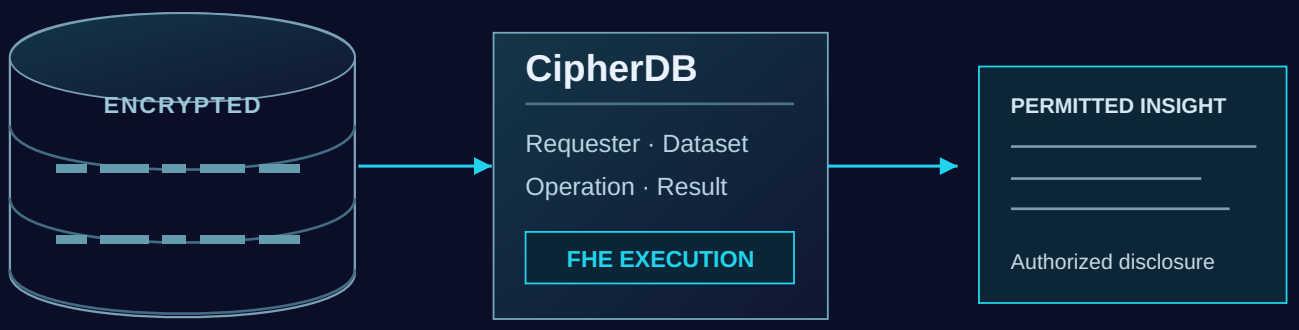
Query sensitive data.
Protect the source.

Use fully homomorphic encryption to run approved analytics across hybrid, multi-cloud and partner environments while source data remains protected.

DATA-IN-USE PROTECTION / CIPHERDB & FHE QUERIES



Data at rest, in transit and in use.

Supported operations over encrypted data.

Encrypted result. Auditable execution.

ARCHITECTURE CAPABILITIES · SUPPORTED OPERATIONS ONLY

3 States

Protect data at rest, in transit and in use

FHE

Perform supported computation on encrypted data

Query-Level

Enforce policy and preserve an auditable access trail

THE BUSINESS CHALLENGE

Secure storage is not secure processing.

Organizations need answers from sensitive databases across clouds, subsidiaries, partners and subcontractors. Conventional collaboration often requires exporting data, creating copies or decrypting records before computation.

Encryption at rest and in transit leaves a gap **at the moment data is used**. A conventional query engine generally exposes plaintext inside its processing environment.

Copies, exports, data clean rooms, proxies and partner-controlled systems add places where raw records can be accessed. Privileged administrators can become part of the trust model even when they do not need to know the underlying data.

The business requirement is usually an answer, score, match or aggregate—not the entire source dataset.

Governance implications

Data minimization · Integrity · Confidentiality
Accountability · Sovereignty · Contractual boundaries[3–4]

THE EXPOSURE BOUNDARY

3

exposure windows

At rest · In transit
During computation

Every copy
Another access, retention and audit scope.

Every privileged path
More people and systems must be trusted.

Organizations need the result, not the raw dataset

Move or reveal the dataset

Privacy, sovereignty and contractual boundaries can prevent copying data into another organization's environment. Network access control alone does not remove plaintext exposure in a query engine.

Move the approved operation

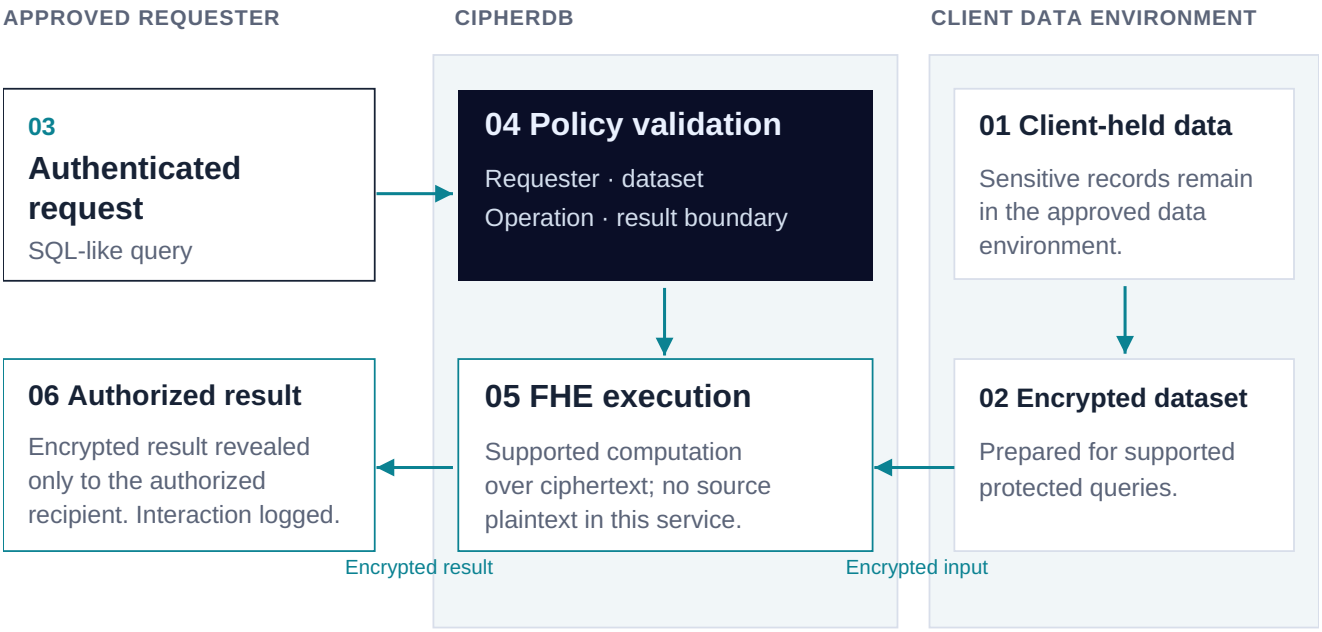
Apply a permitted computation to encrypted data, then return only the authorized result. Limit the dataset, operation and result boundary before execution.

