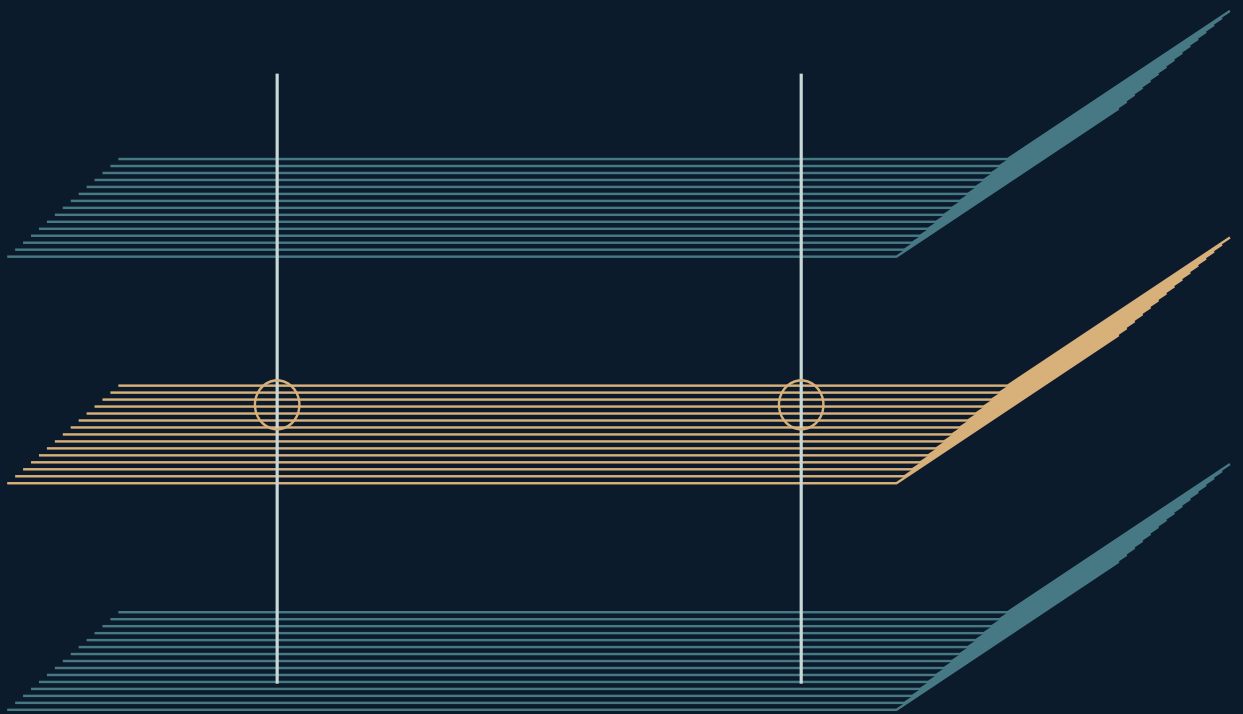


ENGINEERING / OCTOBER 2026

Data sovereignty is an architecture

A practical control map for AI systems operating across borders



THE DECISION IN BRIEF

Sovereignty is an enforceable control over the full AI data path - including support, failover and exit - not a property established by the location of the model endpoint.

- 01

Classify the information and map every processing route before selecting a deployment. Storage, inference, administration, telemetry and recovery can have different boundaries.
- 02

Compare only architectures that satisfy the applicable requirements. Local hosting, encryption and transfer safeguards answer different questions; none alone establishes compliance.
- 03

Preserve flexibility through approved routes with demonstrable controls. Test restricted-data routing, support access, deletion and exit before treating them as procurement assurances.

