



WHITE PAPER · DATA GOVERNANCE

Data Sovereignty and Cross-Border Compliance in Multi-Cloud

Transfer law in the EU, UAE, Saudi Arabia and Egypt, and the technical controls that support it

White Paper 4 · Data Governance series · Version 1.0 · October 2026

Bassirah Technology — Innovation & R&D

Data Sovereignty and Cross-Border Compliance in Multi-Cloud

White Paper 4 · Data Governance series · Bassirah Technology — Innovation & R&D · 28 October 2026

Document control

Field	Value
Series	Data Governance, paper 4 of 6
Author	Bassirah Technology — Innovation & R&D
Version	1.0 · 28 October 2026
Scope	A technology and regulatory survey. It describes official legal texts, regulatory guidance, published research and publicly documented systems; it does not report Bassirah benchmarks or customer results, and it is not legal advice.

Contents

1. Abstract	4
2. Introduction	4
2.1 Why sovereignty is a governance question	4
2.2 About the Data Governance series	4
2.3 Scope	5
2.4 Terms used in this paper	5
3. Three layers of sovereignty	5
4. EU transfer law	5
4.1 GDPR Chapter V	5
4.2 Schrems II and transfer impact assessments	6
4.3 What counts as a transfer	6
4.4 The EU-US Data Privacy Framework	6
4.5 Proposed changes	7
5. EU data and cloud rules beyond personal data	7
5.1 The Data Act	7
5.2 Cloud sovereignty certification and the proposed Cloud and AI Development Act	7
5.3 Financial services	8
6. The UAE, Saudi Arabia and Egypt	8
6.1 United Arab Emirates	8
6.2 Saudi Arabia	9
6.3 Egypt	9
6.4 What the regimes share	9
7. Technical controls	9
7.1 Location guardrails	9
7.2 Sovereign cloud offerings	10
7.3 Customer-held keys	10

7.4 What encryption achieves legally	10
7.5 Confidential computing	11
7.6 Compute to data.....	11
7.7 Copies and evidence.....	11
8. The cost of localization.....	12
9. The operating model.....	12
10. Comparative analysis.....	12
11. Open challenges and future opportunities.....	13
11.1 Processing in the clear.....	13
11.2 Legal stability	13
11.3 Defining sovereignty levels.....	13
11.4 Guardrail coverage	13
11.5 Policy-aware federation.....	14
11.6 Jurisdiction-aware lineage.....	14
11.7 Gulf and Egyptian implementation	14
11.8 Key custody at scale	14
12. What this means for platform decisions	14
References	15

1. Abstract

Organizations that run data across several clouds, regions and countries must answer three questions for every data set: where it is stored and processed, whose law can reach it, and who can operate the systems that hold it. These questions are usually grouped under data sovereignty, a term that covers residency, jurisdiction and operational control. This paper sets out the legal position as of October 2026 for organizations operating in the European Union, the United Arab Emirates, Saudi Arabia and Egypt. It covers GDPR Chapter V and the Schrems II judgment, transfer impact assessments, the EU-US Data Privacy Framework and the pending appeal against it, the EU Data Act's cloud switching rules and its safeguard against foreign government access, the proposed Cloud and AI Development Act, and the transfer regimes of the UAE, its financial free zones, Saudi Arabia and Egypt. It then describes the technical controls available: location guardrails, sovereign cloud offerings, customer-held keys, confidential computing, compute-to-data query patterns and evidence of where data and copies live. It is explicit about what each control can and cannot achieve, compares them, sets out open challenges and closes with notes for platform decisions.

2. Introduction

2.1 Why sovereignty is a governance question

Multi-cloud architectures spread data by design. A single analytics workload may read from object storage in one region, run in a managed service in another, write backups to a third and be supported by engineers in a fourth country. Each of these is a decision about location, about which laws apply and about who can access the data. Many of them are made by default settings rather than by anyone responsible for governance.

