



Data Storage Policy

Data Storage Policy

Data Storage and Protection Policy — Black Box Smart Data LLP

This policy outlines how Black Box Smart Data LLP stores and protects client data using Hetzner for data hosting and Nextcloud, Astrolabe, Qdrant, and Mistral AI for secure knowledge access and processing workflows.

1) Purpose

The purpose of this policy is to define how client data is securely stored, accessed, and protected across our hosting and AI-assisted search stack.

2) Scope

This policy applies to all client data stored within Hetzner data centres and any client-related information accessed via Scout AI within our environment. It covers technical controls, access management principles, hosting locations, and compliance claims directly provided by our vendors.

3) Data Storage Architecture

Black Box Smart Data LLP stores client data in Hetzner data centres located in Germany and Finland. These facilities provide geo-redundant high-speed fibre optic connectivity and robust resilience standards.

Hetzner data centres are ISO 27001 certified and implement extensive physical security, including perimeter protection, CCTV, rigorous access control, and advanced intruder alarms. They also employ certified fire-rated construction, very early fire detection, and nitrogen fire suppression for critical rooms.

Scout AI infrastructure and vector database operations are hosted on secure European servers within certified sovereign cloud environments, following ISO 27001 and SOC2 standards, with additional TISAX and BSI C5 certifications.

4) Data Processing with Scout AI

The stated purpose of Scout AI is not to process personal data beyond immediate retrieval, and it does not store user data.

Scout AI does not create unauthorised copies of the source data; instead, it integrates with existing repositories and respects existing access controls.

Scout AI adopts existing access rights from Active Directory/SSO and does not create new access structures, helping ensure least-privilege enforcement remains consistent with our identity provider.



Data Storage Policy

Our AI stack is 100% GDPR compliant and has successfully addressed GDPR compliance and integration of existing access rights in customer deployments.

5) Technical and Organisational Measures (TOMs)

- **Hosting Environment:** Provides a physically secure and resilient environment with ISO 27001 certification, high availability in Germany and Finland, perimeter security, CCTV, rigorous access controls, advanced intruder detection, early smoke detection, and nitrogen fire suppression in critical rooms.
- **Scout AI Environment:** Hosting environment follows ISO 27001 and SOC2 standards, operated on secure European servers within certified cloud environments, with additional certifications including TISAX and BSI C5 for the hosting provider.
- **Access Integration:** Scout AI integrates with existing enterprise identity (Active Directory/SSO) and does not replicate access structures, which reduces risk from access drift and shadow permissions.
- **Data Minimisation:** Scout AI does not store user data and does not create copies of the underlying data, which supports data minimisation and reduces data spread across systems.

6) Compliance Alignment

- **Hosting Infrastructure:** Carries ISO 27001 certification, evidencing information security best practices at the data centre level.
- **Scout AI Tech Stack:** States adherence to ISO 27001 and SOC2 standards and communicates 100% GDPR compliance.

7) Sustainability and Data Centre Operations (Informational)

Hetzner operates on 100% renewable energy with additional sustainability measures such as renewable power sources in Germany and Finland, alongside energy-efficient designs and ISO 50001 for energy management.

8) Access Control Principles

Access to data via Scout AI is constrained by the organisation's existing identity and access management, as the platform adopts existing Active Directory/SSO permissions without creating new access structures.

9) Data Replication and Retention

Scout AI does not create copies of the data being searched, supporting a minimisation approach to data replication across tools.

Organisation-specific retention schedules, archival rules, and deletion procedures are to be defined by Black Box Smart Data LLP and applied at the data source and hosting levels with each organisation.



Data Storage Policy

10) Data Processing Agreements and Documentation

Our sovereign technology stack provides Data Processing Agreements (DPA) and maintains technical and organisational measures alongside a robust SaaS security concept.

11) Operational Responsibilities

Black Box Smart Data LLP is responsible with each client for:

- Defining and maintaining identity, role-based access controls, and conditional access policies consistent with our SSO/Active Directory.
- Configuring repositories and permissions so Scout AI can correctly inherit and enforce existing access rights.
- Managing data lifecycle, retention, and deletion at the data source and storage layers.

Vendors are responsible for: The controls and assurances described in their materials, including data centre certifications and security features for Hetzner, and security posture and integration behaviour for our sovereign AI components (Nextcloud, Astrolabe, Qdrant, and Mistral AI).

12) Exceptions and Changes

Any deviations from this policy require approval by Black Box Smart Data LLP's information security leadership and must maintain alignment with the vendor-stated controls and certifications referenced herein.

13) Summary of Key Vendor Assurances

Hetzner:

- European data centres in Germany and Finland offering high availability and geo-redundant connectivity.
- ISO 27001 certified data centres with strong physical security and fire protection controls.
- Sustainable operations including 100% renewable energy and ISO 50001 for energy management.

Sovereign AI Stack (Nextcloud, Astrolabe, Qdrant, Mistral AI):

- Hosted on secure European servers; follows ISO 27001 and SOC2 standards, with mentions of TISAX and BSI C5 for the hosting environment.
- No user data stored and no copies of source data created; adopts existing AD/SSO access rights.



Data Storage Policy

- Maintains 100% GDPR compliance and successful handling of GDPR requirements in customer deployments.

World-Class Infrastructure & Organisational Accreditations

- **ISO/IEC 27001 Certification:** The gold standard international certification for Information Security Management Systems (ISMS). This independently audited framework ensures that comprehensive, institutional-grade physical and digital security controls protect all hosting environments, development lifecycles, and scanning bureaus.
- **ISO/IEC 27701:2019 & ISO 9001:** Global benchmarks ensuring structural Quality Management alongside rigorous Privacy Information Management Systems (PIMS). This attests that data handling procedures follow maximum corporate transparency and comply fully with UK and European data privacy frameworks.
- **Cyber Essentials Approved:** A vital, government-backed security accreditation confirming that our immediate company perimeter, data transmission boundaries, and operational devices are fully fortified against common vulnerabilities and cyber threats.
- **SOC 2 Type II & BSI C5:** Fully compliant with the stringent security criteria catalogues outlined by the German Federal Office for Information Security (BSI), backed by continuous SOC 2 Type II compliance audits verifying security operational effectiveness over extended observation periods.
- **GDPR Compliance & Zero-Logging:** Operating firmly inside European data protection boundaries, our tech stack supports robust Data Processing Agreements (DPAs). This includes tools for precise data erasure, strict zero corporate logging parameters, and an absolute guarantee that training inputs are never retained.
- **ISO 14001 & ISO 50001 (Green Infrastructure):** Official certifications validating efficient environmental and energy management. The primary Hetzner data centres utilise 100% green energy from renewable sources to power your cloud storage sustainably.
- **DIN EN 50600 / TÜV-Audited Physical Resilience:** The comprehensive European infrastructure standard confirming optimal physical security, advanced fire protection, climate controls, and comprehensive technical resilience against hardware failures or downtime.
- **Open-Source & Open-Weight Sovereignty:** Offering unprecedented transparency compared to closed proprietary "black box" alternatives, our inspectable, auditable stack—powered by Nextcloud and open-weight model architectures—allows for complete deployment choice across hybrid structures, private clouds, or fully secure local servers.

Signed:

On behalf of Black Box Smart Data LLP