Shufti

GUIDE

Where Does Identity Live?

A regulated business's guide to data residency

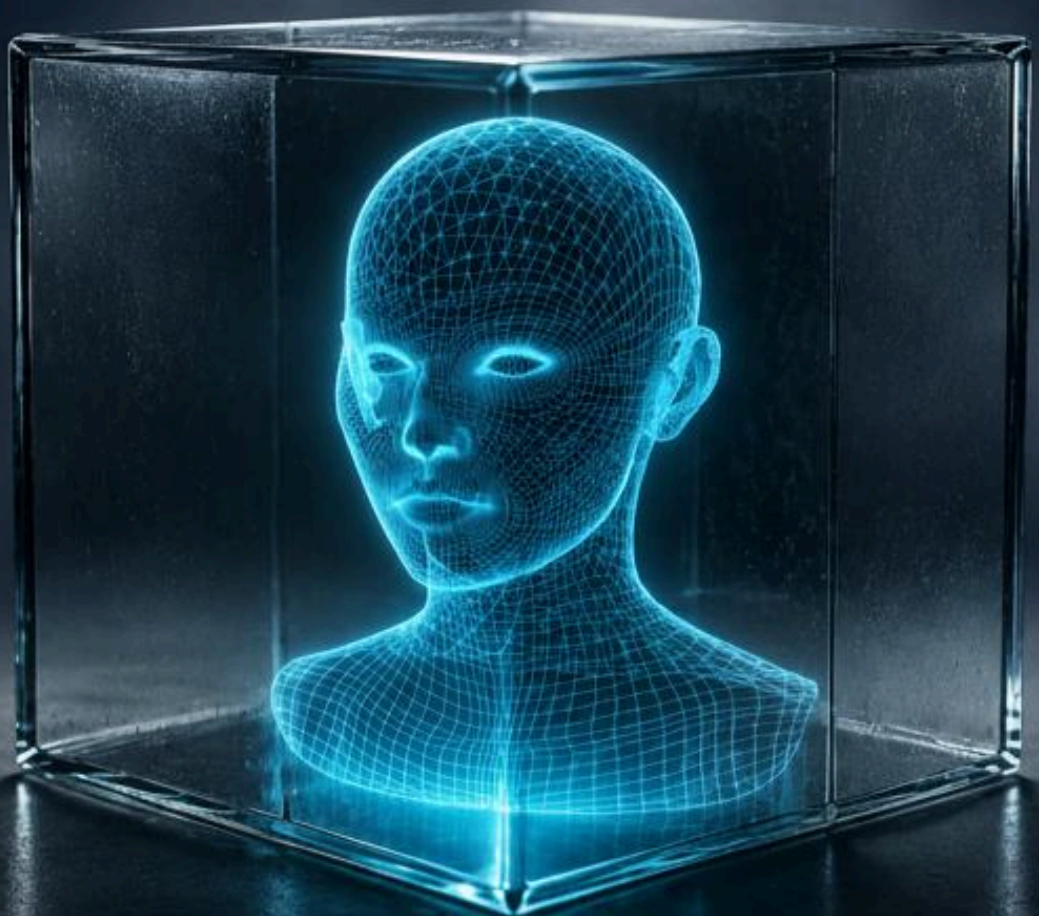

Table Of Contents

Executive Summary

Data privacy obligations are tightening worldwide, while digital services and remote onboarding are increasing the volume of sensitive identity data businesses process. To meet KYC, AML, and privacy requirements, businesses must choose an identity verification vendor whose deployment model aligns with legal and regulatory obligations.

The challenge extends beyond privacy laws. For regulated sectors such as financial services, insurance, and payments, outsourcing regulations can impose additional requirements on where data is stored, processed, and accessed. In some markets, these rules effectively create data localisation expectations even where privacy laws do not.

Businesses must therefore assess not only a vendor's compliance with privacy regulations, but also its ability to meet localisation requirements, outsourcing rules, and regulatory expectations around auditability, supervisory access, and cross-border data transfers. A vendor's use of subprocessors is equally important, as extensive subprocessor chains can increase compliance complexity and data-transfer risks.

The strongest identity verification providers combine flexible deployment options with a limited reliance on third parties, helping businesses meet privacy, outsourcing, and localisation requirements without compromising efficiency or customer experience.

This guide answers the five questions a decision-maker has to settle:

- **What are the key terms regarding data privacy?**
  Data residency is where data is stored, data localisation is whether the law requires it to remain in country, and data sovereignty is which jurisdiction's laws apply to it.

- **How does identity verification deployment differ under privacy laws and localisation requirements?**
  Privacy laws govern how data is handled, while localisation requirements govern where it must be stored and processed.

