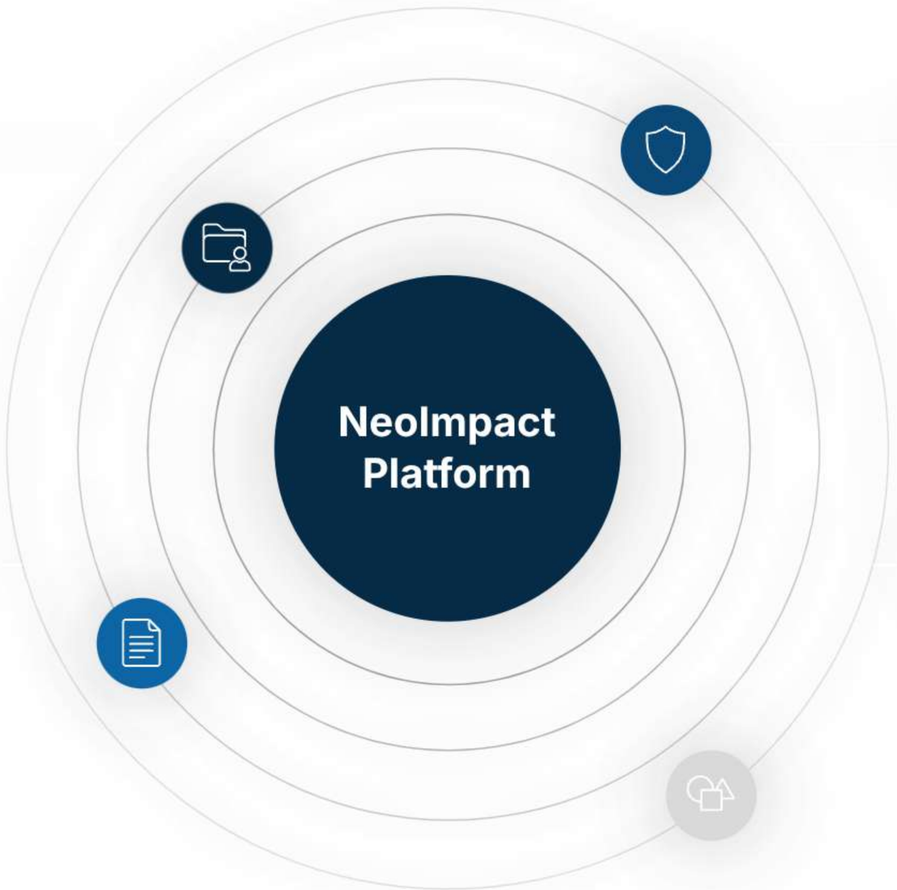
NeoImpact Data Storage & Handling Policy

This policy describes how NeoImpact stores, processes, and protects ESG and related portfolio company data collected through our platform. It applies to private equity, venture capital, and credit clients ("PEVCs") using NeoImpact's platform, portfolio companies ("PortCos") granted access by PEVCs to upload ESG and operational data, and all NeoImpact-controlled systems where such data is stored, processed, or transmitted.



