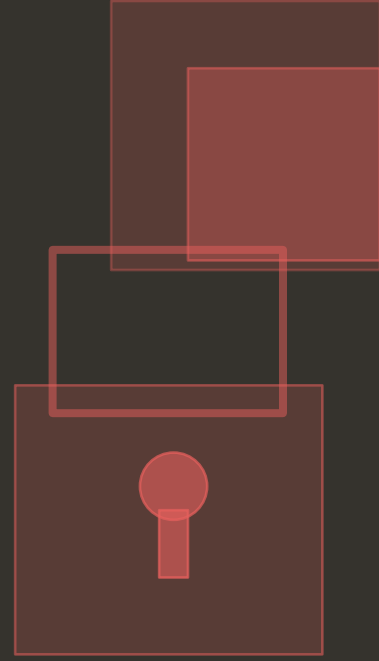
WHY YOUR DATA MUST STAY YOURS.



Data segregation in facial recognition — a guide for security professionals and data protection officers.

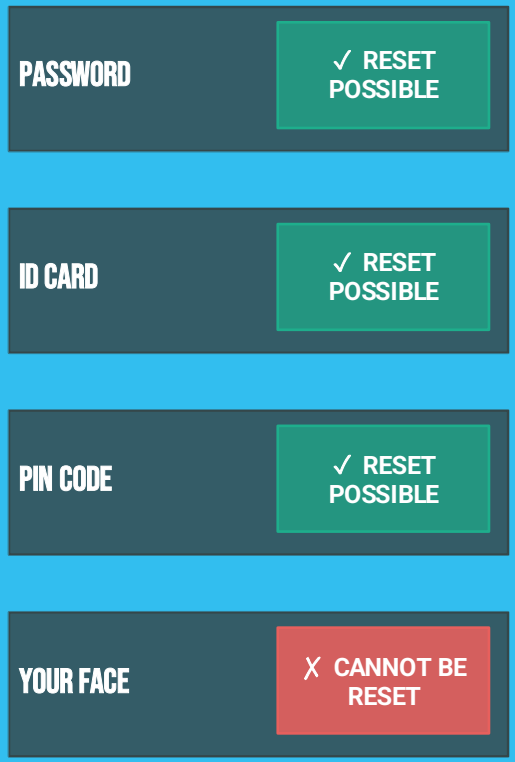
FACE TECH
THE ETHICAL AI COMPANY

THIS ISN'T JUST DATA. IT'S PERMANENT.

Biometric data is unlike any other data your organisation holds. A password can be reset. An ID card can be reissued. A PIN can be changed.

A FACE CANNOT.

If a facial recognition database is breached, every enrolled individual is permanently compromised. This is why data segregation is not a nice-to-have — it is a legal and ethical obligation.



SECTION ONE

THIRD-PARTY CONTROL.

What actually happens when you hand your most sensitive data to someone else to manage?

THIRD-PARTY CONTROL

WHAT 'HANDING OVER CONTROL' REALLY MEANS.

✗ THE ASSUMPTION

"The provider handles security — that's their job. We don't need to worry about it."

Once your biometric data leaves your premises, your visibility ends. You can no longer audit who accesses it, how it is used, or whether it has been breached.

VS

✓ THE PRINCIPLE

"Your data. Your liability. Your responsibility — regardless of who holds it."

Under UK GDPR and EU GDPR, you remain the Data Controller. The provider is a Data Processor. Legal accountability never transfers — it stays with you.

DUE DILIGENCE

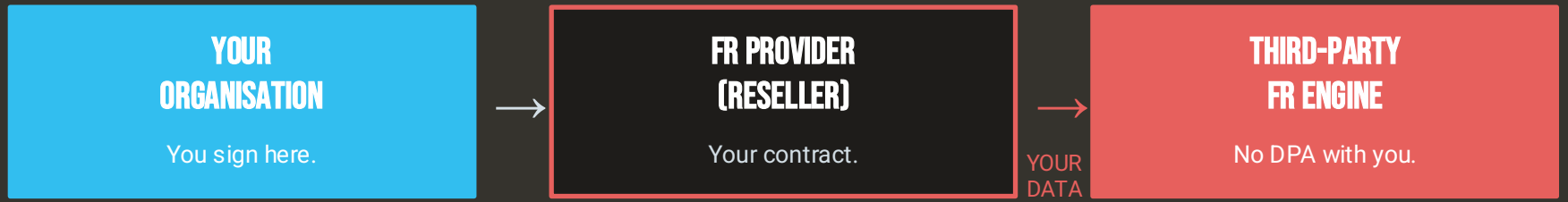
5 QUESTIONS TO ASK BEFORE HANDING OVER YOUR DATA.