- **When is in country deployment needed over offshore cloud?**
  Offshore cloud is acceptable in most markets, but in country deployment may be required where law, regulation, or outsourcing approval requirements make offshore arrangements impractical.

- **In what circumstances must data reside within the country?**
  Where national laws or sector specific regulations require data to be stored on local infrastructure within the jurisdiction.

- **What is the right identity verification vendor to support secure data deployment?**
  One that supports local regulatory requirements, minimises subprocessor dependencies, and can deploy in country where required.

What Businesses Should Know about Capabilities of Identity Verification Vendors?

When a regulated business outsources identity verification to a third-party provider, and most do, it takes on a question its own regulator will hold it to, and one it must be able to answer in plain terms: is this provider handling our customers' identity data in line with the law of every jurisdiction we operate in? Three things sit inside that question, and a regulated organisation needs a clear answer to each one. First, is the data processed according to the law of the jurisdiction, on a lawful basis and with any cross-border movement properly authorised. Second, is it stored and located where that jurisdiction's law or financial regulator obliges it to sit, which in several markets means inside the country itself. Third, can the organisation, its auditors and its regulator actually reach and audit that data, wherever it is held. Because the answers turn on how the provider is built and where it can run, a provider's deployment model and compliance posture belong in due diligence from the first conversation, not as a detail to settle later.

Three terms:

Data residency, data localisation and data sovereignty

These three concerns map onto three terms that are often tangled together, and separating them is where a clear answer begins. Each one carries a different obligation.

Data residency

Where the data is physically stored and located. Data residency answers the question:

Where does our customers' identity data actually sit?

Although the location is often determined by a provider's deployment model, regulated businesses may be obliged to identify, disclose, assess, or obtain approval for that location under privacy, outsourcing and financial-sector regulations.

Data localisation

A legal command to keep, and sometimes process, data inside a country's borders. It answers:

Does the law oblige that data to stay in-country?

Although the location is often determined by a provider's deployment model, regulated businesses may be obliged to identify, disclose, assess, or obtain approval for that location under privacy, outsourcing and financial-sector regulations.

Data sovereignty

The principle that data is subject to the laws, and the government-access powers, of wherever it sits. It answers:

whose law governs this data, and who can lawfully demand access to it?

A provider can give in-country residency and still be reachable by a foreign government if the provider is subject to that government's law.

In short

Residency answers ***where the data sits, localisation answers whether the law forces it to stay, and sovereignty answers whose law can reach it.***

Why biometric data is treated differently

The data inside a single verification is not uniform in the eyes of the law. An identity document, a name, a date of birth or an address is personal data and protected, but a face, a fingerprint or an iris scan is biometric data, and most modern privacy laws place biometric data used to identify a person in a higher, more tightly controlled category. That higher tier brings heightened obligations, among them explicit consent, an impact assessment before processing, stricter limits on moving the data across borders, and tighter retention. So identity data is not one block to which a single standard applies, and a business should should expect a provider to handle the biometric element with the heavier care it attracts.

How jurisdictions classify biometric data

How a market treats the biometric element is where identity verification differs from ordinary software, and four patterns recur.

Special category

The strictest framing. The EU and the UK place biometric data used to identify a person in a named, heightened tier under GDPR Article 9, which needs a specific legal condition.

Sensitive

The most common framing worldwide. Saudi Arabia, the UAE, China, Vietnam, Indonesia, Nigeria, South Korea, Canada and Quebec, Australia and Brazil oblige explicit consent and extra safeguards.

Not a separate class

India, Hong Kong and Singapore have no statutory sensitive tier, so biometric data is treated as ordinary personal data, though Hong Kong and Singapore expect stronger handling through guidance.

State biometric laws

The United States has no federal biometric category. State statutes such as Illinois BIPA, Texas, Washington and Colorado, and the sensitive-data rules inside state privacy laws, govern it, which is a patchwork rather than one rule.

The data journey of a single verification

A single identity check passes through six stages, and a different rule can attach at each one. Seeing the journey turns the law from a wall of acronyms into a map of decision points.

01
Capture

Consent and notice, explicit for biometrics.

02
Transmit

Leaving the country triggers transfer rules.

03
Process

Localisation can force this in-country.

04
Decide

Pass, fail or refer, decision rules attach.

05
Store

Residency and localisation bite hardest here.

06
Retain & delete

Retention minimums versus erasure rights.

Compliance teams tend to own the consent, transfer and retention points, while engineering owns where processing and storage physically happen. The two meet at the processing stage.

