YOUR DATABASE.
YOUR DATA.
YOUR CALL.

Independent vs Shared Database Models in Facial Recognition

A guide for UK retailers

FACE TECH
THE ETHICAL AI COMPANY

BEFORE YOU SIGN ANYTHING

TWO MODELS. ONE RIGHT ANSWER.

Not all facial recognition databases are configured the same way. Before your organisation commits to a provider, you need to understand how your biometric data will be stored — and who else it will be stored alongside.

✕ SHARED DATABASE

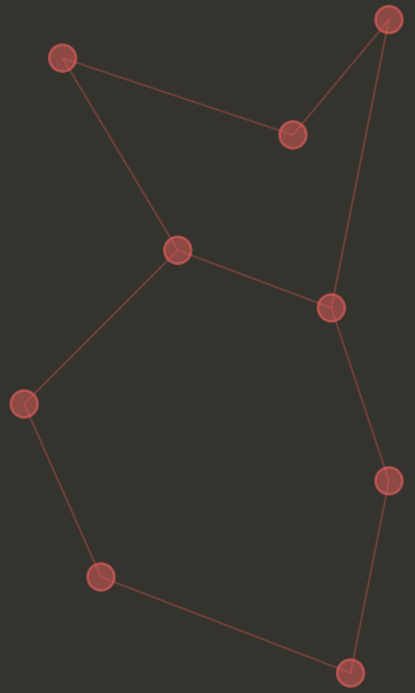
Your biometric data sits in the same database as other organisations. You share infrastructure, storage, and — in some configurations — watchlist data.

✓ INDEPENDENT DATABASE

Your biometric data is stored in a database dedicated exclusively to your organisation. No other retailer's data shares your environment. Full isolation.

SECTION ONE

THE SHARED DATABASE MODEL.

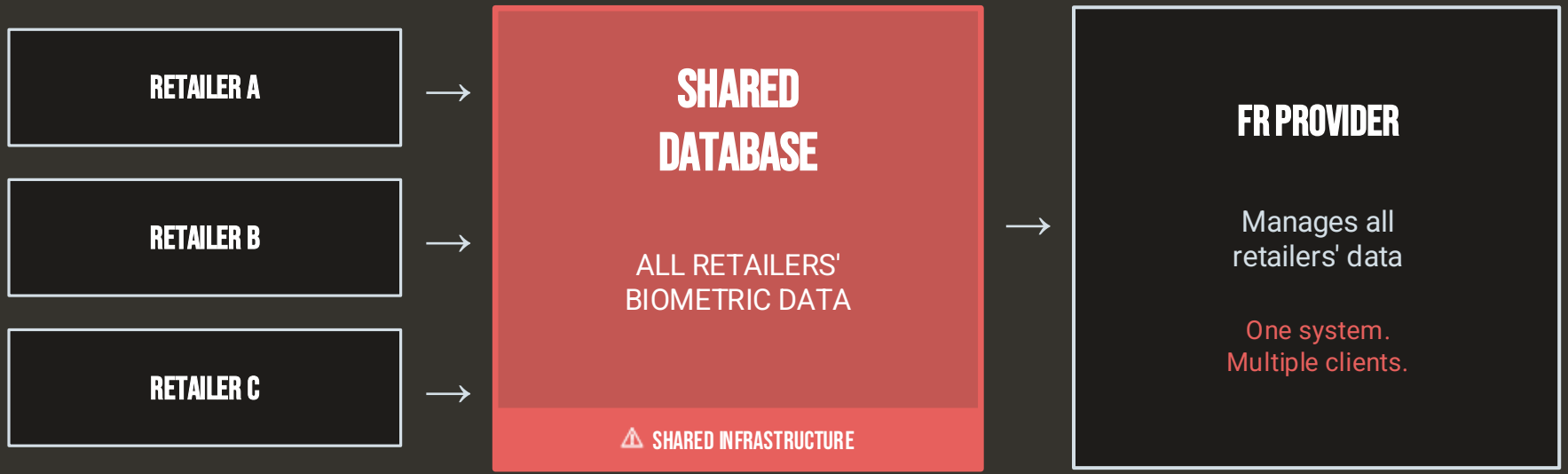


What it is. Why it's a problem.

HOW IT WORKS

IN A SHARED MODEL, YOUR DATA IS POOLED.

Multiple retailers enrol face profiles into the same underlying database. Your data sits alongside data from Retailer B, C, and D — managed by one provider, on shared infrastructure.



RISK ONE — DATA CONTAMINATION

ONE BAD RECORD IN. EVERYONE'S AFFECTED.

If another retailer incorrectly enrolls a person — a case of mistaken identity, a staff error, or a malicious entry — that record now sits in the same database your store queries. You had no say in it. You may not even know it happened.

Their mistake. Your legal exposure.

FALSE ALERTS IN YOUR STORE

Your system flags someone based on a record you didn't create and cannot verify.

WRONGFUL ACCUSATION RISK

An incorrect enrolment from a competitor becomes your legal exposure when you act on it.

NO AUDIT TRAIL TO SOURCE

In a shared database you cannot always trace which organisation created a specific profile.