Data Storage

Centralized lakes and encrypted warehouses

Security

Encryption, IAM, and threat detection

Compliance

Auditing, reporting, and GDPR/SEC controls

PortCos & PEVCs

Data sharing, insights, and performance metrics

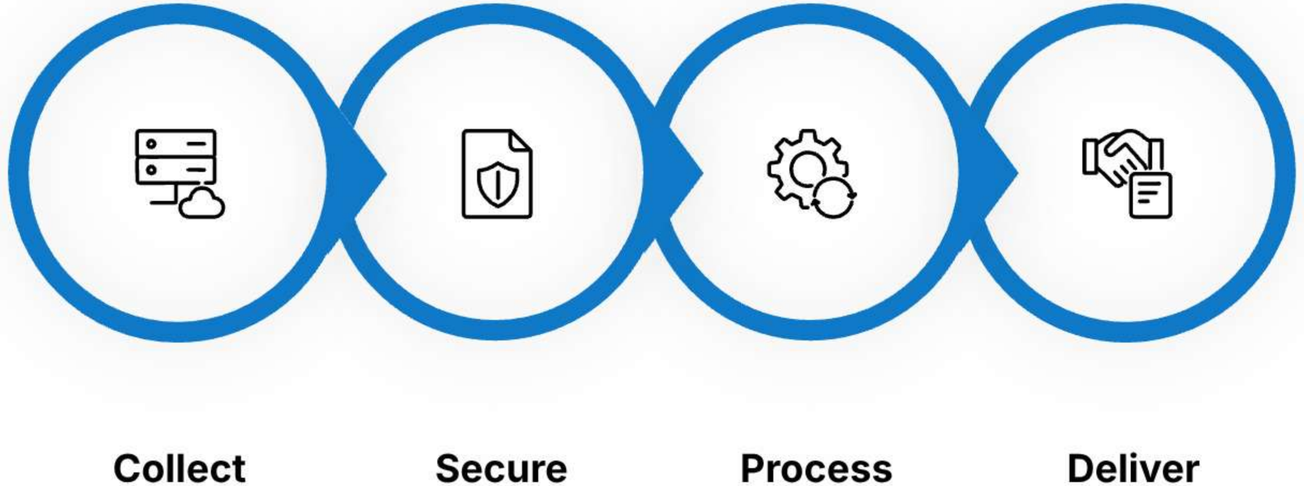
Purpose & Scope

Applicable Entities

- Private equity, venture capital, and credit clients ("PEVCs") using NeoImpact's platform
- Portfolio companies ("PortCos") granted access by PEVCs to upload ESG and operational data
- All NeoImpact-controlled systems where such data is stored, processed, or transmitted

Policy Coverage

This policy describes how NeoImpact stores, processes, and protects ESG and related portfolio company data collected through our platform.



Data Classification & Ownership

Classification

All client and PortCo data is classified as **Confidential – Client Proprietary**.

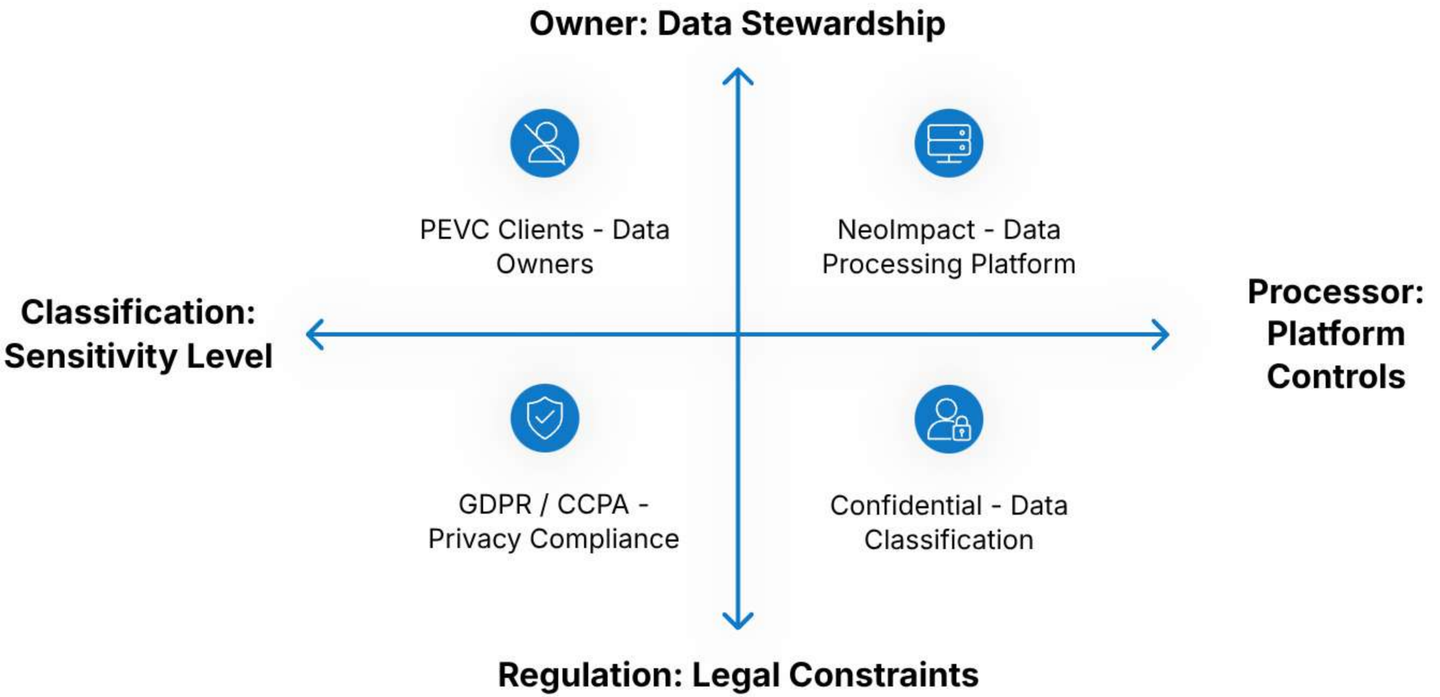
Ownership

The data owner is the client (PEVC), who retains full rights to their data.