The term sovereignty does not settle these questions; it names them. A review of the literature finds that data sovereignty, digital sovereignty and cyber sovereignty are used in substantially different and sometimes unclear ways, and proposes that sovereignty claims concern control and ownership, asserted by actors ranging from individuals to companies to states [1]. A foundational account distinguishes three strands: state autonomy and security, economic autonomy from foreign technology firms, and user autonomy through encryption and data protection [2]. An analysis of EU policy finds that data governance is the most developed part of European digital sovereignty, while control over infrastructure and platforms is weaker and the terminology inconsistent [3]. In 2026 the European Commission proposed legislation that treats dependence on a few third-country cloud providers, subject to extraterritorial laws on data access, as a sovereignty and continuity risk [4].

2.2 About the Data Governance series

This is the fourth of six papers. Paper 1 covered the data that AI systems use. Paper 2 covered continuous, risk-adaptive governance and policy as code, which this paper uses to enforce location rules. Paper 3 covered data products and contracts, whose descriptors can carry location and jurisdiction. Paper 5 covers privacy-enhancing computation, which offers further ways to use data without moving it in the clear, and Paper 6 covers data sharing ecosystems.

2.3 Scope

This paper covers cross-border transfer law and sovereignty policy in the EU, the UAE (including the Dubai International Financial Centre and Abu Dhabi Global Market), Saudi Arabia and Egypt, and the technical controls that support compliance in multi-cloud architectures. Statements about laws, regulations and guidance are general information as of October 2026. They are not legal advice: obligations depend on the facts of each case, the data and sector involved, and guidance and litigation that continue to change, and organizations should take qualified legal advice in each jurisdiction. Where an official text could not be opened for this paper, the statement relies on reputable secondary sources and the text says so; this applies in particular to parts of the UAE, Saudi and Egyptian material. Statements about products reflect documentation accessed in October 2026. The paper quotes no figures from its sources.

2.4 Terms used in this paper

Data residency is the location where data is stored and processed. **Data localization** is a legal or contractual requirement that data stay in a given country. A **transfer** is the movement of personal data, or remote access to it, from one jurisdiction to another in the sense defined by the applicable law. **Jurisdiction exposure** is the possibility that a foreign authority can compel access to data, for example through the provider's corporate group. **Operational control** is the ability to run, support and change the systems that hold the data. **Sovereignty**, in this paper, refers to all three layers together.

3. Three layers of sovereignty

Residency, jurisdiction and operational control are different problems with different controls. Table 1 separates them. Most failures in practice come from treating one as if it solved another, for example assuming that data stored in an EU region is beyond the reach of a provider's home-country law, or that a contract about jurisdiction ensures that backups stay in the region.

Layer	Question	Typical legal hooks	Typical controls
Residency	Where is the data stored and processed, including copies, logs and support access?	Localization rules; transfer rules that treat remote access as a transfer	Region selection, location policies, replica and backup inventory
Jurisdiction	Whose authorities can compel access, directly or through the provider's group?	GDPR Art. 48; Data Act Art. 32; transfer impact assessments	Provider and contract choice, key custody, encryption before upload
Operational control	Who operates, supports and can change the systems?	Sector rules such as DORA; proposed EU cloud sovereignty levels	Sovereign or partner-operated offerings, access approval, operator access logs

4. EU transfer law

4.1 GDPR Chapter V

GDPR Chapter V, Articles 44 to 50, governs transfers of personal data outside the European Economic Area [5]. Every transfer, including onward transfers, must rely on one of three routes:

an adequacy decision by the Commission (Article 45); appropriate safeguards such as standard contractual clauses or binding corporate rules (Articles 46 and 47); or, in specific situations, a derogation such as explicit consent or the establishment of legal claims (Article 49) [5]. Article 48 provides that a judgment or decision of a third-country court or authority requiring disclosure of personal data can be recognized or enforced only on the basis of an international agreement, such as a mutual legal assistance treaty [5]. The EDPB's guidelines on Article 48 confirm that such requests cannot automatically be honored, and address requests received by processors and requests from a third-country parent company to its EU subsidiary [6].

