

PRIVACY POLICY

Overview

This Privacy Policy establishes the controls and processes CodeEye uses internally when handling personal data, both our own and those processed on behalf of clients.

Purpose

Define CodeEye's privacy requirements and controls for collecting, processing, storing, sharing, and disposing of personal data within our GRC consulting operations, ensuring confidentiality, integrity, and compliance with applicable laws and client obligations.

Audience

This policy applies to all CodeEye employees, contractors, and subcontractors involved in any activity that collects, accesses, processes, or stores personal data for CodeEye or its clients.

Scope

Covers all personal data collected directly by CodeEye (e.g., employee records, prospect and client contact information) and data processed under client engagements (e.g., audit evidence, assessment findings), across all environments and third-party services.

Policy Statement

i. Regulatory & Contractual Compliance

- Identify and document applicable privacy laws, regulations, and contractual obligations for each engagement.
- Ensure all engagement contracts and data-processing agreements include required privacy clauses and safeguards. *[SOC 2 P1.1]*

ii. Notice & Communication

- Provide clear, concise privacy notices to individuals at the point of data collection.
- Publish and maintain a public-facing Privacy Notice; communicate material changes promptly. *[SOC 2 P1.2]*

iii. Consent & Choice

- Obtain explicit consent when required by law or contract before collecting or sharing personal data.
- Offer mechanisms to opt out or withdraw consent, except where prohibited by law. *[SOC 2 P2.1]*

iv. Collection & Use Limitation

- Collect only data necessary to fulfill engagements and internal business purposes.
- Use personal data strictly for purposes defined in engagement letters and privacy notices. *[SOC 2 P3.1]*

v. Privacy Impact Assessments

- Perform a Privacy Impact Assessment (PIA) for any new service, system, or processing activity involving personal data.
- Document identified risks, mitigation strategies, and obtain executive approval before implementation. *[SOC 2 P4.1]*

vi. Data Subject Rights & Requests

- Enable individuals to exercise rights: access, rectification, erasure, restriction, portability, and objection.
- Acknowledge and respond to requests within 30 days; record actions in the Privacy Request Log. *[SOC 2 P5.1, P5.2]*

vii. Data Minimization, Retention & Disposal

- Define retention periods for each data category in the Data Retention Schedule.
- Securely dispose of or archive personal data when no longer required, per the Data Disposal Policy. *[SOC 2 P4.2, P4.3]*

viii. Third-Party & Sub-Processor Management

- Maintain an inventory of all service providers and sub-processors handling personal data.
- Conduct due diligence and contract reviews; include privacy obligations and audit rights.
- Review vendor privacy compliance annually. *[SOC 2 P6.1, P6.2]*

ix. Data Transfers & Cross-Border Flows

- Identify international data transfers and implement appropriate safeguards (e.g., Standard Contractual Clauses, Binding Corporate Rules).
- Document and approve any exceptions. *[SOC 2 P6.3]*

x. Security & Confidentiality

- Apply technical and organizational controls, encryption at rest and in transit, access controls, and network segmentation to protect personal data.
- Align with CodeEye's Access Control, Data Encryption, and Security Incident Response policies. *[SOC 2 P8.1]*

xi. Monitoring & Incident Response

- Log and review access to personal data; generate alerts for anomalies per the Logging & Monitoring Policy.
- Invoke the Incident Response Playbook for privacy incidents; notify affected individuals and regulators within applicable timelines. *[SOC 2 P7.1, P8.1]*

xii. Training & Awareness

- Provide privacy and data protection training to all personnel at onboarding and annually.
- Include PIA procedures, data subject rights, and breach notification requirements. *[SOC 2 P9.1]*

xiii. Recordkeeping & Audit Trails

- Maintain records of PIAs, privacy requests, vendor assessments, and training for audit readiness.
- Retain logs and documents for a minimum of three years or as required by law or client contract. *[SOC 2 P10.1]*

xiv. Enforcement & Sanctions

- Report suspected policy violations to the CISO and HR.
- Apply disciplinary measures up to termination or contract cancellation based on the severity of non-compliance. *[SOC 2 P11.1]*

Annual Policy Review

The policy owner shall review this document annually to confirm it remains accurate, effective, and aligned with applicable regulations and frameworks. Any approved updates shall be recorded in the Revision History with the new effective date.

Enforcement

- Report suspected policy violations to the CISO and HR.
- Apply disciplinary measures up to termination or contract cancellation based on the severity of non-compliance. *[SOC 2 P11.1]*

References

- **Frameworks and Guidelines**

- o AICPA SOC 2 Trust Services Criteria
- o PCI DSS v4.0 Requirements 6, 11, and 12

- Internal Policies**

- o CodeEye Information Security Policy
 - o CodeEye Change Control Policy
 - o CodeEye Information Classification Policy