Security and infrastructure

White paper on how the CoreClarity platform protects client data: hosting, security controls, AI and privacy.

Published
November 2026 · Version 2.1

Prepared by
Meridian West Ltd. and Rubiklab Ltd.

Contact
info@coreclarity.ai

At a glance

CoreClarity is hosted on Google Cloud in Frankfurt, so client data is stored in the European Union. Rubiklab's parent company, DataExpert Services Kft., holds ISO/IEC 27001:2022 certification. Data is encrypted at rest and in transit and kept separate for each client. Client data is never used to train an AI model, and AI only works on material that has already been cleaned, structured and validated.

Hosting
Google Cloud, Frankfurt

Data protection
UK and EU GDPR

Certification
ISO/IEC 27001:2022

Encryption
AES-256 · TLS 1.2+

Penetration test
Red Sentry, 3 December 2025

Model training
Never on client data

Contents

01	Introduction and responsibilities	03
02	Technology infrastructure	04
03	Data security framework	05
04	AI and analytics architecture	06
05	Data protection and privacy	07
06	Incident response and continuity	08
07	People and access	09
08	Client data protection	10
09	Compliance and assurance	11
10	Security roadmap	12
	Glossary	13

Evidence. Certificates, the penetration test confirmation and our policies are available under NDA. Statements describe controls in place in November 2026.

01

Introduction and responsibilities

How CoreClarity protects client data, and which organisation is responsible for each part of the service.

1.1 About CoreClarity

CoreClarity is a joint venture between Meridian West Ltd. and Rubiklab Ltd. Meridian West is a London based insight and management consultancy that has worked with professional services firms, financial institutions, private equity and B2B businesses since 2001.

Rubiklab, part of the DataExpert group, owns and operates the technology, which it has developed with Meridian West since 2023.

1.2 What the platform does

CoreClarity turns complex, largely unstructured material such as interviews, surveys and reports into findings that can be traced back to their source. It combines Meridian West's research methods with statistical analysis, language processing and large language models.

1.3 Who does what

ORGANISATION	DATA PROTECTION ROLE	RESPONSIBLE FOR
Client	Controller	Deciding what data is shared and why. Managing its own users.
Meridian West Ltd.	Processor	The client contract and data processing agreement, research design, analysis and reporting.
Rubiklab Ltd.	Sub-processor	Platform development, hosting, security operations and AI configuration.
Google Cloud	Sub-processor	Data centres, physical security, infrastructure and AI model serving.

1.4 Who this paper is for

Procurement	Clients assessing CoreClarity before purchase
IT and security	Teams reviewing technical controls
Risk and compliance	Officers assessing regulatory obligations
Technology partners	Organisations considering integration

Joint venture
Meridian West and Rubiklab

Technology owner and operator
Rubiklab Ltd.

Serving clients since
2001

02

Technology infrastructure

CoreClarity runs on Google Cloud Platform. Client data is stored in Frankfurt and stays within the European Union.

2.1 Cloud platform

Google Cloud provides the data centres, network and managed services. Physical security, power and hardware are Google's responsibility and are covered by Google's own ISO/IEC 27001, 27017 and 27018 certifications and SOC 2 reports.

2.2 Data storage

Backups	Automated and encrypted
At rest	AES-256 encryption
In transit	TLS 1.2 or higher
Access	Role based, with audit logging

2.3 Availability

Services run on Google Cloud in Frankfurt and scale with demand. Maintenance is scheduled outside UK and EU business hours. Monitoring runs continuously, and automated alerts go to the responsible engineers when an issue occurs.

2.4 Integration

API	Documented REST API
Authentication	Token based, scoped to one client
Import	Documents (PDF, DOCX, PPT, PPTX, TXT, JSON), recordings (MP3, WAV, M4A, MP4, MOV) and data files (CSV, XLS, XLSX, SAV)
Export	Word, Excel, PowerPoint and Markdown, plus audio and video clips
Streaming	Chat answers stream in real time, in the app and over the API

2.5 Infrastructure security

Firewall rules, private networking and a web application firewall protect the service. Development follows the OWASP Top 10. Patches are tested and applied automatically, with an emergency process for high-risk vulnerabilities.