4.2 Schrems II and transfer impact assessments

In Schrems II, the Court of Justice invalidated the EU–US Privacy Shield, upheld the standard contractual clauses as a tool, and held that data transferred under them must receive protection essentially equivalent to that in the EU; exporters and importers must verify, before transferring, whether the destination's law and practice on public-authority access allow that, and must suspend transfers where it does not [7]. The EDPB's recommendations on supplementary measures turned this into a six-step method: know your transfers, identify the transfer tool, assess whether it is effective in light of the destination's law and practice, adopt supplementary measures, take procedural steps and re-evaluate at intervals [8]. The 2021 standard contractual clauses require the parties to warrant, after a documented assessment of the specific transfer, that the destination's laws do not prevent compliance, and to notify each other of changes and of access requests [9].

Two points from the EDPB's recommendations matter most for cloud architecture. Remote access from a third country, for example by support staff, and storage in a cloud outside the EEA are transfers [8]. And while encryption applied before transfer, with keys held only by the exporter or a trusted party in the EEA, can be an effective supplementary measure for storage and backup, the EDPB could not envisage an effective technical measure where a provider or group entity in a third country needs access to the data in the clear and that country's access powers go beyond what is necessary and proportionate [8].

4.3 What counts as a transfer

Not every arrangement with a non-EU provider is a transfer. The EDPB's guidelines on the interplay between Article 3 and Chapter V set three cumulative criteria for a transfer and give the example of an EU processor that is a subsidiary of a third-country parent and processes data only in the EU: this is not a transfer, but the controller must still assess the risk that the processor receives a third-country access request, since complying with it would be a transfer [10]. The controller remains accountable for that risk under the GDPR's security and processor obligations even where Chapter V does not apply [10]. This is the situation of many EU regions of global cloud providers.

4.4 The EU–US Data Privacy Framework

The Commission's adequacy decision on the EU–US Data Privacy Framework, adopted on 10 July 2023, allows transfers to US organizations certified under the framework without further authorization; transfers to non-certified US recipients still need standard contractual clauses or another tool, with an assessment [11]. The General Court dismissed an action for annulment on 3 September 2025, finding that the US ensured an adequate level of protection at the date of adoption and that the Commission must continue to monitor US law [12]. An appeal to the

Court of Justice was lodged on 31 October 2025 and, on the sources found for this paper, was still pending in October 2026; the case number is reported by secondary sources [12]. The Commission's first periodic review, in October 2024, concluded that the necessary structures were in place, with the next review planned about three years later [13]. The framework is therefore valid but contested, and depends on US executive measures that could change.

4.5 Proposed changes

A Commission proposal of November 2025 to simplify the EU digital framework, the Digital Omnibus, would amend the GDPR, the Data Act and other acts. According to the Council's negotiating mandate, Chapter V of the GDPR was not amended by the Commission proposal, the Council added only a limited clarification to Article 49, and the obligation to reduce and remove cloud switching and egress charges under the Data Act is kept [14]. The proposal had not been adopted as of October 2026, and the European Parliament had not adopted its position [14]. It is not law, and organizations should plan on the current texts.

5. EU data and cloud rules beyond personal data

5.1 The Data Act

The EU Data Act has applied since 12 September 2025 [15]. Its Chapter VI requires providers of data processing services, including cloud services, to remove obstacles to switching to another provider or to on-premises infrastructure and to enable the use of several providers in parallel [15]. Switching terms must be in a written contract with a maximum notice period of two months and a maximum transition period of 30 calendar days [15]. Until 12 January 2027 providers may charge reduced switching charges, including data egress charges, not exceeding their direct costs; from that date they may charge none for switching, while egress charges for parallel use of several providers may continue at cost [15]. Article 32 requires providers to take technical, organizational and legal measures to prevent third-country governmental access to non-personal data held in the EU where it would conflict with EU or national law, mirroring GDPR Article 48 for data that is not personal [15]. For governance, the Data Act makes exit planning and multi-cloud a regulated right rather than only a negotiation, and extends jurisdiction concerns to industrial and other non-personal data.