1	WHO HAS ACCESS?	Which of your staff — and at what level — can access our biometric database?
2	IS OUR DATA USED TO TRAIN YOUR MODELS?	Does our enrolled data feed back into your AI training pipeline? If so, that is data sharing.
3	WHAT HAPPENS IF THEY GO UNDER OR SELL?	If this company ceases trading or sells, where does our data go? Who is legally responsible for deletion?
4	CAN WE AUDIT YOUR SECURITY?	Do you allow independent penetration testing and security audits of the infrastructure holding our data?
5	DO WE LEGALLY OWN THIS DATA?	Confirm in writing: we are the Data Controller, you are the Data Processor. We retain full ownership at all times.

THE HIDDEN SUPPLY CHAIN

DOES YOUR PROVIDER OWN THEIR TECHNOLOGY?

Many facial recognition 'providers' are system integrators. They use a third-party engine — a major cloud platform or another vendor's SDK — to actually perform the matching. Your biometric data flows through infrastructure you have never seen, agreed to, or signed a contract with.



Your data. Their infrastructure. Your liability.

WHAT TO LOOK FOR

END-TO-END PROVIDERS. NOT RESELLERS.

An end-to-end provider owns the algorithm, the processing pipeline, and the infrastructure. When they sign a DPA with you, it covers the entire data journey — no hidden layers, no unknowns.

✕ RESELLER / INTEGRATOR

- ✕ FR algorithm owned by a third party
- ✕ Your data processed on external infrastructure
- ✕ No direct DPA with the actual processor
- ✕ Limited or no audit visibility into the engine
- ✕ Hidden subprocessors in your data chain

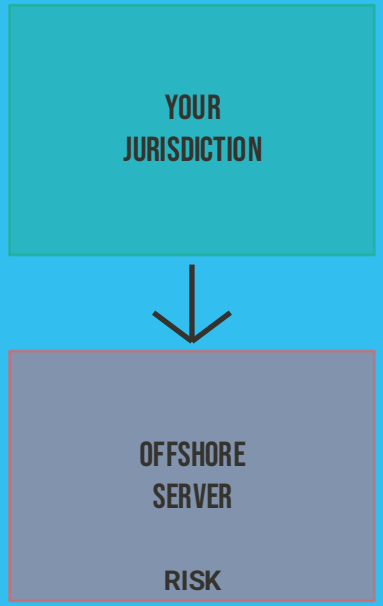
✓ END-TO-END PROVIDER

- ✓ Owns the algorithm from the ground up
- ✓ Controls the full processing pipeline
- ✓ One DPA covers the entire data journey
- ✓ Full audit trail — no black boxes
- ✓ No hidden third parties. No surprises.

SECTION TWO

DATA JURISDICTION.

Where your data is stored is as important as how it is stored.



DATA JURISDICTION

STORED ABROAD = DIFFERENT RULES.

The physical location of your data determines which laws govern it — not where your business is registered.

UK & EU GDPR

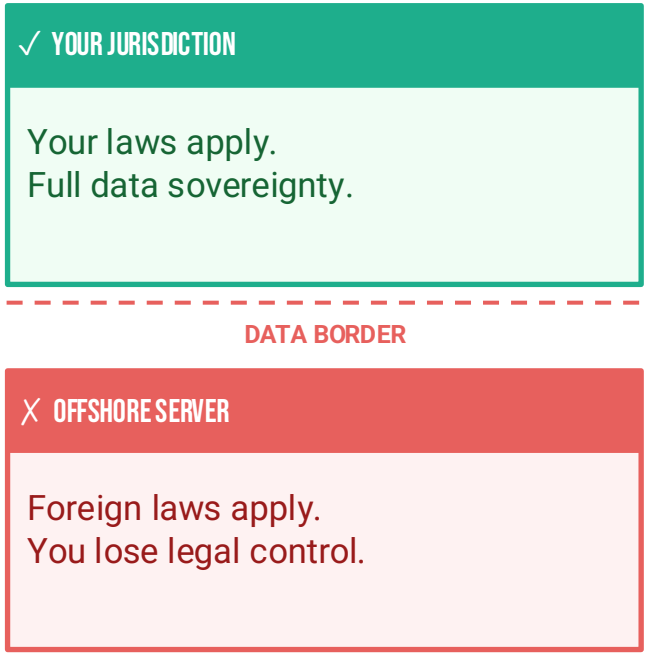
Biometrics are 'special category' data. Transferring them outside the UK/EEA requires an adequacy decision or additional safeguards — and full audit trails.