Processing Role

NeoImpact acts as a data processor under applicable privacy laws (e.g., GDPR, CCPA) and processes data only on documented client instructions.

> NeoImpact's role as a data processor means we handle client data strictly according to their instructions and applicable privacy regulations.



Data Segregation

Tenant-Level Segregation

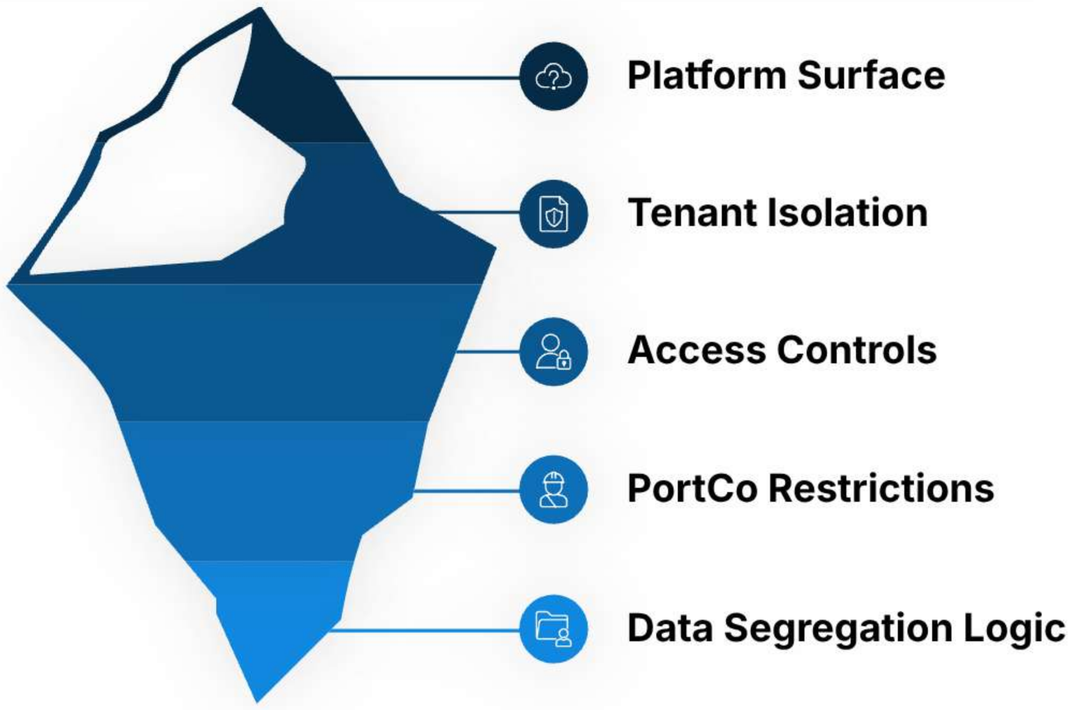
Data from different PEVC clients is logically segregated at the tenant level in our databases.

Access Control

Each tenant has unique access keys and role-based access controls (RBAC) ensuring isolation between clients.

PortCo Restrictions

Within a PEVC's tenant, PortCo access is restricted to their own data unless explicitly granted cross-access by the PEVC.



NeoImpact

Storage Architecture

Primary Datastores

- Relational database (encrypted at rest) for structured ESG, taxonomy, and metadata
- Object storage (encrypted at rest) for supporting documents, reports, and evidence files

Hosting

Cloud infrastructure in ISO 27001-certified AWS data centers

Data Residency

Data is stored in the US East 1 region (no customization options currently available)

Redundancy

All production data is maintained in primary secure storage environments (not multi-zone redundant)