RISK ONE — THRESHOLD MISMATCH

NOT EVERY RETAILER DRAWS THE LINE IN THE SAME PLACE.

Every retailer sets their own internal threshold for watchlist enrolment. In a shared database, those thresholds collide — and the consequences fall on everyone in the pool.

INDEPENDENT CONVENIENCE STORE

Threshold: any theft, any value.

A 14-year-old takes a £1 chocolate bar. The store owner enrolls them on the watchlist. It goes into the shared database.

NATIONAL RETAILER

Threshold: £200+ and repeat behaviour.

Would never enrol a teenager over a chocolate bar. Considers that individual vulnerable. Their policy prohibits it. But that profile is now live in their system.

THE NATIONAL RETAILER NEVER MADE THAT CALL. BUT THEY OWN THE OUTCOME.

That 14-year-old walks into a national retailer. The FR system — fed by a shared database — flags them. Staff are alerted. The teenager is approached or refused entry.

SAFEGUARDING BREACH

Flagging a minor based on a record the retailer never assessed or approved may breach their own safeguarding policy and ICO guidance on proportionate use of biometrics.

UK GDPR PROPORTIONALITY FAILURE

Article 5(1)(a) requires processing to be lawful, fair, and transparent. Processing a child's biometric data without your own lawful basis — inherited from someone else — is none of these.

REPUTATIONAL DAMAGE

'National retailer flags 14-year-old for stealing a chocolate bar' is a headline. The fact that another organisation made the enrolment decision will not protect you in the press.

EQUALITY ACT EXPOSURE

Age is a protected characteristic. Disproportionate treatment of a minor — based on a record you never created — opens the door to discrimination claims.

RISK TWO — GDPR COMPLIANCE

CAN YOU PROVE WHOSE DATA IS WHOSE?

Under UK GDPR Article 5(2) — the Accountability Principle — you must be able to demonstrate compliance at any time. In a shared database, proving data provenance becomes extremely difficult.

The ICO doesn't care whose database it was.

ARTICLE 5(2) — ACCOUNTABILITY

You must demonstrate compliance. Shared databases make this almost impossible to evidence.

ARTICLE 30 — RECORDS OF PROCESSING

Your records must reflect the data you hold. How do you document data you don't fully control?

ARTICLE 17 — RIGHT TO ERASURE

If an individual requests deletion, can you guarantee their record is removed from a shared environment?

RISK THREE — COMMERCIAL SENSITIVITY

YOUR WATCHLIST IS YOUR CRIME MAP.

Every profile on your watchlist represents intelligence about your own crime environment — who is targeting you, which stores, and how often. That is commercially sensitive data. In a shared database, it is available to the same system that serves your competitors.

WHAT'S IN YOUR WATCHLIST

- Known shoplifters & ORC members
- Persons subject to banning orders
- Individuals under civil recovery
- Staff dismissed for theft or misconduct

WHY IT'S COMPETITIVE INTEL

- Crime volume signals footfall & revenue patterns
- Hotspot stores reveal your security weak points
- ORC targeting reveals your supply chain exposure
- Sharing it benefits rivals — never you

SECTION TWO

THE INDEPENDENT MODEL.

What it looks like. Why it's the only right choice.

THE INDEPENDENT MODEL

DEDICATED. SILOED. YOURS ONLY.

FACE TECH
THE ETHICAL AI COMPANY

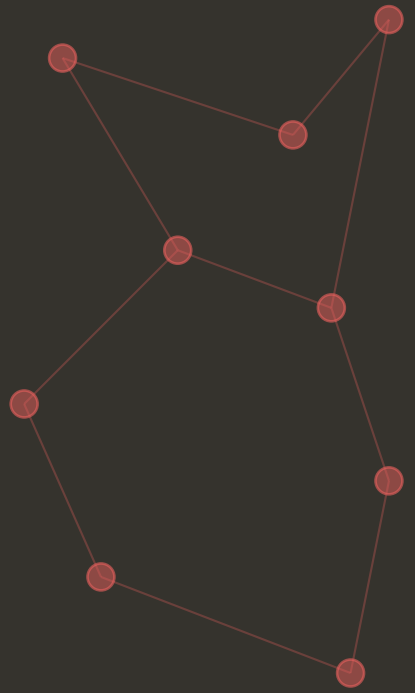
In an independent model, your FR provider hosts a dedicated database instance for your organisation alone. No other retailer's data is stored alongside yours. You are the only client in your environment.

YOUR ORGANISATION → **DEDICATED DATABASE**
Your data only.
No other organisation.
→ **FR PROVIDER**
Manages.
Never shares.

- ✓ No cross-contamination
- ✓ Full GDPR accountability
- ✓ Complete audit trail
- ✓ Your data. Your control.

SECTION THREE

THE UK RETAIL CONTEXT.



ORC. Opportunist theft. Staff misconduct.

YOUR INTELLIGENCE IS YOURS.

ORC GANG

AN ORC GANG TARGETS MULTIPLE RETAIL CHAINS ACROSS A REGION.