THE MAYDEN VIEW

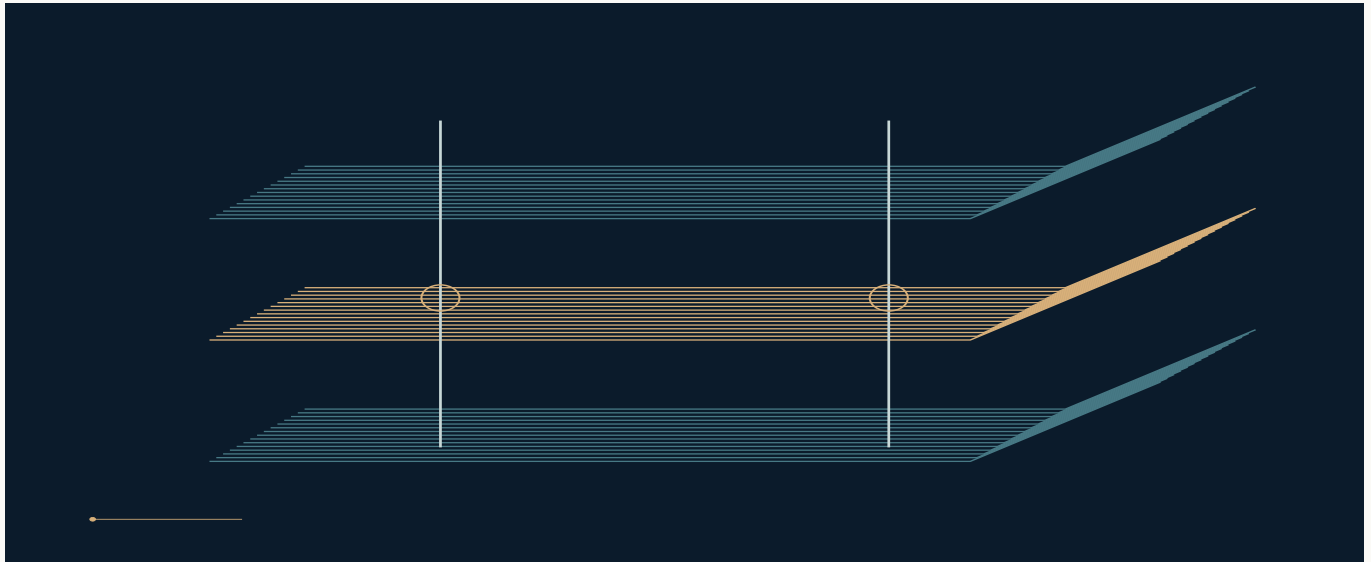
A sovereignty claim is only as complete as the data routes it can explain and control.

INSIDE THIS PERSPECTIVE

The argument at a glance	3
01 / Trace the complete data path	4
Exhibit 01 / Choose the data boundary before choosing the endpoint	5
02 / Qualify the control arrangements	6-7
Exhibit 02 / Trace one restricted customer case through the split route	8
03 / Constrain exceptions and compare costs	9
Exhibit 03 / A deployment label does not describe one universal processing boundary	10
04 / Prove the route and the exit	11
The leadership agenda	12
Method and references	13

ONE DECISION, FOUR CONNECTED QUESTIONS

Control crosses architectural layers



SOVEREIGNTY PLANES / CONCEPTUAL ARTWORK

01 Trace the complete data path

Trace the routes a hosting label leaves out

02 Qualify the control arrangements

Separate location, authority, keys, continuity and evidence

03 Constrain exceptions and compare costs

Constrain support and failover before the incident

04 Prove the route and the exit

Share public evidence without opening restricted routes

A sovereignty claim is only as complete as the data routes it can explain and control.

CHAPTER 01

01

Trace the complete data path

Trace the routes a hosting label leaves out

A database stays in-country while a support ticket copies a customer prompt elsewhere. A regional model uses a different geography during failover. These illustrative paths expose the gap in a hosting label: the service boundary extends beyond its main endpoint. Executives need an enforceable account of where information goes, who can use it and what happens when the normal route fails.