Cloud provider
Google Cloud Platform

Primary region
Frankfurt, Germany

Data residency
European Union

03

Data security framework

Certified management systems, encryption throughout, and access limited to what each person needs.

3.1 ISO/IEC 27001

Rubiklab, which builds and runs CoreClarity, is part of the DataExpert group. Its parent, DataExpert Services Kft., is certified to ISO/IEC 27001:2022 by CERTOP (registration 01-22605/26-16952, valid until August 2029) for data processing and development. All 93 Annex A controls are applied, with annual independent audits.

DataExpert Services Kft. is also certified to ISO 9001:2015 for quality management. Meridian West holds Cyber Essentials Plus.

Certificates are available on request.

3.2 Encryption and integrity

Data at rest	AES-256
Data in transit	TLS 1.2 or higher
Keys	Managed key management, with logged access and regular rotation
Backups	Encrypted, with full restores tested at least annually
Disposal	Deleted on request and at contract end (see 8.4)

3.3 Access control

Access follows a zero trust model: every request is checked for identity and permission, wherever it comes from. Staff can reach only what their role needs. Access to production systems requires multi-factor authentication and is reviewed periodically. Every access to client data is logged, and logs are held centrally, protected from change, for at least six months.

3.4 Monitoring

Automated monitoring and intrusion detection watch for threats, misconfiguration, unusual access and performance problems. Alerts go to the technical team, and findings feed into vulnerability management.

3.5 Independent testing

Web application	Annual penetration test by Red Sentry, last completed 3 December 2025
Infrastructure	Internet-facing infrastructure and APIs are in the annual test
Vulnerabilities	Automated scanning, at least monthly
Code	Peer review, static and dynamic analysis, dependency checks

Certification
ISO/IEC 27001

Encryption
AES-256 at rest, TLS 1.2+ in transit

Access model
Zero trust, MFA

04

AI and analytics architecture

AI in CoreClarity supports expert judgement. Statistical methods, language processing and large language models work together, and every finding can be traced to its source.

4.1 Structure before AI

Material is prepared before any model interprets it. A 25 step validation protocol cleans, checks and structures data, with quality checks and error handling at each stage.

4.2 Language models

Large language models are used under enterprise terms that prohibit the provider from using customer data to train its models. The platform does not search the web to answer questions: answers come only from the client's own sources.

4.3 Validating outputs

Automated checks	Accuracy and consistency checks on every output
Cross reference	Against traditional statistical methods
Citations	Every finding links to the passages it relies on, so the client's own reviewers can check it
Reports we write	Reports Meridian West or Rubiklab prepare for a client are reviewed by a person before release

4.4 AI-specific risks

Prompt injection	Text inside client documents is treated as data, never as instructions, and model actions are limited by the orchestration layer
Cross-client exposure	Each project has its own search index, and every query is limited to one client
Model changes	Model versions are recorded, and changes are tested before release

4.5 Client data never trains a model

Client material is processed for the client's own project and nothing else. It is never used to train, fine tune or calibrate any AI model, whether CoreClarity's own, one built for that client, or a third party's. AI use is governed by Rubiklab's AI Ethics and Governance Policy, available on request.

Sources
The client's own only

Training on client data
Never

Traceability
Every finding cited

05

Data protection and privacy

Privacy is designed into CoreClarity from the start, under UK and EU data protection law.

5.1 Legal framework

United Kingdom	UK GDPR and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025
European Union	EU GDPR, and the EU AI Act where it applies. CoreClarity assists human analysis and makes no automated decisions about individuals
United States	CCPA, acting as a service provider to clients subject to it
Sector rules	Contract terms to support clients' own obligations, such as DORA for financial services

5.2 Agreements and roles

Every engagement is covered by a data processing agreement reflecting the roles in 1.3. As processor we act only on the client's documented instructions and keep records of processing. Rubiklab's Data Protection Officer is Illitch Real.