Relational DBs
ACID storage for core data

Object Storage
Unstructured assets & backups

AWS Hosting
Scalable compute & network

Data Residency
Region controls & encryption

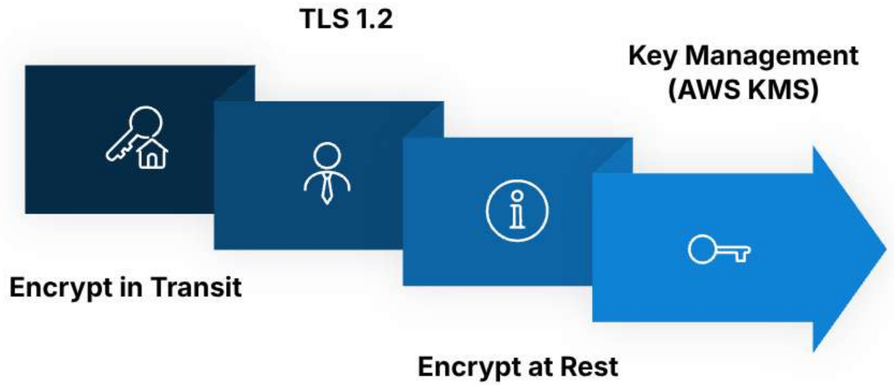
Data in Transit & at Rest

Encryption in Transit

TLS 1.2 for all client–platform communications, APIs, and internal service calls

Encryption at Rest

- AES-256 encryption for databases and object storage
- Encryption keys are managed via AWS KMS and rotated every 6 months



Upload & Taxonomy Handling

Secure Upload

PortCos upload ESG data via a secure web portal with enforced HTTPS (TLS 1.2 encryption)

Security Scanning

Uploaded files are scanned for malware and validated for schema compliance before being stored

Dynamic Forms

Upload forms dynamically adapt to the PEVC's custom ESG taxonomy defined in the platform

Metadata Tagging

Data is tagged with metadata (upload date, uploader ID, taxonomy mapping) for traceability

Access Control

Authentication

Platform-native MFA is enforced for all admin and PortCo logins

Authorization

Role-based permissions; PortCos can only access their own uploads unless otherwise granted by the PEVC

Session Management

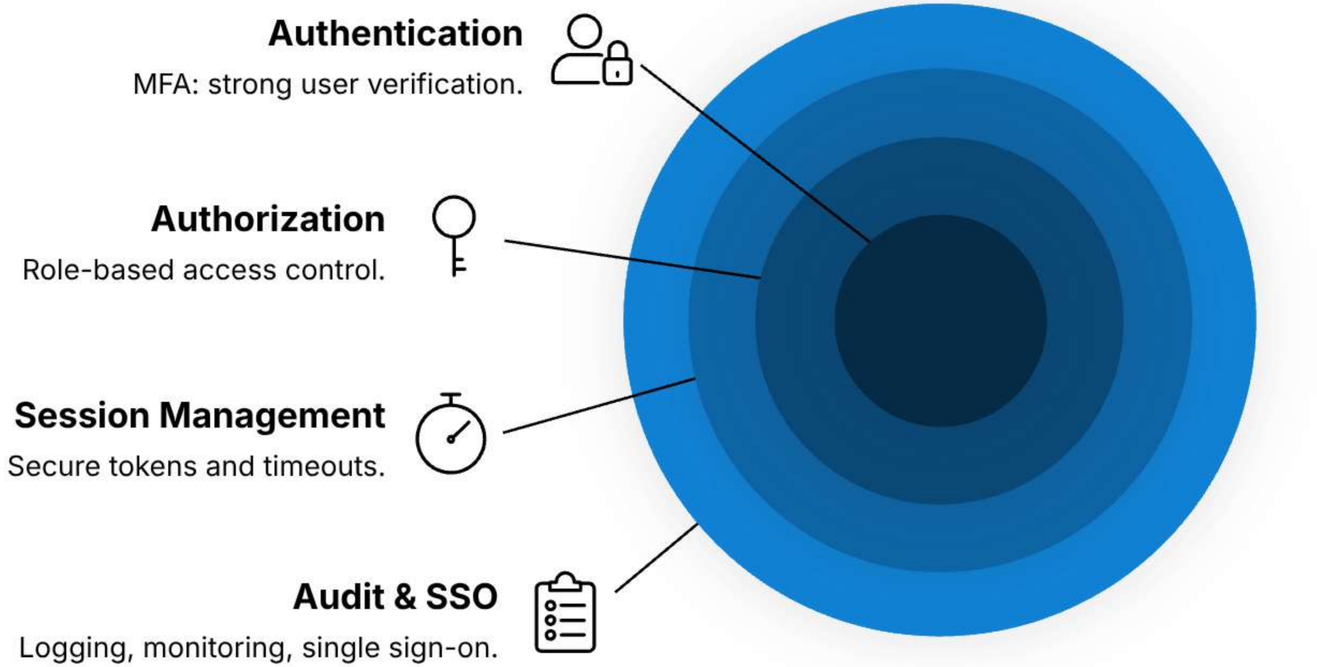
Auto-expiry after one month of inactivity

