

ARCHITECTURE BRIEF

Your data stays on your own infrastructure.

Each Hirebase deployment runs single-tenant, inside your own Azure tenancy, on your own accounts. There is no shared database, no cross-tenant surface, and no vendor-held copy of your workforce data.

Single

Tenant — dedicated environment per client, not shared SaaS

Zero

Cross-tenant leakage surface by design

100%

Client-owned Azure deployment and data

99.9%

Contracted platform uptime SLA

Architecture

DATA OWNERSHIP

Belongs entirely to the client

Hirebase does not hold workforce data on infrastructure it operates or retains rights to.

REGION

No restrictions by default

The deployment sits inside whatever Azure region the client's own tenant already uses.

RETENTION

Configured per client policy

Set by client governance, not a fixed vendor schedule, since the infrastructure is already the client's to govern.

ISOLATION

No cross-tenant surface

No shared multi-tenant database, so there is no cross-tenant leakage surface to manage.

COMPLIANCE POSTURE

Inherited, not layered on

Deployed into the client's own Azure tenancy, the system inherits the compliance posture already maintained there.

RESIDENCY & DPAS

Solved once

One client-hosted system, not a data-processing agreement to renegotiate with every vendor in an assembled stack.

What this changes for your review

A shared-SaaS vendor asks you to...

- Trust an environment you cannot inspect
- Accept the vendor's own data-retention schedule
- Negotiate residency and DPA terms from scratch
- Depend on the vendor's own access controls and admin staff

Hirebase runs in the cloud you already govern

- Reviewed the same way as everything else in your Azure tenant
- Retention set by your own policy, not ours
- Residency and DPA terms already settled inside your tenancy
- Access governed by your own Azure identity and policy controls

THE BOTTOM LINE

Hirebase runs inside infrastructure you already own, govern and audit. There is no vendor-operated environment to inspect and no vendor-held copy of your workforce data — your security review covers the same tenant, the same identity controls and the same policies you already apply across your Azure estate.