US CLOUD ACT

US law enforcement can demand data from any US-owned company, on any server, anywhere in the world — regardless of GDPR protections.

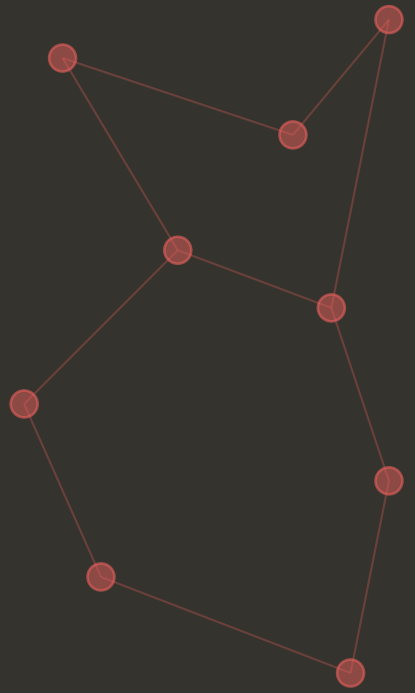
NO FRAMEWORK

Some providers store data in countries with no data protection legislation. Once there, you have zero legal recourse if it is accessed, sold, or lost.



SECTION THREE

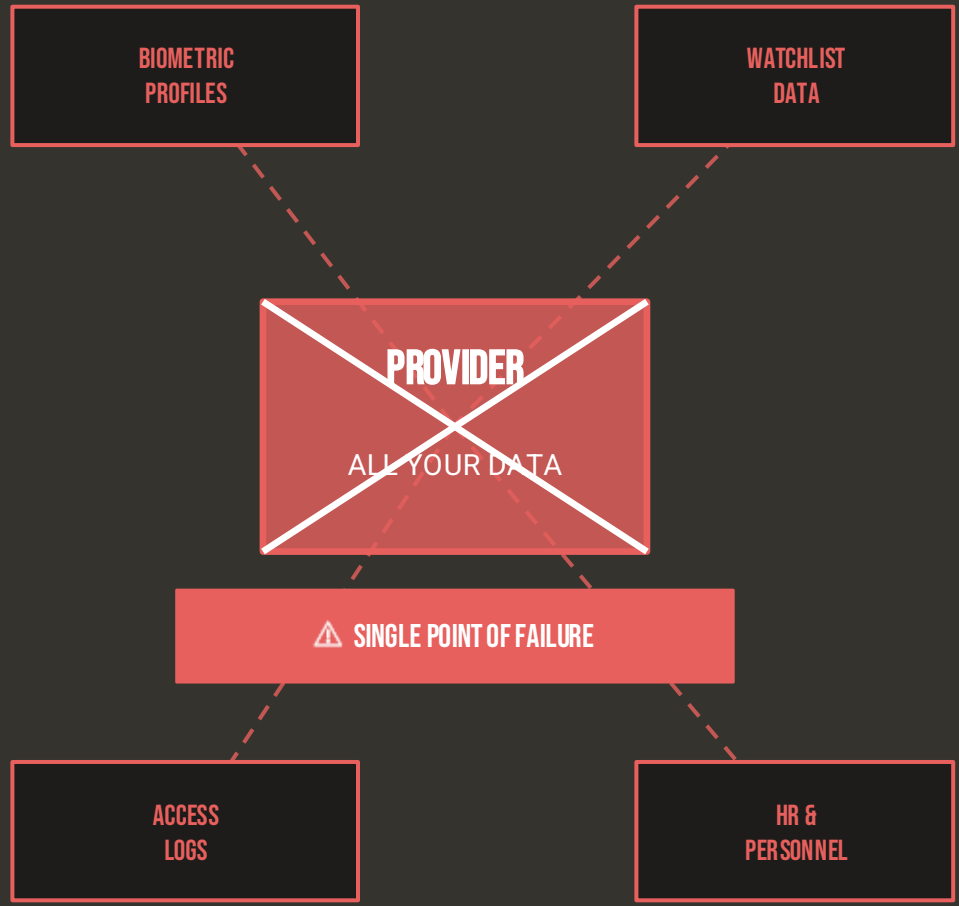
THE SINGLE-PROVIDER TRAP.