5.2 Cloud sovereignty certification and the proposed Cloud and AI Development Act

The European cybersecurity certification scheme for cloud services, EUCS, has not been adopted. The draft published for consultation in 2020 required providers to be transparent about the location of data and applicable law but did not restrict location [16], and the Commission stated in June 2026 that work on the scheme will resume alongside the revision of the Cybersecurity Act [4]. In the same document, the Commission proposed a Cloud and AI Development Act that would establish an EU cloud sovereignty framework with four assurance levels, recognized by national authorities, sovereignty risk assessments for public bodies, and minimum levels for public procurement, with higher levels required for activities relevant to public order [4]. The proposal notes that the Data Privacy Framework does not remove sovereignty concerns, because sovereignty also covers operational autonomy [4]. It was a proposal in October 2026, and its levels may change in negotiation.

5.3 Financial services

DORA adds a corporate-presence rule for critical cloud providers. The European Supervisory Authorities designated critical ICT third-party providers on 18 November 2025, and according to their joint guidance a financial entity may use a designated provider established in a third country only if the provider has established an EU subsidiary within twelve months of designation [17]. This is a rule about oversight and operational control, not data localization, but it shapes which provider entities financial institutions can contract with.

6. The UAE, Saudi Arabia and Egypt

The Gulf and Egypt have adopted comprehensive data protection laws with transfer rules, at different stages of implementation. Table 2 summarizes their status. Readers should note the source column: several official texts could not be opened for this paper.

Regime	Regulator	Main transfer routes	Status as of October 2026	Source basis
UAE federal PDPL (Decree-Law 45 of 2021)	UAE Data Office	Adequate jurisdictions; contract; consent; contract necessity	In force since 2 January 2022; executive regulations not yet issued	Official portal for status; transfer articles from secondary sources
DIFC Data Protection Law 2020	DIFC Commissioner of Data Protection	Adequacy list; standard clauses; binding corporate rules; derogations	In force	Official
ADGM Data Protection Regulations 2021	ADGM Office of Data Protection	Adequacy; standard clauses; binding corporate rules; derogations	In force	Official
Saudi PDPL and Transfer Regulation	SDAIA	Adequacy and listed purposes; SDAIA clauses; binding common rules; accreditation	Fully enforceable since September 2024; amended Transfer Regulation since September 2024	Instruments confirmed officially; content from secondary sources
Egypt PDPL (Law 151 of 2020)	Personal Data Protection Centre	License or permit, with consent and adequate destination	Executive regulations since November 2025; grace period ending about 1 November 2026	Secondary sources

6.1 United Arab Emirates

The federal Personal Data Protection Law has been in force since 2 January 2022 [18]. According to secondary sources, it allows transfers to jurisdictions with adequate protection and, without adequacy, transfers under a contract binding the recipient to equivalent standards, with the data subject's explicit consent where not contrary to public and security interests, or where necessary for a contract in the data subject's interest, with details deferred to executive regulations [18]. Those regulations had not been issued according to the latest sources found, and the official portal still describes the federal Data Office prospectively [18]. The law does not apply in free zones that have their own data protection law. The Dubai International Financial Centre allows transfers to jurisdictions on its published adequacy list and

otherwise under safeguards such as its standard contractual clauses and binding corporate rules [19]. Abu Dhabi Global Market treats transfers to onshore UAE as transfers to another jurisdiction, counts remote access as a transfer and provides adequacy, standard clauses, binding corporate rules and derogations [20]. An organization present onshore and in both free zones therefore operates under three transfer regimes in one country.