Keep the source protected.
Give the authorized recipient the result.

THE AIDATACY APPROACH

Move the computation. Not the raw dataset.

CipherDB provides a SQL-like query path for supported operations on encrypted data. Query-level policies govern who can request which operation and what result can be disclosed.[1–2]



AUDIT EVIDENCE · Material access and execution events remain reviewable.

iCyWALL can add authenticated network access and session controls around the workflow.

Conceptual workflow from the use-case source. Supported FHE computation returns an encrypted result for authorized disclosure; source plaintext is not exposed to the processing service.

What FHE makes possible

Fully homomorphic encryption lets the processing service evaluate supported operations over ciphertext without learning source plaintext. It returns an encrypted result for authorized disclosure.[1–2]

What the policy must define

Specify the requester, permitted dataset, allowed operation, result boundary, key-management responsibilities and audit requirements. Infrastructure operators do not need routine plaintext access inside the protected path.

Validate the supported workload. Neither unrestricted SQL support nor a universal latency is assumed.

IMPLEMENTATION

From query scope to protected operations.

Define the supported workload, policies, key-management responsibilities and result boundary before production. Scale only the datasets and queries that meet agreed criteria.

01

Assessment & Scoping

Inventory sensitive datasets, query workflows, copies, privileged access paths, and collaboration requirements.

OUTPUT

Data-exposure and workload assessment.

02

Architecture Design

Define identities, permitted queries, dataset boundaries, result disclosure, key-management responsibilities, audit requirements, and acceptance criteria.

OUTPUT

Protected-query architecture and policy model.

03

Pilot Implementation

Connect CipherDB to selected encrypted datasets and the required identity and network controls for a bounded set of supported queries.

OUTPUT

Controlled protected-processing pilot.

04

Performance Testing

Measure query correctness, policy enforcement, plaintext isolation, audit coverage, and workload performance against agreed baselines.

OUTPUT

Validated workload and test evidence.

05

Production Rollout

Scale approved datasets, queries, users, and partner workflows while integrating monitoring and governance.

OUTPUT

Production privacy-preserving data service.

06

Continuous Optimization

Optimize supported queries and performance, review policies and audit evidence, and govern onboarding of new workloads and partners.

OUTPUT

Continuously governed protected-data operations.

Deployment roadmap

PHASE 1

Discover

inventory sensitive datasets, recurring queries, data copies, privileged paths, and collaboration needs.

PHASE 2

Define

select supported operations and establish identities, permitted datasets, result boundaries, key responsibilities, and acceptance criteria.

PHASE 3

Pilot

validate correctness, policy enforcement, plaintext isolation, audit coverage, and workload performance.

PHASE 4

Scale

extend only approved datasets and queries, integrate governance, and onboard additional users or partners through the same controlled model.

BUSINESS IMPACT

Less exposure. Stronger governance evidence.

Enable approved insights without unnecessary source-data copies. Reduce routine privileged plaintext access and retain evidence of material interactions.

Collaborate

Protected Collaboration

Partners can obtain approved insights without receiving the full source dataset, reducing unnecessary data movement and exposure.

Limit

Reduced Privileged Exposure

Infrastructure operators can support computation without routine access to plaintext inside the protected query path.

Govern

Stronger Governance Evidence

Query-level policy and audit records support data-minimization, sovereignty and accountability objectives, while the organization retains responsibility for its wider compliance program.

Governance objectives and architecture contribution

Objective	Contribution within the defined workflow
GDPR · Data minimization	Return a permitted result instead of sharing the full source dataset.
GDPR · Integrity and confidentiality	Protect supported computation and govern result disclosure.
GDPR · Accountability	Record material access and execution events for review.
Sovereignty and contractual boundaries	Define dataset boundaries, permitted operations and the authorized result path.

Acceptance testing covers **query correctness, policy enforcement, plaintext isolation, audit coverage and workload performance** against agreed baselines. Only approved datasets and supported queries are extended into production.

GDPR principles and the EU Data Act are retained as source context.[3–4] Technology alone does not create compliance; wider legal, operational and governance responsibilities remain with the organization.

NEXT STEPS

Start with the result your business needs.

FROM A SENSITIVE QUERY TO A CONTROLLED RESULT

Assess a Protected-Query Use Case

Select a recurring sensitive-data query and define the boundary around its approved answer. Keep the source protected; give the authorized recipient the result.

- → Map datasets, existing copies, privileged paths and the collaboration need.
- → Define supported operations, requester identity, result disclosure and key responsibilities.
- → Validate correctness, policy enforcement, plaintext isolation, audit and workload performance.

contact@aidatacy.com

aidatacy.com ↗

References & sources

01 NIST — Fully Homomorphic Encryption (FHE)
https://csrc.nist.gov/Projects/pec/fhe

02 HomomorphicEncryption.org
https://homomorphicencryption.org/

03 European Commission — Principles of the GDPR
https://commission.europa.eu/law/law-topic/data-protection/information-business-and-organisations/principles-gdpr_en

04 EUR-Lex — Regulation (EU) 2023/2854
https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng

Source basis: “USECASE iCYWALL.xlsx”, UC 02 EN narrative and source URLs. Reference descriptors identify the institution or regulation; they do not imply product certification or automatic compliance.