The European Commission's official overview describes mechanisms for international personal-data transfers, including adequacy and safeguards. It does not establish a universal requirement that every European workload remain inside one national boundary. ^[1] Equally, meeting an international-transfer condition does not answer every question about lawful processing, security or sector requirements. A procurement team should avoid compressing these separate issues into a single sovereign or compliant checkbox.

Start with the business information, affected people, jurisdictions and consequences of lost control. Separate mandatory conditions from commercial preferences. A public-information assistant and a confidential employee service may justify different designs. That distinction prevents investment in a restrictive deployment that still leaves the material exposure unresolved.

Map the whole service from intake to deletion

Create a flow inventory from intake through deletion. Include uploaded files, extracted text, embeddings, prompts, generated responses, cached results, evaluation examples and operational logs. Record where each item is stored, where it is processed and which actors can access it. Distinguish the intended path from emergency behavior. A failover arrangement that silently changes processing geography can invalidate the assumptions behind an otherwise carefully designed service.

Microsoft's current Foundry documentation differentiates processing locations for Standard, Global and DataZone deployment types and separately describes storage geography. Stateful features and abuse monitoring also have documented handling arrangements. These are vendor statements about specified services and configurations, not independent verification of a customer's implementation. ^[2] Their value is to show why a cloud resource's region label cannot stand in for a full processing map.

Place shared services on the map. A global observability platform may receive prompts through diagnostic logging. A development team may copy an incident into a ticket. An evaluation service may retain examples long after the production cache expires. These are illustrative pathways to investigate, not claims about every supplier. The data owner should be able to explain which pathways exist, why they are needed and how their configuration was verified. Unknown pathways should remain explicit procurement and engineering questions.

ILLUSTRATIVE DECISION TOOL

Choose the data boundary before choosing the endpoint

Fictional EU/Saudi manufacturer choice

Shared service	Separate regional services	Split by information class
Mandatory evidence before use Every included data class, processing path and support route is approved Trade-off to price Common capability; an unresolved route may exclude sensitive records	Mandatory evidence before use Each entity has approved inference, administration, logs and failover Trade-off to price Duplicated operation and evaluation; region labels alone do not settle access	Mandatory evidence before use Public manuals use a shared route; restricted records stay on approved paths Trade-off to price Routing, derived-data classification and cross-route recovery need owners

THE MANAGEMENT IMPLICATION

Reject options that fail mandatory conditions; compare capability, cost and continuity among the remainder.

No option is declared lawful. Legal and security owners must establish applicable conditions for each entity and flow. Sources: [1], [2], [5], [6], [7]

CHAPTER 02

02

Qualify the control arrangements

Separate location, authority, keys, continuity and evidence

mayden proposes a five-layer sovereignty map: location, authority, key control, continuity and evidence. Location concerns processing and retention. Authority concerns who may administer or compel access under the applicable arrangements. Key control concerns who can authorize cryptographic use. Continuity concerns the ability to operate or exit under supplier disruption. Evidence concerns the records that support these claims. The framework is original synthesis, not a legal definition or a validated scoring system.

Google Cloud's KMS documentation distinguishes key-management roles, access controls, logs and geographic handling.^[3] The management implication is to ask which operation a customer-controlled key actually governs. Control of storage encryption does not automatically mean that a service can perform useful inference without processing readable information. Evaluate the precise threat model, service design and contractual commitment. Claims about encryption become meaningful when the protected asset and access scenario are specified.

Confidential computing addresses a different exposure from encryption at rest. Google's

technical documentation describes hardware-based trusted execution environments that protect data while it is being processed.^[8]

That capability belongs in an architecture assessment, but it does not replace an assessment of who can invoke the service, what leaves the protected environment or which laws and contractual terms apply.

Ask suppliers to demonstrate the complete path with an actual workload: entry, processing, output, diagnostics and recovery. Specify which components are attested and which are outside that boundary. mayden proposes treating each unprotected path as an explicit design decision with an owner. A protected computation that sends unrestricted output into a support log has not resolved the whole confidentiality problem.