5.3 Sub-processors

Sub-processors are engaged only under written agreements that include confidentiality, security and data protection obligations. The current list comes with the data processing agreement, and clients are told in advance of any new sub-processor and can object.

5.4 Location and transfers

Client data is stored in the EU. UK staff access it under the EU's adequacy decision for the UK, renewed in December 2025 and valid until December 2031. Any transfer outside the UK and EU uses Standard Contractual Clauses or the UK IDTA, with a risk assessment.

5.5 Rights and privacy by design

All data subject rights are supported, and requests are answered within the one month the law allows. A data protection impact assessment comes before any new high-risk processing, and names of people, organisations and occupations can be redacted from transcripts at upload.

Primary regime
UK GDPR and EU GDPR

Data location
Frankfurt, EU

Transfers
Adequacy, SCCs or IDTA

06

Incident response and continuity

Contain incidents quickly, tell clients promptly, and restore the service from verified backups.

6.1 Detection

Automated monitoring and human review work together to separate genuine threats from false alarms, so real incidents get a fast response.

6.2 Response steps

Rubiklab follows a documented Incident Response and Recovery Plan.

1 Assess	Classify the incident and establish its scope
2 Contain	Isolate affected systems and accounts
3 Preserve	Keep logs and evidence for investigation
4 Remove	Eliminate the cause
5 Recover	Restore service from verified backups
6 Notify	Inform affected clients (see 6.3)
7 Review	Root cause analysis, with lessons fed back into procedures

6.3 Telling clients

If a personal data breach affects a client's data, we notify the client without undue delay and within 24 hours of confirming it, with the facts known at the time. This leaves the client time to meet the 72 hour deadline for reporting to a regulator.

6.4 Continuity and recovery

Backups	Automated, encrypted and tested by full restores
Plans	Documented business continuity and disaster recovery plans
Testing	Business continuity and disaster recovery tested at least annually, incident response several times a year

Client notice
Within 24 hours

Recovery
Documented and tested

Testing
Restores and drills

07

People and access

Everyone at Meridian West and Rubiklab who works on CoreClarity follows the same security rules.

7.1 Screening and training

Staff with access to client data are screened before they start, with identity, right to work, CV, reference and criminal record checks, and sign confidentiality agreements. Security and data protection training begins on the first day and is refreshed at least annually, for contractors and interns as well as employees. Staff who work with AI also receive AI literacy training, in line with the EU AI Act.

7.2 Access management

Staff access follows least privilege. Joiner, mover and leaver processes update access promptly, and sensitive operations require additional verification.

7.3 Devices and data handling

Company devices	Encrypted, updated automatically, managed remotely
Personal devices	Cannot connect to internal systems: remote access is limited to company-managed devices, with MFA
Data handling	Training in classification, storage and disposal
Assurance	Checked through internal audit

7.4 Reporting concerns

Staff have clear channels for raising security concerns without fear of blame, and each person knows their role in an incident.

7.5 Suppliers

Suppliers that handle client data are assessed for security, data protection and incident response before they are engaged, and reviewed periodically.

Training

From day one, refreshed annually

Authentication

MFA on all systems

Devices

Encrypted and centrally managed

08

Client data protection

Clients trust us with sensitive business intelligence and client feedback. Each client's data is kept apart and stays under that client's control.

8.1 Separation between clients

Each client's data is kept apart by access controls in the application, and each project has its own search index, so a user working for one client cannot reach another client's data.

8.2 Client controls

Users and permissions	Managed by the client's own administrators
Sign-in	A one-time code sent by email, or single sign-on with Microsoft Entra ID
Retention	Set to the client's policy
Activity	Access and activity reports on request

8.3 Data lifecycle

Data is encrypted from the moment it enters the platform and validated before processing. Stored data is encrypted at rest, and every access and change is recorded.

8.4 End of an engagement

When an engagement ends, client data is returned or deleted, as the client chooses,. Deletion is confirmed in writing.