One breach. Everything exposed. All at once.

ONE PROVIDER.
ONE BREACH.
EVERYTHING GONE.

Giving all your sensitive data — face profiles, access records, watchlists, personnel files — to a single provider creates a single, catastrophic point of failure.



THE BREACH SCENARIO

WHEN IT ALL GOES WRONG.

A single provider breach doesn't just expose one system. It exposes everything — at the same time, permanently.

You can reset a password. You can cancel a card. You cannot reset someone's face.

BIOMETRIC PROFILES EXPOSED

Every enrolled individual is permanently compromised. No reissue possible.

WATCHLISTS LEAKED

Bad actors now know exactly who is flagged — and can tip them off.

INCIDENT RECORDS BREACHED

Criminal data, case notes, and event logs out in the open alongside faces.

FULL LEGAL LIABILITY

As Data Controller, every consequence of this breach lands with you.

THE INDEMNIFICATION MYTH

YOUR CONTRACT WON'T SAVE YOU.

No indemnification clause in any provider contract removes your legal responsibility for a data breach.
Under UK GDPR and EU GDPR, you are the Data Controller — or at minimum a joint Data Controller.
That cannot be contracted away.

01 YOU ARE THE DATA CONTROLLER.

The moment you collect biometric data from individuals, you become the Data Controller. A third-party processor does not change that.

02 THE REGULATOR COMES TO YOU.

If there is a breach, the ICO or your local supervisory authority will contact you — not your provider. The liability is yours to answer.

03 CONTRACTS SHIFT RISK. THEY DON'T REMOVE IT.

A contract can create obligations between you and a provider. It cannot shield you from enforcement action, fines, or civil claims from affected individuals.

THE CRITICAL SPLIT

FACES AND INCIDENT DATA MUST NEVER MIX.

When biometric profiles and criminal or incident records are stored together, a single breach doesn't just expose data — it exposes identities, investigations, and individuals at the same time.

FR DATA — KEEP SEPARATE

- Face maps & biometric profiles
- Live camera feeds & match logs
- Enrollment records

INCIDENT DATA — KEEP SEPARATE

- Criminal records & watchlist flags
- Incident reports & case notes
- CCTV event logs & officer actions

THE RIGHT APPROACH

KEEP THEM SEPARATE.

Segregate your data across separate providers, systems, and jurisdictions. If one is compromised, the others remain protected.

✓ SEPARATE

FACIAL RECOGNITION

Provider A
Your jurisdiction only
You own the data

✓ SEPARATE

ACCESS CONTROL

Provider B
Separate system
No biometric link

✓ SEPARATE

HR & PERSONNEL

Provider C
Internal or separate
Strict access control

THE BOTTOM LINE.

FACE TECH
THE ETHICAL AI COMPANY

1. Biometric data is permanent — unlike a password or ID card, a person cannot reset their face after a breach.
2. No contract removes your legal responsibility. You are the Data Controller — or joint Data Controller. That cannot be contracted away.
3. If a breach happens, the regulator comes to you — not your provider. Enforcement, fines, and civil claims all land with you.
4. Always ask: does your provider own their technology? Many are resellers — your data flows through a third-party engine you've never signed a contract with.
5. Insist on an end-to-end provider. One DPA. One data chain. No hidden subprocessors.
6. Store data only in your jurisdiction. Foreign servers are subject to foreign laws, including the US CLOUD Act.
7. A single-provider breach exposes everything at once. Segregation limits the blast radius.
8. Never mix facial recognition data with incident management or criminal records. A combined breach exposes identities and investigations simultaneously.