The real data privacy compliance challenge an identity verification solution must overcome

The sub-processor problem

The duty to protect identity data does not stop at the provider's front door. A regulated organisation has to show how every party in the chain handles the data, including any third party the provider relies on. Many verification vendors are stitched together rather than built end to end, taking liveness from one supplier and document checks from another, so a single verification can pass through several companies. Each added party is another place the data can be exposed, another jurisdiction it can move into, and another set of processing to document and prove, often with little visibility into a sub-processor the organisation never chose. A provider built on a long chain is harder to keep compliant and more exposed, while one that owns its core verification stack keeps the chain short and accountability in one place. Some regimes now make this explicit. The EU's Digital Operational Resilience Act (DORA), in force since January 2025, obliges financial entities to manage ICT third-party risk directly, keep a register that maps the whole chain, and write specific oversight and audit terms into their contracts, with the most critical providers under an EU oversight framework. A vendor that hands data to several sub-processors makes each of those obligations harder to satisfy.

Two layers of legal obligation

The duty arrives as two distinct layers in every market, and the two do not always point the same way.

The privacy layer:

lawful basis, governance and audit Before any question of where data sits, privacy laws such as the GDPR across European Union require organisations to demonstrate that customer identity data is stored, processed and accessed lawfully, with a valid legal basis and any cross border transfers properly authorised. They must also maintain the governance and control needed for themselves, their auditors and regulators to audit data handling across the provider and its subprocessor chain.

The localisation layer:

when data must stay in country on top of the privacy layer, a sector regulator may require data localisation, meaning data must be stored, and sometimes processed, within the country's borders. This is common in financial services, where banking and payment regulators often require customer or payment data to remain in country, with any transfer abroad subject to approval. Unlike privacy obligations, which are largely satisfied through governance and documentation, localisation is an architectural requirement. Where it applies, data must be deployed on in country cloud infrastructure or other local infrastructure, making compliance dependent on the provider's deployment model rather than its paperwork.

How Data Sovereignty Concerns Are Shaping Identity Verification Procurement in Europe

The US CLOUD Act (Clarifying Lawful Overseas Use of Data Act, 2018) allows US authorities, subject to applicable legal process, to require certain providers under US jurisdiction to disclose data within their possession, custody or control, regardless of whether that data is stored inside or outside the United States. As a result, data hosted in European data centres may still be subject to US disclosure orders where the provider remains subject to US jurisdiction and controls the data. This has created ongoing concerns in Europe around data sovereignty and regulatory control, particularly for organisations handling sensitive or regulated information, and has contributed to growing interest in sovereign cloud models, EU controlled providers and other arrangements designed to reduce exposure to non EU governmental access requests.

As a result, many European organisations now scrutinise an identity verification provider's corporate structure, cloud architecture, subprocessor chain and deployment model as part of their due diligence process. Providers that can offer EU based or in country deployments, minimise reliance on third party subprocessors, provide greater control over data access and encryption, and reduce exposure to non EU legal claims are often viewed as the lower risk option for handling sensitive identity data.

Identity Verification Data Residency Laws in Different Countries

Each country below is read through the two layers that bind a vendor's data handling: the general data- protection law and the financial-sector regulator. For each, the guide sets out what each one obliges and what it means for where a vendor must store identity data, with a link to the primary source. Positions are dated, and clause and paragraph numbers can change between rulebook versions, so the linked source is the authority.

Interestingly, the privacy layer is more uniform than it first looks. In most of these jurisdictions the general data-protection laws land on a similar set of obligations, much of it echoing the GDPR. What genuinely varies is localisation, whether identity data must stay inside the border and on what terms it may leave. That difference comes from one of two places: data sovereignty, the position that data generated in a country should remain under its own control and jurisdiction, or sector-specific mandates, usually from financial regulators governing how a regulated firm may outsource material functions or place identity data with a third party offshore.

Saudi Arabia

Regulators

SAMA (prudential), SDAIA (privacy, under the PDPL).

Data-protection law

The PDPL classes biometric data as sensitive. Cross-border transfer is permitted to an adequate country, or under SDAIA standard clauses or binding common rules after a risk assessment, with no adequacy list published yet.

Sector regulator

The SAMA (Saudi Central Bank) Cloud Computing Regulatory Framework applies to SAMA-supervised financial institutions and classifies data by sensitivity, placing customer data in the highest tier. That data is expected to remain in-Kingdom, whether on a private data centre or on certified local cloud regions hosted under SAMA-inspectable agreements. Cross-border arrangements are permitted only in narrow, documented circumstances and need SAMA approval with strict security and compliance safeguards

Vendor local-storage requirement

Store and process customer identity data in-Kingdom, offshore cloud needs explicit SAMA approval.[1,2,3]

United Arab Emirates

Regulators

CBUAE (prudential), UAE Data Office under Federal Decree-Law 45/2021 (federal privacy). DIFC and ADGM operate separate regimes and regulators.