AWS's Bedrock data-protection guidance emphasizes identity permissions and secure transport, among other protections.^[4] These controls belong alongside location requirements. A locally hosted service with broad internal permissions can expose information through authorized accounts; a geographically distributed service may enforce narrower access. The architecture decision should compare the relevant risks without treating geography as a substitute for identity design. Each layer needs its own owner, evidence and exception process.

CHAPTER 02

02

Qualify the control arrangements

Attach each legal obligation to a specific flow

The EU and Saudi Arabia are separate regulatory contexts. The European Data Protection Board's adopted recommendations address supplementary measures supporting transfer tools. ^[5] SDAIA's current Knowledge Center provides the Kingdom's transfer regulation and standard contractual clauses. The transfer text sets conditions; the clauses describe one form of appropriate safeguard and obligations for the parties. ^{[6][7]} These instruments should be interpreted for the specific controller, processing purpose and transfer, with relevant sector rules considered.

Legal currency is itself an evidence problem. Review the authority's current Knowledge Center and confirm the identity of the instrument, rather than relying on a saved document or an ambiguous portal path. The

implementing regulation and the transfer regulation answer different questions. An enterprise should retain the reviewed instrument, access date, applicability analysis and legal owner. A policy copied into an architecture slide without a version can remain influential after its basis changes.

Do not assume that an arrangement approved for one entity, data class or country applies to another. A group may contain government-related operations, regulated financial services and ordinary commercial activities. Their constraints may differ even when they share a cloud account. The practical task is to record the applicable obligation beside the affected data flow and control. Where interpretation remains unresolved, restrict that flow while the owner resolves the question. This creates a concrete engineering boundary instead of a vague risk statement.

ILLUSTRATIVE ROUTE RECORD · NO IMPLEMENTATION AUDIT

Trace one restricted customer case through the split route

Fictional restricted-customer-case route; all unknowns are illustrative

Route step	Conditional split design	Unknown, owner and restriction
Input	Classify correspondence separately from public manuals	Unknown: classification. Data owner holds real records outside the shared route
Retrieval	Public manuals and restricted customer evidence use approved access paths	Unknown: derived-data access. Search owner limits testing to synthetic cases
Inference	Send restricted context only to its approved processing arrangement	Unknown: endpoint scope. Architecture owner blocks restricted-context calls
Logs	Retain necessary diagnostics under the case classification	Unknown: log payload/retention. Operations blocks launch until verified
Administration	Named support roles and approved access locations	Unknown: emergency access. Security owner withholds that access
Failover	Use an approved equivalent or stop and hand off	Unknown: fallback geography. Service owner disables automatic route expansion
Deletion and exit	Track source, derivatives, retained records and export conditions	Unknown: full deletion scope. Records owner requires an exercise before dependence

THE MANAGEMENT IMPLICATION

A split design is available only when each mandatory route condition is evidenced; an unknown carries an owner and a restriction.

Conditional design, not an approved architecture or claim about any provider. Relevant EU and Saudi obligations require entity-specific legal assessment. Unknown status describes this fictional review, not a real implementation. Sources: [1], [2], [5], [6], [7]

CHAPTER 03

03

Constrain exceptions and compare costs

Constrain support and failover before the incident

Operational exceptions deserve the same attention as the standard path. List who can obtain support access, where incident evidence may be viewed and how emergency failover works. Identify subprocessors and external dependencies that can change the effective service boundary. Define the evidence required before enabling a new feature. A supplier's product release can introduce a stateful component or a new processing route even while the organization's own application code remains unchanged.

Use policy enforcement close to the data flow. For example, a routing service can select an approved endpoint based on data class, and a deployment check can reject configurations that do not match the approved environment. These are proposed controls requiring testing. They should fail visibly, with a documented fallback, instead of silently choosing a cheaper or more available route. A commercial objective should never be allowed to obscure a mandatory architectural constraint.