Audit Logging

All access, edits, and downloads are logged with timestamp, user ID, and action details. Logs are immutable and retained for one month

Single Sign-On

SSO available for enterprise clients upon request



Backup & Recovery

Backup Frequency

Automated, encrypted backups of all databases and file storage are performed daily

Backup Retention

30 days for hot backups, 1 year for archival backups

Disaster Recovery

Restore points are available to enable rapid restoration if needed. Recovery Point Objective (RPO) and Recovery Time Objective (RTO) details available upon request

DR Testing

DR plans are tested at least annually

NeoImpact

Data Retention & Deletion

Retention

Data is retained for the duration of the client contract unless otherwise requested

Verification

A dry run system is used to check and verify client data before deletion

Deletion Requests

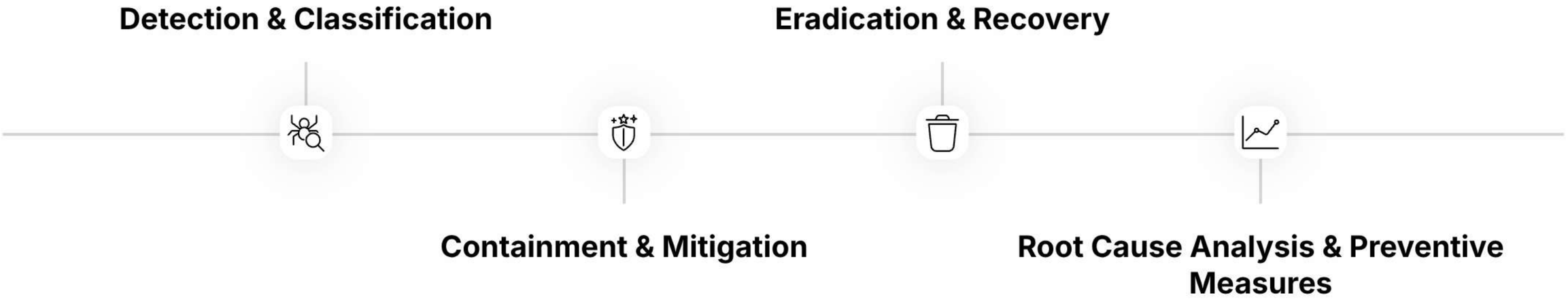
Clients may request deletion of their data at any time

Secure Wipe

Deletion requests follow a secure wipe process with cryptographic erasure verification

Monitoring & Incident Response

Continuous monitoring of infrastructure for unauthorized access attempts, unusual data transfer patterns, and potential vulnerabilities



Incident response process aligned with ISO 27035

Clients are notified of any confirmed data breach within **3 hours** in accordance with contractual and legal requirements.

Compliance & Certification

Hosting Provider

AWS, with ISO 27001 and SOC 2 compliance

ISO 27001

Information Security Management

ISO 27701

Privacy Information Management

NeoImpact Alignment

NeoImpact policies and controls are designed to align with:

- ISO 27001 (Information Security Management)
- ISO 27701 (Privacy Information Management)
- GDPR / CCPA / other applicable privacy laws

Client Responsibilities

ESG Taxonomy

Define and maintain the ESG taxonomy to be used for PortCo uploads

PortCo Management

Ensure PortCo representatives have the necessary permissions and training

Anomaly Reporting

Notify NeoImpact of any access changes or anomalies

Policy Review & Updates

Review Schedule

This policy is reviewed annually or upon significant infrastructure change

Availability

The latest version is always available upon request

Contact Information

For any questions, data requests or to request a copy of this policy, please contact:
webmaster@neoimpact.com

1 Annual Review

Scheduled policy assessment

2 Infrastructure Changes

Review triggered by system updates

3 Regulatory Updates

Compliance with new requirements

NeoImpact is committed to maintaining the highest standards of data security and privacy. Our policies evolve with the changing technology landscape and regulatory environment to ensure continuous protection of your valuable ESG data.