transition.
- Complete exports during the agreed transition period and validate the exported data before final disposal.
- Provide and maintain receiving systems, storage capacity, encryption controls and access permissions for Customer-managed copies.

- Coordinate successor-provider dependencies, Customer-managed integrations and identity changes.
- Notify PCL One of active legal holds or records-freeze instructions affecting data that PCL One is expected to preserve.

14. Exceptions and customer-specific terms

Transition arrangements may vary where required by law, public-sector records obligations, regulated-industry requirements, technical limitations, active security investigations, legal holds or negotiated customer terms.

- A customer-specific Order or Service Schedule may define a particular export window, format, transition deliverable, retention period or deletion procedure.
- Additional transition assistance may be subject to a separate SOW and fees where it falls outside the standard subscribed service.
- PCL One may delay deletion where a binding legal or regulatory obligation requires preservation, but the affected data remains subject to appropriate access restrictions.
- Nothing in this policy requires PCL One to disclose proprietary source code, internal security architecture, another customer's data or information that PCL One is legally prohibited from providing.

15. Assurance and evidence

PCL One maintains records reasonably necessary to support operation of the end-of-service controls described in this policy. Detailed evidence may be restricted and provided through controlled due diligence where appropriate.

Evidence type	Typical availability
Exit or export record	Customer-specific operational evidence, where maintained for the applicable service.
Transition or SOW records	Available to the contracting parties for the applicable engagement.
Retention or legal-hold record	Restricted to authorized parties because it may contain confidential or legally sensitive information.
Secure-disposal confirmation	Available where requested or contractually required and supported by the applicable process.
SOC 2 Type 2 report	Restricted-use assurance evidence, subject to eligibility, confidentiality and report-use restrictions.

16. Related documents

This policy forms part of the broader PCL One contractual and Trust Centre framework. The following documents may apply depending on the subscribed service and customer arrangement:

- PCL One Cloud Services Agreement and applicable Ordering Document.
- PCL One Cloud Service Description and customer-specific Service Schedule.
- PCL One Data Processing Addendum.
- PCL One Data Retention, Backup & Secure Disposal Policy.
- PCL One Professional Services Terms and applicable Statement of Work.
- PCL One Data Residency & Location Policy and Information Security Practices.

17. Statement of changes

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