Test deletion and exit with representative data before production dependence becomes large. Confirm what can be exported, what metadata accompanies it and what remains in backups or retained operational records under the contract. Deletion promises need scope and timing; an interface button alone is incomplete evidence. Exercise credential revocation and restoration as well. The business should understand both the control gained and the availability risk created when a key or account is disabled.

Compare the cost of architectures that actually qualify

Regional separation can duplicate infrastructure, reduce access to model options and make operations harder. A company that fragments every workflow by country may lose economies of scale and create inconsistent customer experiences. Local operations can also depend on a small pool of expertise, making incident recovery slower. These are real trade-offs. Sovereignty should be evaluated against a specified threat and obligation, with costs made visible. The most restrictive design is not automatically the best design for every process.

Compare complete qualifying options: a shared service with segregation, a regional service or a dedicated environment. Evaluate capability, cost, recovery and residual dependence after the mandatory requirements are met. mayden recommends keeping those dimensions visible rather than collapsing them into an unvalidated sovereignty score.

A selective architecture may therefore be appropriate. Keep sensitive evidence within a controlled environment while allowing approved public information to use broader services. Whether a transformation sufficiently reduces sensitivity requires case-specific assessment; removing names does not necessarily remove identifiability. Treat derived data, summaries and embeddings as separate objects to classify, rather than assuming they are safe because they differ from the original document. The point is to make a defensible decision about each information product.

DOCUMENTED COMPARISON

A deployment label does not describe one universal processing boundary

Vendor-documented architecture comparison

Standard	Documented processing scope Customer-specified geography; regional routing may occur	Interpretation limit Geography is not necessarily one region
Global	Documented processing scope Any geography hosting the relevant model	Interpretation limit At-rest location does not fix inference location
DataZone	Documented processing scope Within the specified zone	Interpretation limit Zone scope must match the approved requirement
THE MANAGEMENT IMPLICATION		
Verify the selected deployment and its complete data flow before making a location claim.		

Microsoft documentation updated 19 May 2026, accessed 10 October 2026. Applies to specified Models sold by Azure configurations; not an independent configuration audit. Sources: [2]

CHAPTER 04

04

Prove the route and the exit

Share public evidence without opening restricted routes

Consider a fictional manufacturer with an EU customer-support operation and a Saudi operating company. Both want an assistant that searches public product manuals and internal customer correspondence. A single regional hosting claim cannot settle the design. The public manual collection, customer records, extracted summaries and support logs need separate classification. The legal and security teams must establish the applicable conditions for each entity and flow; this example assumes no particular transfer is lawful or prohibited.

Compare a shared service for all material, separate regional services and a split design that shares public evidence while processing restricted records through approved routes. For each option, trace administration, evaluation and failover as carefully as ordinary inference. Estimate operating effort and recovery needs alongside model capability. A cheaper endpoint may create additional review or duplication costs. A more restrictive deployment may still leave an unresolved support-access pathway. The comparison should expose these differences before procurement narrows the choices.

Exhibit 02 follows one restricted customer case through the proposed split design. Its unknown labels are deliberately fictional: classification, derived-data access, inference location, logs, support access, failover and deletion have not been verified. Each has an owner and a restriction. Synthetic material can test routing while those questions remain open; real restricted records cannot enter an unapproved path merely because the public-manual route works. An outage should invoke an approved alternative or a staffed handover, not silently broaden processing geography. Technical

blocking and deletion exercises test the configuration; the legal owner must still assess the basis and conditions of actual processing.

Decide by information class. Public manuals may use the shared route after classification; customer correspondence stays restricted until its processing, support and failover conditions are satisfied. Classify summaries and embeddings separately. If routing cannot enforce these distinctions, the split design is not yet an available option. Record that restriction, its owner and the evidence needed to change it.

Approve a control map and prove the exit

Approve three records together: a control map, an exception register and an exit demonstration. The map connects each information product to its processing route and responsible actors. The register gives unresolved conditions an owner, restriction and review date. The demonstration establishes what the business can export and how access ends under the agreed terms.

