ClearRock Security & Privacy Overview

Effective Date: May 12, 2026

ClearRock, Inc. (ClearRock) provides executive coaching, leadership development, talent optimization, and career transition services. Protecting the confidentiality, privacy, and security of client and participant information is fundamental to how we operate.

This Security & Privacy Overview describes how ClearRock manages and protects information in connection with its services.

1. Our Operating Model

ClearRock is a fully remote organization and does not operate on-premise servers or proprietary infrastructure.

Information used in connection with our services is stored and processed using reputable cloud-based software platforms hosted and secured by their respective vendors.

ClearRock focuses its internal security practices on protecting the devices, identities, and access methods through which our team accesses those platforms and client data.

2. Roles in Data Processing

In most engagements:

- The client organization acts as the data controller with respect to personal data relating to its employees or former employees.
- ClearRock acts as a service provider and, where applicable under data protection law, as a data processor that processes personal data solely to deliver the contracted services.

ClearRock processes personal information only for the purpose of providing coaching, leadership development, career transition, and related consulting services.

3. Types of Information We Handle

Depending on the engagement, ClearRock may process:

- Contact and professional information
- Coaching notes and reflections
- Assessments, goals, and progress tracking
- Engagement reports and aggregated insights
- Administrative and billing information
- Communications related to the engagement

Information processed in connection with the services is referred to as Service Data.

4. Coaching Confidentiality

Confidentiality is central to ClearRock's coaching model.

ClearRock treats all coaching discussions, notes, and related Service Data as confidential. Individual-level coaching content is not shared with sponsoring organizations except:

- in aggregated or anonymized form
- with explicit authorization from the coaching participant
- or where required by law

Client reporting typically focuses on participation status, general themes, and high-level progress indicators consistent with professional coaching practices.

5. Security Practices

ClearRock maintains commercially reasonable administrative, technical, and organizational safeguards designed to protect Service Data from unauthorized access, disclosure, alteration, or destruction. ClearRock maintains administrative, technical, and organizational safeguards designed to protect Service Data from unauthorized access, disclosure, alteration, or destruction, in accordance with applicable law and industry best practices.

Our security practices focus primarily on securing user access to cloud-based systems and include:

Endpoint Protection

Managed endpoint protection is used on team devices to detect and prevent malware, ransomware, and other threats.

Identity Monitoring

Identity monitoring tools help detect suspicious sign-in activity or credential misuse that could lead to unauthorized access.

Email Security

Email filtering and monitoring help protect against phishing, impersonation attempts, and malicious links.

Device Management

Devices used to access ClearRock systems are monitored and maintained to ensure operating systems and applications remain up to date with security patches.

These measures are designed to reduce the risk of unauthorized access to cloud-based systems and information.

6. Cloud Platforms and Sub-Processors

ClearRock uses trusted cloud platforms to support service delivery and business operations.

These platforms may store or process Service Data on ClearRock's behalf and therefore may act as sub-processors under applicable data protection law.

Examples of such platforms may include systems used for:

- customer relationship management
- invoicing and accounting
- coaching documentation and progress tracking
- email and collaboration

These platforms are hosted and secured by their respective providers. ClearRock does not manage the underlying infrastructure of these systems but selects vendors that maintain appropriate security and data protection practices.

A current list of major service providers is available upon reasonable request.

7. Use of AI-Enabled Tools

ClearRock may use AI-enabled tools in a limited, assistive manner to support certain aspects of service delivery and internal operations, such as:

- notetaking support
- summarization of information
- report drafting
- internal analysis

AI tools are used to assist ClearRock professionals, not to replace professional judgment.

Where AI tools process personal information, they do so only at ClearRock's direction and solely to support the delivery of services.

ClearRock does not permit client or participant data to be used to train public or shared AI models.

All AI-generated outputs are subject to human review before being used in client communications or deliverables.

8. Recording of Meetings and Sessions

ClearRock does not routinely record coaching sessions. Recording of meetings, workshops, or group sessions may occur in limited circumstances for legitimate purposes such as documentation, quality assurance, or participant access. In such cases:

- recording is conducted only with appropriate notice and, where required, consent

- participants are informed in advance when a session will be recorded
- recordings are accessed only by authorized individuals and used solely for the intended purpose
- recordings are retained only as long as reasonably necessary and then deleted in accordance with our data retention practices

Coaching sessions involving sensitive personal discussions are generally not recorded unless there is a specific and agreed-upon reason to do so.

9. Data Retention

ClearRock retains Service Data only for as long as reasonably necessary to:

- deliver services
- maintain appropriate business records
- comply with legal, regulatory, and professional obligations

Upon request and subject to applicable retention obligations, ClearRock may delete or anonymize engagement-related Service Data.

10. International Data Protection Considerations

ClearRock primarily operates in the United States but may occasionally provide services to individuals located in the United Kingdom or European Union.

Where applicable, ClearRock shall process personal data in accordance with relevant data protection laws, including the EU General Data Protection Regulation (GDPR) and UK GDPR.

11. Security Limitations

While ClearRock implements safeguards designed to protect Service Data, no security measure can eliminate all risk.

ClearRock applies a risk-based approach to security that is appropriate to the nature of its services and the information processed.

12. Updates to This Overview

ClearRock may update this Security & Privacy Overview from time to time to reflect changes in technology, business practices, or legal requirements.

The most current version will always be available on our website.

13. Contact

For questions regarding privacy, security, or data protection practices, please contact **privacy@clearrock.com**