6.2 Saudi Arabia

Saudi Arabia's Personal Data Protection Law, as amended in 2023, has been in force since 14 September 2023 and fully enforceable since September 2024, with the Saudi Data and Artificial Intelligence Authority as regulator [21]. SDAIA's official listing confirms the law, its implementing regulation, the Regulation on Personal Data Transfer Outside the Kingdom, standard contractual clauses and a guideline on assessing transfer risks [21], [22]. According to secondary sources, the amended Transfer Regulation of September 2024 permits transfers to jurisdictions SDAIA finds adequate and for listed purposes, and otherwise under one of three safeguards: SDAIA's standard contractual clauses, which must be used without modification, binding common rules for corporate groups, or certificates of accreditation [22]. A transfer risk assessment is required when relying on a safeguard and for continuous or widespread transfers of sensitive data, and SDAIA had not published an adequacy list on the sources found [22].

6.3 Egypt

Egypt's Personal Data Protection Law of 2020 became operational when its executive regulations were issued in November 2025, according to secondary sources, which designate the Personal Data Protection Centre as regulator [23]. Transferring, storing or giving access to personal data outside Egypt requires a license or permit from the Centre, explicit consent and a destination with an adequate level of protection [23]. The one-year period to regularize ended at about the end of October 2026, so full enforcement begins as this paper is published [23]. All Egyptian details in this paper come from secondary sources and should be checked against the official texts.

6.4 What the regimes share

Despite their differences, the regimes share a structure that can be governed in one program: an inventory of where personal data goes, a legal route for each flow, a documented risk assessment for flows that rely on safeguards, and the ability to suspend a flow when the assessment changes. The EU's transfer impact assessment [8], the DIFC's export assessment tools [19] and SDAIA's transfer risk assessment [22] are variations on that pattern. The main differences are in prior approval, which Egypt requires through licenses and permits [23], and in the clauses themselves, which Saudi Arabia requires to be used verbatim [22].

7. Technical controls

7.1 Location guardrails

All major clouds offer preventive controls on where resources can be created, expressed as policy. Google Cloud's resource location organization policy restricts the locations of new resources using curated value groups, but it is not retroactive, does not cover global resources and does not detect existing violations [24]. Assured Workloads binds a folder to a control package that restricts regions, and documents that its residency commitment covers customer data at rest for location-configurable services, not resource names, labels or service data such

as billing metadata [25]. Azure's built-in "Allowed locations" policy denies creation or update of resources outside an allowed list, and excludes resources that use the global region [26]. AWS Control Tower offers Region deny controls implemented as service control policies, with exemptions for certain global services and the home Region [27]. Every guardrail has documented gaps, so preventive policy must be paired with detective inventory, and personal data should not be placed in resource names or labels [25].

7.2 Sovereign cloud offerings

Providers now offer constructs aimed at residency and operational control. Microsoft's EU Data Boundary commits to storing and processing customer data and personal data for its enterprise online services in the EU and EFTA, completed in phases from 2023 to February 2025 [28]; its documentation describes limited continuing transfers and per-service configuration, and excludes some arrangements, so the boundary is a matter of configuration and contract rather than a single switch [29]. Amazon Web Services announced general availability of its European Sovereign Cloud in January 2026, with a first region in Germany described as physically and logically separate from other regions and operated by EU residents [30]. Google Cloud's Dammam region in Saudi Arabia illustrates a partner-operated model: customers billed in the Kingdom access it through a local partner, and control packages include partner-operated sovereign controls with a partner-managed external key manager [31]. These offerings address residency and operational control. Whether corporate and operational separation fully addresses exposure to the provider's home-country legal process is a legal question that the documentation does not settle and that each organization must assess with advice [8], [10].

7.3 Customer-held keys

Key custody is the main technical lever on jurisdiction exposure. NIST's key management recommendation provides the vocabulary for who generates, stores, uses, rotates and destroys keys [32]. The options form a spectrum from provider-managed keys, through customer-managed keys and imported keys, to keys held outside the provider. Google Cloud External Key Manager keeps key material in a partner key manager outside Google, with per-request justifications [33]. AWS KMS External Key Store performs cryptographic operations in a customer-owned key manager through a customer-operated proxy, and AWS states that for most workloads the availability and latency risk will exceed the perceived benefit [34]. Azure Managed HSM offers single-tenant hardware security modules with attestation-gated key release, and documents external key management as a last-resort option whose end-to-end availability is not covered by its service level [35]. In all three, revoking an external key makes data unreadable, and losing it can make data unrecoverable [33], [34].