Data-protection law

Biometric data is sensitive. Transfer is permitted to an adequate country, under appropriate safeguards, or by a derogation such as explicit consent. No general federal localisation.

Sector regulator

CBUAE Outsourcing Regulation for Banks, Article 6: the Master System of Record, including all confidential data, must be continuously maintained and stored within the UAE. Customer confidential data must not be shared outside the UAE without Central Bank approval and the customer's prior written consent. The Central Bank can access the bank's data on request, and a notice of no-objection is needed before outsourcing any activity.

Vendor local-storage requirement

Hold the record of customer data in the UAE, no offshore store without CBUAE approval.[4,5]

Singapore

Regulators

MAS (prudential and central bank), PDPC (privacy).

Data-protection law

The PDPA imposes no localisation, its Transfer Limitation Obligation expects comparable protection abroad, typically by contract. Biometric data is governed by the same PDPA obligations as other personal data.

Sector regulator

The MAS Guidelines on Outsourcing treat cloud services as a form of outsourcing and oblige confidentiality and security, audit and inspection rights for the institution and MAS over the provider and its sub-contractors, control of sub-outsourcing, notification of data-location changes, and assurance that offshoring does not impede MAS supervision. A material-outsourcing register is expected.

Vendor local-storage requirement

No in-country storage mandate, the vendor must guarantee MAS and auditor access and a transparent sub-processor chain.[6,7]

Malaysia

Regulators

Bank Negara Malaysia Privacy Law (Personal Data Protection Act 2010)

Data-protection law

The PDPA imposes no hard localisation. From 1 April 2025, amended Section 129 replaced the unused whitelist with prescribed transfer bases, mainly substantially similar law or adequate protection in the destination (usually with a transfer impact assessment) or data subject consent. The 2024 Amendment also treats biometric data as sensitive personal data and adds breach-notification and data-protection-officer duties.

Sector regulator

BNM's Outsourcing Policy requires prior approval for material outsourcing, controls offshore arrangements, and requires a board approved outsourcing plan, including the cloud roadmap. RMiT requires cloud risk assessment and BNM access, with first time consultation and later notification for critical public cloud use, while non critical cloud no longer requires prior notification under the risk based approach.

Vendor local-storage requirement

No absolute mandate, but critical systems face consultation gates on first-time public-cloud adoption and scrutiny on offshore arrangements. Expect in-region or in-country hosting with BNM access preserved.[8,9,10]

Thailand

Regulators

PDPC (privacy, under the PDPA) and the Bank of Thailand (BOT) for banks and payment service providers.

Data-protection law

The Personal Data Protection Act (PDPA), in force since June 2022, classes biometric data as sensitive personal data. Cross-border transfer is permitted to a destination with adequate protection, under appropriate safeguards, or with the data subject's consent. The PDPA imposes no general data-localisation mandate.

Sector regulator

The Bank of Thailand's technology and outsourcing expectations call for a documented risk assessment before cloud adoption and preserved BOT and auditor access to outsourced systems and data, without a blanket in-country storage mandate.

Vendor local-storage requirement

No general mandate. A vendor must guarantee BOT and auditor access and maintain a clear, transparent sub-processor chain.[11]

India

Regulators

RBI (payments and prudential), Data Protection Board of India (under the DPDP Act 2023).

Data-protection law

The DPDP Act 2023 is permissive on cross-border transfer, allowing transfer except to a government-restricted set of destinations not yet issued. Biometric data is not given a separate sensitive tier.

Sector regulator

The RBI "Storage of Payment System Data" directive (6 April 2018) obliges all payment-system data to be stored only in India. The 2019 FAQ defines that data to include customer data such as name, mobile number, email, Aadhaar number and PAN, payment-sensitive data, payment credentials and transaction data. Processing abroad is allowed only if the data is deleted overseas and brought back to India within one business day.

Vendor local-storage requirement

Hold the payment-system data store of record, including the identity PII within it, only in India.[12,13]

European Union / EEA

Regulators

National data protection authorities and the EDPB (privacy), national competent authorities under the EBA, and the European Supervisory Authorities under DORA (prudential).

Data-protection law

The GDPR imposes no localisation. Personal data may leave the EEA only under a transfer mechanism, an adequacy decision, standard contractual clauses or binding corporate rules, with a transfer impact assessment where clauses apply. Biometric data used to identify a person is special-category, needing an Article 9 condition.

Sector regulator

The EBA outsourcing guidelines require a register of all outsourcing, access, information and audit rights for the institution and its regulator over the provider and its sub-contractors, extra safeguards for third-country providers, and location specified and controlled in critical-or-important contracts. DORA (in force January 2025) adds ICT third-party-risk obligations.