SHARED:

Gang members enrolled by Retailer A appear in your system — even if you never agreed to cross-enrolment. If their data is inaccurate, wrong people get flagged across the whole retail network.

INDEPENDENT:

You enrol only individuals based on your own evidence, your own incidents, and your own legal basis. Your records are clean, accurate, and defensible in court.

OPPORTUNIST

A REPEAT SHOPLIFTER TARGETS A SINGLE STORE ON YOUR RETAIL PARK.

SHARED:

That person's profile may already exist from a different retailer's incident — with a different legal basis, possibly outdated, and not your enrolment.

INDEPENDENT:

You manage your own enrolments based on your own banning orders and civil recovery cases. Your legal basis is documented and yours alone.

STAFF MISCONDUCT CASES

THE MOST SENSITIVE DATA OF ALL.

When facial recognition is used in cases of staff theft, misconduct, or abuse, the individuals involved have specific legal protections under employment law. This data must be contained within your dedicated environment.

EMPLOYMENT LAW SENSITIVITY

Staff cases often run alongside disciplinary or legal proceedings. Biometric data relating to these cases must not be accessible to any other organisation.

DATA MINIMISATION

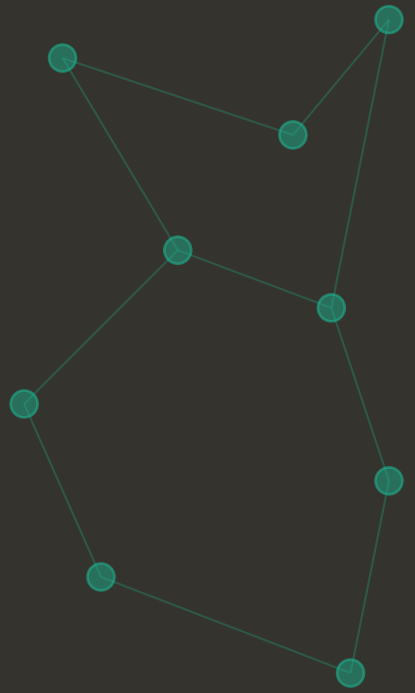
Under UK GDPR Article 5(1)(c), you must only process what is necessary. Staff biometric data should never leave your dedicated database environment.

SHARED DATABASES CREATE LEAKAGE

If a current or former employee's profile enters a shared database, they may be flagged at other retailers without your knowledge, consent, or legal basis.

SECTION FOUR

DUE DILIGENCE.



Questions to ask. What to demand in writing.

DUE DILIGENCE

5 QUESTIONS TO ASK YOUR PROVIDER.

1	IS OUR DATA IN A DEDICATED OR SHARED DATABASE?	The answer should be 'dedicated'. If they hesitate or qualify the answer, probe further.
2	WHO ELSE'S DATA SHARES OUR DATABASE?	A shared-model provider should clearly name the boundaries — or confirm there are none.
3	IF ANOTHER OF YOUR CLIENTS IS BREACHED, DOES IT AFFECT US?	Understand your blast radius. In a shared model, someone else's breach can become your incident.
4	CAN WE SEE A FULL AUDIT TRAIL OF OUR ENROLLED DATA?	You should be able to see every record — when it was created, by whom, and when it was accessed.
5	DO YOU USE OUR DATA TO TRAIN OR IMPROVE YOUR MODELS?	If your enrolled biometrics feed a training pipeline, your data is being used beyond its original lawful purpose.

THE BOTTOM LINE.

1. Shared databases pool your biometric data with other organisations. You have no visibility or control over what sits alongside yours.
2. Every retailer sets their own enrolment threshold. A shared database ignores those thresholds — a record created by a corner shop using any-theft criteria sits live in a national retailer's system.
3. Enrolling a vulnerable individual — a minor, someone with a low-value theft — that you would never have added yourself is a safeguarding and GDPR proportionality failure. Even if someone else made the call.
4. Data contamination creates false alerts and wrongful exposure. Another retailer's bad enrolment becomes your legal problem the moment your system acts on it.
5. Under UK GDPR, you must demonstrate compliance. That is near-impossible when you don't fully control the database your data lives in.
6. Your watchlist is commercially sensitive intelligence. Sharing it — even indirectly — benefits competitors and undermines your operation.
7. An independent, dedicated database — hosted by your provider but exclusive to you — is the only model that gives you full accountability.
8. Always ask your provider in writing: is our data dedicated or shared? Then check your contract says the same thing.

NEXT STEPS.

FAICE TECH
THE ETHICAL AI COMPANY

Two things to do after this conversation.

01 REVIEW YOUR AGREEMENTS

Pull your current FR provider contract and check:

- Does it explicitly state your data is in a dedicated database?
- Are you named as Data Controller?
- Do you have audit rights over your enrolled data?
- Is there a clear deletion and retrieval process?

If any of these are missing or vague — that is a problem worth solving now.

02 SPEAK WITH FAICETECH

FAICETECH operates a fully independent, dedicated database model as standard. Every client is siloed. No data sharing. No cross-contamination.

We can walk you through:

- How our database architecture compares to your current provider
- What a migration looks like and what it protects
- How our DPA framework confirms your full Data Controller status