7.4 What encryption achieves legally

The EDPB's recommendations define when encryption helps. It can be an effective supplementary measure where data is encrypted before it leaves the exporter's control, the encryption is strong and well implemented, and the keys are retained solely by the exporter or a trusted party in an adequate jurisdiction [8]. That fits storage, backup and archive. It does not fit cloud processing that needs the data in the clear: for that case the EDPB found no effective technical measure given the state of the art [8]. Externally held keys used by a provider's services to decrypt data inside the cloud therefore reduce some risks, but do not by

themselves turn active processing by a provider exposed to disproportionate foreign access into a compliant transfer.

7.5 Confidential computing

Confidential computing is the technology most often proposed to close that gap. The Confidential Computing Consortium defines it as protecting data in use by computing in a hardware-based, attested trusted execution environment, and its threat model excludes sophisticated physical attacks, upstream supply-chain attacks and availability attacks, and acknowledges side channels as a residual risk [36]. Remote attestation, standardized in vocabulary by the IETF, allows keys or data to be released only to an environment that proves what it is running [37], and attestation-gated key release links key custody to confidential computing [35]. Researchers have criticized industry definitions as ambiguous and incomplete [38], a survey catalogs vulnerabilities and countermeasures for one enclave technology [39], an overview of confidential virtual machines documents published attacks and partial mitigations and notes that the hardware manufacturer remains a root of trust [40], and a 2024 attack showed that a malicious hypervisor can break confidential virtual machines on two major platforms [41]. Legal researchers have examined how enclaves relate to data protection obligations [42]. Confidential computing narrows the data-in-use gap, but it is not recognized in the EDPB's recommendations as a supplementary measure for clear-text processing, and its assurances depend on hardware, firmware and patch levels [8], [41].

7.6 Compute to data

The alternative to moving data is to move the computation. Research on compliant geo-distributed query processing shows that conventional distributed query optimizers can produce plans that violate declared data-flow policies, and that a policy-aware optimizer can produce compliant plans [43]; a demonstration shows users declaring constraints such as "only aggregates may leave this site" and the system executing only compliant plans [44]. In products, Starburst's Stargate connector lets a local cluster query a catalog on a remote cluster, pushing joins, limits and common aggregations to where the data lives [45]. Its documentation does not state that only aggregates leave the remote site; what crosses depends on the query and pushdown, so residency must be enforced by access control on the remote side, and the object storage used for parallel result transfer is itself a location decision [45]. Starburst Galaxy's cross-region querying, a private preview within one cloud provider, reads and writes across regions and is a data movement mechanism rather than a residency control [46].

7.7 Copies and evidence

Copies are where residency most often fails. Storage replication can copy objects to other regions or accounts, and the same feature can satisfy or breach residency depending on the destination [47]. Disaster recovery, backups and failover therefore belong in the location inventory and in policy scope. Evidence of location comes from several sources: lineage events identify data sets by a namespace that encodes their storage endpoint, though mapping endpoints to jurisdictions requires an inventory [48]; customer audit logs record the organization's own access; and provider access logs, such as Google Cloud's Access Transparency, record access by provider personnel, including their location [49]. Together they let an organization show, rather than assert, where data and its copies live and who accessed them.

8. The cost of localization

Location rules have costs as well as benefits. Peer-reviewed economic research associates more restrictive data policies, especially restrictions on cross-border data flows, with lower imports of data-intensive services [50]. The Data Act addresses one cost directly by limiting switching and egress charges and protecting parallel multi-cloud use [15]. For an organization, the practical conclusion is to localize where law or risk requires it and to avoid localizing by default, because each additional region, provider and copy adds governance work, cost and failure modes.