Vendor local-storage requirement

No in-EEA mandate, but the vendor must let the institution and its regulator reach and audit the data wherever it sits, sit on the register, and meet third-country conditions if outside the EEA, which in practice favours transparent sub-processor chain.[14,15,16]

United Kingdom

Regulators

PRA and FCA (prudential and conduct), ICO (privacy).

Data-protection law

UK GDPR and the Data Protection Act 2018. No localisation, transfer via UK adequacy regulations, the International Data Transfer Agreement, or the UK Addendum to the EU clauses. Biometric data used for unique identification is special-category.

Sector regulator

PRA Supervisory Statement SS2/21 takes a risk-based approach to data location and imposes no localisation mandate. It obliges full access and unrestricted audit and information rights for the firm, its auditors, the PRA and the Bank, plus sub-outsourcing governance and exit planning.

Vendor local-storage requirement

No mandate, document a data-location risk assessment and guarantee regulator and auditor access over a clear sub-processor chain.[17,18]

Indonesia

Regulators

OJK (financial services), the Ministry of Communication and Digital (general electronic systems), and the personal-data authority under the PDP Law.

Data-protection law

The PDP Law (Law 27 of 2022) classes biometric data as specific (sensitive) personal data. Transfers are tiered: a country with equal-or-higher protection, adequate binding safeguards, or, failing both, the data subject's consent. Government Regulation 71/2019 lets private electronic-system operators store data inside or outside Indonesia under supervision, requires public operators to stay onshore, and defers the financial sector to the central bank and OJK.

Sector regulator

OJK rules oblige banks to keep data centres and disaster-recovery centres inside Indonesia, with offshore processing needing OJK approval.

Vendor local-storage requirement

For OJK-regulated banks, hold an in-country data centre and disaster recovery, offshore processing only on OJK approval.[19,20]

Qatar

Regulators

QCB. The Qatar Financial Centre has its own regulator and rules.

Data-protection law

The QCB framework, under the QCB Law (Law 13 of 2012) and the Instructions to Banks, obliges prior QCB approval for material outsourcing and a board- approved outsourcing policy covering intra-group and third-party arrangements. For overseas providers, the vendor must confirm that no legal or regulatory restriction would prevent QCB, auditor or internal-audit access to records and data. The QCB E-KYC Regulation obliges prior QCB approval before running E-KYC verification for non-Qatari or non-resident customers.

Vendor local-storage requirement

No absolute storage mandate, but offshore outsourcing is QCB-consent-gated and QCB and auditor access must be guaranteed, non-resident E-KYC carries its own approval gate.[21,22]

Bahrain

Regulators

CBB (Central Bank of Bahrain) Privacy Law (Personal Data Protection Law, Law No. 30 of 2018).

Data-protection law

The CBB Rulebook's Operational Risk Management Module, Chapter OM-2, obliges prior written CBB approval to outsource functions containing customer information, expressly including payment services, card and data processing, and IT functions including cloud services, and obliges customer information to be encrypted. Outsourcing to a third party outside Bahrain needs prior CBB approval, with cloud data services handled by post-notification, on at least 30 calendar days' notice, and the service-level agreement must give the CBB, external auditors, internal audit and compliance unrestricted access to the provider's relevant records.

Vendor local-storage requirement

No absolute in-country mandate, but outsourcing customer-information functions and any offshore arrangement are approval-gated, customer data must be encrypted, and CBB access must be contractual.[23,24]

Hong Kong

Regulators

Office of the Privacy Commissioner for Personal Data (PCPD); Hong Kong Monetary Authority (HKMA) for authorised institutions.

Data-protection law

The Personal Data (Privacy) Ordinance (PDPO) contains no general data-localisation requirement. Personal data may be transferred or accessed across borders, provided organisations continue to meet their obligations under the PDPO. Biometric data is not classified as a separate sensitive category under the law, although the PCPD expects enhanced safeguards where the sensitivity of the data warrants it.

Sector regulator

The HKMA's outsourcing and technology-risk framework requires authorised institutions to maintain effective oversight of outsourced services, preserve audit and inspection rights, manage subcontracting risks, and ensure that outsourcing arrangements do not impair operational resilience or supervisory access.

Vendor local-storage requirement

No in-country storage mandate. A vendor must support regulatory access, auditability and oversight of its sub-processor chain. For material outsourcing arrangements, a local or dedicated deployment may reduce compliance friction

Canada

Regulators

Office of the Privacy Commissioner of Canada (OPC); Office of the Superintendent of Financial Institutions (OSFI) for federally regulated financial institutions..