8.5 Working with your security team

We complete security questionnaires, join calls with IT and risk reviewers, and share evidence under NDA.

Separation
Per client

Sign-in
Email code or Microsoft SSO

Exit
Return or delete, confirmed in writing

09

Compliance and assurance

Independent checks are how we demonstrate our security, and the evidence is available for clients' own due diligence.

9.1 Penetration testing

Red Sentry carried out an independent web application penetration test of the Rubiklab platform that runs CoreClarity, completed on 3 December 2025, with a Grade A outcome. Findings are tracked to resolution and retested where needed. The confirmation letter is available under NDA. The next test is due by December 2026.

9.2 Certifications

DataExpert Services Kft.	ISO/IEC 27001:2022 and ISO 9001:2015, certified by CERTOP until August 2029
Meridian West Ltd.	Cyber Essentials Plus
Google Cloud	ISO/IEC 27001, 27017 and 27018, SOC 2
ISO/IEC 42001	Governance mapped against the standard, ahead of certification

9.3 Ongoing assurance

Internal audits, management reviews and annual surveillance audits under the ISO/IEC 27001 certificate. Findings are tracked until closed.

9.4 Client requirements

We can agree audit rights, exit arrangements and incident terms, including those financial services clients need under DORA, and support clients' supplier assurance reviews. Meridian West holds public liability, professional indemnity, employer's liability and product liability insurance.

Penetration test
Red Sentry, 3 December 2025

Certification
ISO/IEC 27001

Next test
December 2026

10

Security roadmap

Our priorities for the next twelve months.

10.1 AI management system

Working towards certification to ISO/IEC 42001.

10.2 Infrastructure

Continued investment in resilience and in isolation between workloads.

10.3 AI security

Monitoring for unusual model behaviour, and prompt injection testing added to the annual penetration test.

10.4 Encryption

Customer-managed encryption keys for clients who want them, and a review of readiness for post-quantum cryptography.

10.5 Regulation

EU AI Act obligations as they take effect, and guidance issued under the Data (Use and Access) Act 2025.

Next certification
ISO/IEC 42001

Resilience
Continued investment

Horizon
Post-quantum readiness

Glossary

AES-256
Advanced Encryption Standard with a 256-bit key, used to protect stored data.

API
Application Programming Interface: the way other software connects to the platform.

Audit trail
A time-ordered record of activity in a system, kept as evidence.

Data controller
The organisation that decides why and how personal data is processed.

Data processor
An organisation that processes personal data on a controller's behalf.

DPIA
Data protection impact assessment: a structured review of privacy risk before new processing starts.

IDTA
International Data Transfer Agreement: the UK's approved contract for sending personal data abroad.

ISO/IEC 27001
The international standard for information security management systems.

ISO/IEC 42001
The international standard for AI management systems.

MFA
Multi-factor authentication: two or more checks are needed to sign in.

Penetration test
An authorised, simulated attack carried out to find weaknesses.

Prompt injection
An attempt to manipulate an AI model through instructions hidden in the material it reads.

SCCs
Standard Contractual Clauses: the EU's approved contract terms for transferring personal data abroad.

Single sign-on
Signing in once with an organisation's own identity provider to reach several systems.

Sub-processor
A company engaged by a processor to help process personal data.

TLS
Transport Layer Security: the protocol that encrypts data in transit.

Zero trust
A security model that verifies every access request, wherever it comes from.

CoreClarity

Questions from your security team?

We will answer security questionnaires, join a call with your IT and risk reviewers, and share certification and testing evidence under NDA.

Contact
info@coreclarity.ai
+44 (0)20 7261 4700

Meridian West Ltd.
Uncommon, 1 Long Lane
London SE1 4PG

Rubiklab Ltd.
1A Falmer Court, London Road
Uckfield TN22 1HN
Company no. 14018118

CoreClarity is a joint venture between Meridian West Ltd. and Rubiklab Ltd., part of the DataExpert group. Rubiklab owns and operates the technology. This document describes controls in place in November 2026 and is reviewed annually. Version 2.1.