9. The operating model

The legal and technical material above can be governed as one program:

- **Classify by jurisdiction.** Tag data sets and products with the regimes that apply to them, their permitted locations and the transfer routes they rely on, and carry these tags in product descriptors and contracts (Paper 3).
- **Keep a transfer register.** Record each flow, including remote access, support, backups and replicas, with its legal route and the date of its last assessment [8], [9].
- **Enforce location as policy.** Use cloud location guardrails at creation time and query-engine and catalog policies at read time, with detective checks for what guardrails miss [24], [26], [27]. Paper 2 describes the policy-as-code approach.
- **Match key custody to the use.** Hold keys outside the provider for storage, archive and backup where the assessment requires it; for active processing, rely on provider and contract choice and on minimizing the data processed [8], [34].
- **Prefer compute to data.** Run queries where data lives, and constrain what may leave [43], [45].
- **Collect evidence.** Combine lineage, inventory, audit logs and provider access logs [48], [49].
- **Reassess on change.** Re-run assessments when laws, court rulings, providers, regions or data change, and watch the pending items in this paper: the appeal against the Data Privacy Framework, the Digital Omnibus, the Cloud and AI Development Act, the UAE executive regulations and enforcement in Egypt [14], [12], [4], [18], [23].

10. Comparative analysis

Table 3 compares the controls by the layer they address, their main limits and a qualitative judgment of maturity drawn from the sources cited.

Control	Layer addressed	Main limits	Maturity
Location guardrails	Residency	Global services, metadata and existing resources outside scope	Mature, with known gaps
Customer-managed and imported keys	Jurisdiction (partly)	Provider still operates the key service	Mature
Externally held keys	Jurisdiction	Availability, latency and data-loss risk; limited service coverage; no help for clear-text processing	Maturing

Control	Layer addressed	Main limits	Maturity
Sovereign cloud offerings	Residency and operational control	Scope set by documentation and contract; legal exposure assessed separately	Maturing
Confidential computing	Data in use	Active attack research; not recognized as a transfer measure	Maturing technically; open as a safeguard
Compliance-aware federated query	Residency	Research prototypes; products push down but do not enforce policy	Open problem
Evidence of location	All layers	Jurisdiction mapping is manual; logs cover supported services only	Maturing

No single control addresses all three layers. A defensible design combines guardrails for residency, provider choice, contracts and key custody for jurisdiction, and offerings and access controls for operational control, with evidence across all of them.

11. Open challenges and future opportunities

11.1 Processing in the clear

Challenge. No technical measure is recognized for clear-text processing by a provider exposed to disproportionate foreign access [8]. **Research direction.** Confidential computing with robust attestation and resistance to the attacks shown in recent research [40], [41].

Opportunity. A recognized measure for data in use would allow processing in global clouds with assurance comparable to encrypted storage.

11.2 Legal stability

Challenge. Key instruments are contested or pending, including the Data Privacy Framework appeal and the Digital Omnibus [12], [14]. **Research direction.** Architectures that can switch transfer routes or providers quickly, supported by the Data Act's switching rights [15].

Opportunity. Designs that tolerate legal change would turn rulings from crises into planned migrations.

11.3 Defining sovereignty levels

Challenge. The meaning of cloud sovereignty is contested and EU certification is unsettled [1], [16]. **Research direction.** Assurance levels with testable criteria, as proposed in the Cloud and AI Development Act [4]. **Opportunity.** Shared levels would let buyers compare offerings on evidence rather than labels.

11.4 Guardrail coverage

Challenge. Location guardrails miss global services, metadata and existing resources [25], [24], [26], [27]. **Research direction.** Detective tooling and inventories that cover every resource type and copy. **Opportunity.** Complete coverage would make residency verifiable rather than assumed.

11.5 Policy-aware federation

Challenge. Query engines push work to remote sites but do not enforce cross-border data-flow policies [43], [45]. **Research direction.** Policy-aware optimizers in production engines [44].

Opportunity. Engines that refuse non-compliant plans would make compute-to-data a control rather than a convention.