Data-protection law

he Personal Information Protection and Electronic Documents Act (PIPEDA) permits cross-border processing and outsourcing, provided the organisation remains accountable for personal information handled by service providers. Biometric information is generally treated as sensitive personal information, and certain provincial regimes.

Sector regulator

OSFI Guideline B-10 on Third-Party Risk Management requires federally regulated financial institutions to assess and manage risks arising from outsourcing arrangements, including data location, foreign legal exposure, subcontracting, auditability, security and operational resilience.

Vendor local-storage requirement

No localisation mandate. A vendor must provide transparency regarding data location, support audit and access rights, and maintain a clear and manageable sub-processor chain. For material outsourcing arrangements, a local or dedicated deployment may simplify third-party risk assessments.

Brazil

Regulators

National Data Protection Authority (ANPD); Central Bank of Brazil (BCB) for regulated financial institutions.

Data-protection law

The Lei Geral de Proteção de Dados (LGPD) classes biometric data as sensitive personal data. Cross-border transfers are permitted through recognised transfer mechanisms, including adequacy decisions, contractual safeguards and other lawful bases approved under the LGPD. The law imposes no general data-localisation requirement.

Sector regulator

Financial institutions remain subject to outsourcing, cloud-computing and operational-resilience requirements issued by the Central Bank of Brazil. These requirements focus on governance, auditability, risk management and supervisory access rather than mandatory local hosting.

Vendor local-storage requirement

No general in-country storage mandate. A vendor must support regulatory access, audit rights and oversight of subcontractors. For regulated institutions, a local deployment may provide a lower-friction compliance model by simplifying supervisory access, auditability and outsourcing oversight.

United States

Regulators

No single federal privacy regulator. Oversight is divided among federal and state regulators, together with sector-specific supervisory authorities.

Data-protection law

The United States has no comprehensive federal privacy law and no general data-localisation requirement. Biometric data is regulated primarily through state laws, including Illinois' Biometric Information Privacy Act (BIPA), as well as state privacy statutes that classify biometric information as sensitive personal data.

Sector regulator

Financial institutions remain responsible for the oversight of third-party service providers and must ensure appropriate controls around security, auditability, subcontracting and operational resilience. Expectations are reflected in guidance issued by federal banking regulators and other supervisory authorities.

Vendor local-storage requirement

No federal localisation mandate. A vendor must support biometric privacy compliance where applicable, provide transparency regarding its sub-processor chain and enable effective oversight of outsourced services.

Compliance with Data Privacy May Not Always be Compliance with Data Localisation Requirements

It can also arise from sector specific rules governing the material outsourcing of sensitive data. Privacy compliance alone does not confirm localisation compliance; a vendor may handle data lawfully, yet still fail to meet separate in country storage, processing, or residency obligations by sector. In some markets, approval requirements for offshore cloud outsourcing can also create regulatory friction, making in country deployment a stronger option and giving vendors with established local deployment capabilities a clear advantage.

When Do Businesses Need an In-Country Deployment?

Two questions decide it

The decision rests on two questions. First, does the law oblige in-country storage? Second, the one that catches businesses out, even where it does not, how much friction does offshore create, through **no-objection processes, prior approvals, access guarantees and a heavier proof burden**? Saudi Arabia is the clearest example. Private-sector localisation is not mandatory, yet outsourcing critical systems or infrastructure outside the Kingdom **needs both an overseas no-objection and explicit SAMA approval**, which makes offshore the more burdensome option and **often favours an in-Kingdom solution** even before the cloud-framework residency rule applies.

Where in-country deployment wins

Across some Gulf countries and the residency-gated parts of Asia, in-country deployment is the only lawful or clearly lower-friction option. The UAE and Indonesia oblige it outright, India obliges it for payment data, and Saudi Arabia, Qatar and Bahrain make offshore slow and approval-heavy even where it is permitted. The data must stay in the country, delivered on a local cloud region, private cloud, on-premises or air- gapped, whichever suits the business. Malaysia sits between, with critical systems leaning in-country or regional and offshore cloud fine for non-critical functions.

Offshore cloud, a shared or foreign region, is genuinely fine in the EU, the UK and Singapore, provided the vendor can be audited by the organisation and its regulator and runs a short, transparent sub-processor chain.

