



TRUST CENTRE

Uploaded Media & Location Metadata Privacy Policy

PHOTO, ATTACHMENT AND EMBEDDED METADATA HANDLING

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.

01	Overview	
02	Scope and applicability	
03	Definitions	
04	Metadata-minimization policy	
05	Customer responsibilities	
06	Exceptions and exclusions	
07	Assurance and evidence	
08	Statement of changes	

1. Overview

Digital photos and other media can contain hidden metadata such as capture time, device information and precise GPS coordinates. This policy explains PCL One's data-minimization approach for uploaded media and distinguishes hidden metadata from location information intentionally entered as part of a business process.

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 PCL One-managed media-processing routes where metadata-minimization controls are enabled for uploaded photos or attachments.

Covers embedded EXIF or equivalent metadata, explicit geolocation fields, evidentiary originals and integrations that bypass PCL One media processing.

Does not represent that every legacy route, third-party repository, bulk-import process or external integration automatically strips source-file metadata.

Relationship to customer agreements

Customer-specific requirements for evidentiary preservation, geolocation, retention, privacy notice or records management are documented in the applicable service design or agreement. Those approved requirements take precedence for the relevant workflow.

3. Definitions

Term	Meaning
EXIF Metadata	Embedded information commonly stored in image files, which may include capture time, camera/device attributes and GPS coordinates.
Embedded Location Metadata	Location information stored within file metadata rather than visibly entered by a user in a business form.
PCL-Managed Media Route	An upload or processing path operated by PCL One and configured to apply the controls described in this policy.
Evidentiary Original	An original file that must be preserved without alteration because of a documented legal, records or evidentiary requirement.

4. Metadata-minimization policy

BASELINE PRINCIPLE

PCL One does not require hidden GPS or EXIF location metadata for core municipal finance, tax, utility, HR or payroll workflows. Hidden metadata should be retained only where a documented business or evidentiary purpose requires it.

Scenario	Baseline treatment
Photo uploaded through a PCL-managed media route	Where metadata minimization is enabled, unnecessary EXIF fields that may expose precise GPS location or device identifiers are removed before the application-managed copy is persistently stored.
Business process explicitly requires geolocation	Retain only the location information required for the documented purpose, with appropriate customer approval, notice, access controls and retention.
Location entered as a normal form field	Treat as ordinary customer data under the configured retention, access and audit controls. This is separate from hidden EXIF metadata.
Original evidentiary file must be preserved	The original may be retained where the customer has a documented records or evidence requirement. Access should be restricted and the presence of embedded metadata understood.
External repository, bulk import or integration bypasses PCL media processing	Source-file metadata may remain. Responsibility for metadata minimization is defined in the source-system or integration design.

Use limitations

Embedded location metadata is not used by PCL One for advertising, generalized profiling or unrelated analytics.

Embedded location metadata is not provided to an AI service unless the customer has approved a use case that requires it and the applicable data controls permit it.

Where metadata is stripped, visible image content is preserved; metadata stripping does not remove location information visibly present within the image itself.

Verification and exceptions

The control described in this policy applies only to PCL-managed media-processing routes where metadata minimization is enabled. Third-party repositories, external integrations and routes outside PCL-managed media processing may preserve source-file metadata. Any approved exception to retain embedded location metadata should identify the purpose, scope, retention and access controls.

5. Customer responsibilities

Identify workflows where geolocation or unaltered evidentiary originals are required before production configuration is finalized.

Provide any required privacy notice, records classification or retention instruction for business processes that intentionally capture location information.

Apply appropriate controls to external repositories or integration routes that are outside PCL One-managed media processing.

6. Exceptions and exclusions

Legacy, external or bypass routes may retain source metadata unless they are separately configured and verified for metadata minimization.

File formats and third-party transformations may handle metadata differently; route-specific validation is required where the behavior is material to the customer requirement.

Preservation requirements may justify retaining an original file with embedded metadata if the workflow has been documented and access is appropriately restricted.

7. 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.

Upload-path configuration or design records.

Route-specific metadata validation tests where performed.

Approved exception records where metadata is intentionally retained.

Privacy-impact or data-flow documentation for location-dependent features where applicable.

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.

8. Statement of changes

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