Assign an executive to resolve trade-offs across legal, security, architecture and operations. Reassess material changes in supplier configuration, subprocessors and processing routes. Keep jurisdiction-specific evidence current. A static approval cannot support a service whose effective boundary has changed.

Test the proposed portfolio capability on one new route: can the organisation classify the information, establish its applicable conditions, enforce the route and operate the fallback without rebuilding the application? Measure that work and the residual dependency. The objective is flexibility within verified arrangements. Where no qualifying route exists, retain a restricted or manual service while the missing condition is resolved.

FROM INSIGHT TO ACTION

Decisions to take forward

DATA AND LEGAL OWNERS

Approve or restrict each flow; do not approve a whole service from its region label.

Evidence to require: Entity-by-entity classification and obligation map

ARCHITECTURE AND SECURITY OWNERS

Reject a configuration whose exception path crosses an unapproved boundary.

Evidence to require: Routing, logs, support and failover tests

SERVICE OWNER AND PROCUREMENT

Choose among qualifying options with operating effort and residual dependence visible.

Evidence to require: Usable export, revocation and continuity demonstration

mayden connects senior judgement, research and engineering to turn strategic choices into working capabilities.

EVIDENCE YOU CAN INSPECT

Research notes

Method and boundaries

Structured synthesis of eight official regulatory or vendor technical sources accessed 10 October 2026; architecture analysis by mayden.

EU transfer overview and EDPB guidance, Saudi current transfer instruments, and three cloud providers' technical documentation.

Scoped comparison, not a comprehensive legal opinion or compliance certification. No UAE-wide conclusions are made. Vendor documentation is not an independent configuration audit. Dynamic pages require reassessment before implementation.

Primary sources and author research

[1] International dimension of data protection

European Commission / Live guidance; accessed 2026-10-10. International transfers and adequacy. EU overview of international-transfer mechanisms; not a blanket localization requirement or a case-specific assessment of a transfer.

[Read the source](#)

[2] Data, privacy, and security for Foundry Models sold by Azure

Microsoft Learn / 2026-05-19; accessed 2026-10-10. Location of processing; storage; abuse monitoring. Vendor documentation for specified deployment types, accessed on the stated date; customer configuration, contracts and access paths require separate verification.

[Read the source](#)

[3] Cloud KMS encryption and key management deep dive

Google Cloud / September 2026; accessed 2026-10-10. Key control; access; logging; data residency. Vendor key-management architecture; customer control of keys does not by itself prove that plaintext is never processed or establish legal sovereignty.

[Read the source](#)

[4] Data protection: Amazon Bedrock

AWS / Living documentation; accessed 2026-10-10. Data protection recommendations. Vendor guidance for Amazon Bedrock; not independent verification of a particular service configuration or all connected tools.

[Read the source](#)

[5] Recommendations 01/2020 on measures that supplement transfer tools

European Data Protection Board / 2021-06-18 final; accessed 2026-10-10. Final adopted recommendations. EU transfer guidance adopted in 2021; applicability and supplementary measures depend on the actual transfer and legal context.

[Read the source](#)

[6] Regulation on Personal Data Transfer outside the Kingdom

SDAIA Knowledge Center / Current portal text accessed 2026-10-10. Articles2 and subsequent transfer/safeguard provisions. Current official Arabic portal text as retrieved. Transfer purposes, safeguards and conditions must be read together with the PDPL and any sector rules; not a complete legal assessment or blanket prohibition on export.

[Read the source](#)

[7] Standard Contractual Clauses For Personal Data Transfer

SDAIA Knowledge Center / Current portal text accessed 2026-10-10. Introduction; purpose; scope. Official Saudi contractual-safeguard instrument; clauses are one part of the transfer framework and do not by themselves establish every transfer as lawful.

[Read the source](#)

[8] Confidential Computing overview

Google Cloud / Updated 2026-10-07. Overview; End-to-end encryption. Capability description; not independent assurance or legal determination. Availability and configuration require workload-specific checks.

[Read the source](#)