Why flexibility is the lower-risk choice

The cost of getting this wrong is not symmetric. A vendor that runs only from a shared or foreign region may not suit organisations that need regulatory approval for material outsourcing or face limits on outsourcing critical systems and infrastructure offshore, while one that can deploy in-country where needed and run from a shared region elsewhere covers a wider range of requirements through a single integration. So for any organisation in more than one of these jurisdictions, the answer is a provider that can place the data in-country as an option, because the mandated and friction-heavy markets make that flexibility the lower-risk, lower-cost choice. A business confined to the EU, the UK or Singapore may not need that option today, but is better served by a vendor that could provide one if requirements change and whose service does not depend on a complex sub-processor chain, which keeps privacy, outsourcing and data-transfer compliance easier.

Choosing the Right Identity Verification Solution Based on Data Residency and Privacy-Law Requirements

A businesses privacy obligations split into two kinds, and the split is what ties them to the deployment model. Some are contractual, a data-processing agreement, breach notification, and the duty to act only on the businesses documented instructions. These travel with any deployment model because they live in the contract, and a credible vendor meets them whether it serves the businesses as SaaS or on the businesses own infrastructure. The rest are architectural, where the data sits, who holds the encryption keys, how long the sub-processor chain is, whether the data ever enters a shared environment, whether a foreign government can reach it, and whether the businesses and its regulator can audit it directly. These are decided by the deployment model, not the contract.

The single biggest variable, then, is the vendor's deployment model, because it decides which patterns are even available. A SaaS-only vendor is fine where transfer paperwork is in order, but it cannot satisfy a rule that obliges the data to stay in-country, and "EU residency via a hyperscaler" does nothing for a Gulf or South-East Asian localisation rule.

A deployment-flexible vendor, one that can run as SaaS, on local cloud, or on the customer's own infrastructure, serves the easy transfer-based markets and the hard in-country markets from the same platform, without stitching vendors together.

Within that, moving along the spectrum changes the architecture, not the contract, and turns several contractual-only assurances into structural ones. A localised or dedicated single-tenant deployment lets the businesses pin the region, narrow the chain, hold its own keys, and keep its data out of any shared pool. A private cloud, on-premises or air-gapped deployment takes that further, placing the keys, the infrastructure and the audit surface entirely with the business. One factor cuts across all of it: a vendor that builds and owns its core verification stack starts with a shorter sub-processor chain at every model, which improves the sub-processor, sovereignty and audit position even in its SaaS form. The practical test for a business is not which cloud, but how much architectural control the deployment model gives over isolation, keys, the chain and auditability, and whether the vendor can move along that spectrum to add control exactly where a requirement bites.

Conclusion

Data residency is not a single rule to clear but a set of obligations that differ by market and by sector. The practical step for a regulated business is to map each market it operates in against both layers, the privacy law and the sector regulator, and to choose a verification partner that can follow the resulting obligation into each market rather than one fixed to a single architecture.

How Shufti Helps Businesses Meet Data Sovereignty, Data Residency and Data Localisation Requirements

Across all of the above, two properties decide whether a provider can carry a regulated business across markets: a short sub-processor chain, so accountability and sovereignty sit in one place, and deployment flexibility, so the data can sit in-country where a market obliges it and offshore where it does not.

This is how Shufti is built, and it is the core of what it offers a regulated business. Shufti develops and owns its entire verification stack in-house, rather than licensing any of it from third parties. Because every step of the verification runs on technology Shufti owns, the verification data is not passed along a chain of third-party sub-processors, and that wholly owned stack removes a whole layer of vulnerability and makes the privacy obligations, the proof, the audit and the accountability, far easier to meet in one place.

On top of it sits genuine deployment flexibility. The identity verification solution can run as flexible cloud or SaaS for speed and scale, as an in-country (local) cloud where a market obliges the data to stay onshore, on-premises for organisations that need it deployed entirely within their own servers, or as a hybrid of these, so the data sits wherever each market's rules demand from a single integration.

The liveness stack is independently assessed as iBeta Level 3 conformant under ISO/IEC 30107-3, and the platform holds ISO 27001, SOC 2 and PCI DSS and is built to GDPR, which gives a business the assurance and audit position the privacy layer calls for.

The question for a business was never cloud or not cloud. It is whether a provider's ownership keeps the sub- processor chain short, and whether its deployment model can follow the obligation into each market. A provider built on both can expand across the whole map from a single integration while keeping each jurisdiction's privacy, localisation and sovereignty obligations answerable to its regulator.

The vendor assessment checklist

Take these questions to any identity verification vendor, including Shufti. The answers show whether a provider's architecture matches the markets you operate in.

Storage and processing

- [ ] In which countries or regions can you store our data, and can you pin it to one?
- [ ] Where is data processed, as distinct from where it is stored?
- [ ] Can you deploy in-country, on local cloud, or on our own infrastructure?

Transfers and sovereignty

- [ ] What transfer mechanism do you rely on for each region?
- [ ] Who are your sub-processors, where are they, and whose laws apply to them?
- [ ] Could our data be compelled by a foreign government regardless of where it is stored?

