PRIVACY POLICY

ComplianceOS Audit Capture — Chrome Extension

Effective Date: 12 February 2025 | Version 1.01

1. Introduction

This Privacy Policy describes how Practicl AI SAS (**“Practicl,” “we,” “our,” or “us”**), a company registered in France (Siège social: Toulouse, France), collects, uses, stores, and protects information when you use the ComplianceOS Audit Capture Chrome Extension (the “Extension”). This Extension is designed for compliance auditors and professionals working within regulated financial institutions.

By installing and using the Extension, you agree to the practices described in this Privacy Policy. If you do not agree, please uninstall the Extension immediately.

2. Data We Collect

2.1 Data Collected Automatically

When you use the Extension to capture audit evidence, the following data is collected:

Screenshot image data: A visual capture of the currently visible browser tab content at the time you initiate a capture.

Page metadata: The URL, page title, and document character set of the page being captured.

Timestamp: The exact date and time (UTC) at which the capture was initiated.

Cryptographic hash: A SHA-256 hash of the screenshot and associated metadata, used to verify evidence integrity.

Trusted timestamp token: An RFC 3161 timestamp obtained from a qualified Timestamp Authority to provide independently verifiable proof of capture time.

Authenticated user identity: Your ComplianceOS account identifier, used to attribute the capture to the auditor who performed it.

2.2 Data You Provide

You may optionally provide:

Audit context tags: The audit engagement, finding, or report section to which the captured evidence should be linked within ComplianceOS.

Notes or annotations: Any descriptive text you add to the capture before submission.

2.3 Data We Do Not Collect

The Extension does not collect or transmit:

Browsing history or activity outside of explicit, user-initiated captures.

Cookies, form data, passwords, or authentication credentials from websites you visit.

Data from any tab or window other than the one you are actively viewing when you initiate a capture.

Keystroke data, mouse movements, or any form of behavioural tracking.
Personally identifiable information beyond your ComplianceOS account identity.

3. How We Use Your Data

All data collected by the Extension is used solely for the following purposes:

Evidence preservation: Storing captured screenshots as tamper-evident audit evidence within your ComplianceOS workspace.
Integrity verification: Using cryptographic hashes and trusted timestamps to allow independent verification that evidence has not been altered after capture.
Audit trail maintenance: Linking captures to specific audit engagements, findings, and report sections to maintain a complete chain of custody.
User authentication: Verifying that captures are attributed to authorised ComplianceOS users.

We do **not** use any data collected by the Extension for advertising, profiling, analytics beyond service operation, or any purpose unrelated to your compliance and audit activities.

4. Data Storage and Security

4.1 Where Data Is Stored

Captured evidence and associated metadata are transmitted via encrypted HTTPS connections and stored within the ComplianceOS platform infrastructure:

Screenshot images are stored in encrypted cloud object storage (AWS S3 or Google Cloud Storage, depending on your organisation's deployment configuration).
Metadata, cryptographic hashes, and timestamp tokens are stored in our database (Supabase with PostgreSQL), protected by encryption at rest and row-level security policies.
All data is stored within the European Union or in regions specified by your organisation's data residency requirements.

4.2 Security Measures

We implement the following security measures to protect your data:

TLS 1.2 or higher for all data in transit between the Extension and ComplianceOS servers.
AES-256 encryption at rest for all stored evidence and metadata.
Role-based access controls ensuring only authorised users within your organisation can access captured evidence.
Immutable audit logs recording all access to and actions performed on captured evidence.
Regular security assessments aligned with our ISO 27001 Information Security Management System.

5. Data Sharing

We do not sell, rent, or trade your data to any third party. Data collected by the Extension may be shared only in the following limited circumstances:

Timestamp Authority: The cryptographic hash (not the screenshot or its content) is submitted to an RFC 3161-compliant Timestamp Authority to obtain a trusted timestamp. No image data or page content is shared with the Timestamp Authority.

Your organisation: Captured evidence is accessible to authorised users within your ComplianceOS organisational workspace, in accordance with your organisation's access control policies.

Infrastructure providers: Our cloud hosting providers (AWS, Google Cloud, Supabase) process data on our behalf under strict data processing agreements compliant with GDPR Article 28.

Legal obligations: We may disclose data if required by applicable law, regulation, or valid legal process.

6. Data Retention

Captured evidence is retained for the duration specified by your organisation's data retention policies within ComplianceOS. In the absence of a specific organisational policy, evidence is retained for a minimum of seven (7) years from the date of capture, consistent with typical regulatory retention requirements for financial institutions.

You or your organisation's ComplianceOS administrator may request deletion of specific captures, subject to any applicable regulatory retention obligations. Upon account termination, all associated data will be deleted within ninety (90) days unless retention is required by law.

7. Your Rights

Under the General Data Protection Regulation (GDPR) and applicable French data protection law (Loi Informatique et Libertés), you have the following rights:

Access: Request a copy of the personal data we hold about you.

Rectification: Request correction of inaccurate personal data.

Erasure: Request deletion of your personal data, subject to legal retention obligations.

Restriction: Request that we limit the processing of your personal data.

Portability: Request your data in a structured, machine-readable format.

Objection: Object to processing of your personal data.

Withdrawal of consent: Withdraw consent at any time by uninstalling the Extension.

To exercise any of these rights, contact us at **privacy@practicl.com**. We will respond within thirty (30) days. You also have the right to lodge a complaint with the Commission Nationale de l'Informatique et des Libertés (CNIL), the French supervisory authority.

8. Permissions Justification

The Extension requests only the minimum Chrome permissions necessary to perform its function:

activeTab: Required to capture a screenshot of the tab you are currently viewing when you explicitly initiate a capture. This permission grants access only to the active tab, and only at the moment of capture.

identity: Required to authenticate you with your ComplianceOS account and attribute captures to the correct user.

storage: Required to store your Extension preferences and authentication state locally on your device.

The Extension does not request broad permissions such as access to all URLs, browsing history, or background execution. All captures are user-initiated and require explicit action.

9. Updates to This Policy

We may update this Privacy Policy from time to time to reflect changes in our practices or applicable law. We will notify you of material changes through the Extension or via the ComplianceOS platform. The “Effective Date” at the top of this policy indicates the date of the most recent revision. Continued use of the Extension after an update constitutes acceptance of the revised policy.

10. Contact Information

If you have questions or concerns about this Privacy Policy or our data practices, please contact:

Practicl AI SAS

16 rue saint Antoine du T

31000 Toulouse, France

Email: **privacy@practicl.com**

Website: **https://practicl.com**