Biometric and sensitive data

- [ ] How do you handle biometric data, in terms of consent, storage location and retention?
- [ ] Can you delete biometric data immediately after a verification decision?
- [ ] How do you support the consent and retention schedules that strict biometric regimes expect, such as Illinois BIPA?

Retention and deletion

- [ ] What are your default retention periods, and are they configurable per market?
- [ ] How do deletions propagate across backups and sub-processors?
- [ ] How do you reconcile deletion rights with anti-money-laundering retention minimums?

Assurance

- [ ] Which certifications do you hold, such as ISO 27001 and SOC 2, and can we see the reports?
- [ ] Do you own your core technology, or is it assembled from third parties?

References

1. SAMA Rules on Outsourcing (PDF). https://www.sama.gov.sa/en-US/RulesInstructions/BankingRules/Rules%20on%20Outsourcing.pdf
2. SAMA Rulebook, overseas third-party outsourcing. https://rulebook.sama.gov.sa/en/v-outsourcing-third-party-service-providers-located-overseas 3. SAMA Rulebook (search the Cloud Computing Regulatory Framework here). https://rulebook.sama.gov.sa
4. CBUAE Outsourcing Regulation for Banks. https://rulebook.centralbank.ae/en/rulebook/outsourcing-regulation-banks
5. Article 6 (Outsourcing Outside the UAE). https://rulebook.centralbank.ae/en/rulebook/article-6-outsourcing-outside-uae
6. MAS Guidelines on Outsourcing. https://www.mas.gov.sg/regulation/guidelines/guidelines-on-outsourcing
7. Guidelines on Outsourcing (Banks) PDF. https://www.mas.gov.sg/-/media/mas-media-library/regulation/guidelines/bd/guidelines-on-outsourcing/ guidelines-on-outsourcing-banks.pdf
8. BNM Policy Document on Outsourcing. https://www.bnm.gov.my/index.php?ch=en_announcement&pg=en_announcement&ac=684
9. Outsourcing PD (PDF). https://www.bnm.gov.my/documents/20124/938039/PD_Outsourcing_20191023.pdf
10. RMiT (updated 1 June 2023) and the amended PDPA Section 129 (in force 1 April 2025) via the BNM website and the Personal Data Protection Commissioner.
11. Thailand PDPA via the Office of the Personal Data Protection Committee. Bank of Thailand outsourcing and IT-risk notices. https://www.bot.or.th 12. RBI notification (Storage of Payment System Data). https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11244
13. RBI FAQ. https://www.rbi.org.in/scripts/FAQView.aspx?Id=130
14. GDPR (Regulation (EU) 2016/679). https://eur-lex.europa.eu/eli/reg/2016/679/oj
15. EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02, PDF). https://www.eba.europa.eu/sites/default/files/documents/ 10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf
16. DORA (Regulation (EU) 2022/2554). https://eur-lex.europa.eu/eli/reg/2022/2554/oj
17. PRA SS2/21. https://www.bankofengland.co.uk/prudential-regulation/publication/2021/march/outsourcing-and-third-party-risk-management-ss 18. Data Protection Act 2018. https://www.legislation.gov.uk/ukpga/2018/12/contents
19. OJK portal (search the relevant outsourcing and data-centre regulations). https://www.ojk.go.id
20. Government Regulation 71/2019 and the PDP Law (Law 27 of 2022) via the official Indonesian government sources.
21. QCB Instructions to Banks. https://www.qcb.gov.qa/en/pages/instructionstobanks.aspx
22. QCB Instructions, Part VII (Supervision and Control), PDF. https://www.qcb.gov.qa/Documents/BankInstructions/EN/07-04.pdf
23. CBB Rulebook, Operational Risk Management Module (Vol 1, Conventional Banks, PDF). https://cbben.thomsonreuters.com/sites/default/files/ net_file_store/Vol_1_OM_January_2021.pdf
24. CBB outsourcing section. https://cbben.thomsonreuters.com/entiresection/115772

Shufti

Meeting Data Residency Obligations for Identity Verification

Too many businesses feel limited by their identity verification solution. It either falls short of strict data residency and sovereignty requirements, or it lacks the flexible deployment models needed to comply with them. As these obligations keep diverging across jurisdictions and sectors, that limitation quietly turns market expansion into a compliance problem.

Shufti is built to remove that constraint. It enables organisations to comply not only with each jurisdiction's privacy laws but also with sector-specific residency and localisation requirements, through flexible deployment across in-country, SaaS, air-gapped and on-premises models, reducing friction where regulators mandate in-country hosting.

REQUEST A DEMO!