11.6 Jurisdiction-aware lineage

Challenge. Lineage records storage endpoints, not jurisdictions [48]. **Research direction.**

Lineage and catalog models that carry legal location and transfer route. **Opportunity.** Transfer registers generated from lineage would stay current without manual effort.

11.7 Gulf and Egyptian implementation

Challenge. Implementing rules are missing or new, adequacy lists are unpublished, and official texts are hard to access [18], [22], [23]. **Research direction.** Comparative studies of transfer regimes in the region as they mature. **Opportunity.** Clearer rules and mutual recognition would

reduce the cost of regional data flows.

11.8 Key custody at scale

Challenge. Externally held keys shift availability and recovery risk to the customer and cover limited services [33], [34], [35]. **Research direction.** Resilient external key management with attestation-gated release [35], [37]. **Opportunity.** Practical key custody would let more

workloads keep cryptographic control outside the provider.

12. What this means for platform decisions

Start with an inventory of data sets, flows, copies and support access, and classify each by the regimes that apply. Decide per data class which sovereignty layer matters most, residency, jurisdiction or operational control, and choose controls for that layer rather than relying on one label. Use location guardrails everywhere, add detective checks, and keep personal data out of resource names and labels. Hold keys outside the provider for storage and backup where your assessment requires it, and do not assume that external keys make clear-text processing compliant. Treat replication, backup and failover as transfers to be assessed. Prefer running queries where data lives, and enforce what may leave with access control on the remote side. Collect evidence of location and access, and reassess when the pending legal changes in this paper are decided. Take legal advice in each jurisdiction, especially where this paper relies on secondary sources.

For federated query across regions and clouds, Bassirah works with Starburst as a Strategic Technology Partner; Starburst documents connectors that run queries where data lives with pushdown, and residency outcomes still depend on remote-side access control and on where intermediate results are stored. For catalog, lineage and location metadata, Bassirah provides independent support for DataHub Core, the open-source edition of DataHub; this support is Bassirah's own and is not vendor support from DataHub's maintainers. Other products, projects and standards named in this paper are ecosystem references. In each case, validate the design against your own data, legal advice, providers and versions before relying on it.

Paper 5 turns to privacy-enhancing computation, which offers further ways to analyze data without exposing it in the clear, including some that bear directly on the open challenge of processing data across borders.

References

1. Hummel, P., Braun, M., Tretter, M. & Dabrock, P. (2021). Data sovereignty: A review. *Big Data & Society*, 8(1), 2021, doi:10.1177/2053951720982012. (<https://doi.org/10.1177/2053951720982012>)
2. Pohle, J. & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, 9(4), 17 December 2020, doi:10.14763/2020.4.1532. (<https://policyreview.info/concepts/digital-sovereignty>)
3. Roberts, H., Cows, J., Casolari, F., Morley, J., Taddeo, M. & Floridi, L. (2021). Safeguarding European values with digital sovereignty: an analysis of statements and policies. *Internet Policy Review*, 10(3), 30 September 2021, doi:10.14763/2021.3.1575. (<https://policyreview.info/articles/analysis/safeguarding-european-values-digital-sovereignty-analysis-statements-and-policies>)
4. European Commission (2026). Proposal for a Regulation of the European Parliament and of the Council establishing a framework of measures for strengthening Europe's cloud and AI ecosystem (Cloud and AI Development Act), COM(2026) 502 final, 2026/0138 (COD). European Commission, Brussels, 3 June 2026 (transmitted as Council document ST 10104/26, 4 June 2026). (<https://data.consilium.europa.eu/doc/document/ST-10104-2026-INIT/en/pdf>)
5. European Parliament and Council of the European Union (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Chapter V, Articles 44–50. *Official Journal of the European Union*, L 119, 4 May 2016, pp. 1–88 (CELEX 32016R0679). (<https://eur-lex.europa.eu/eli/reg/2016/679/oj>)
6. European Data Protection Board (2025). Guidelines 02/2024 on Article 48 GDPR, Version 2.1. EDPB, final version adopted 4 June 2025 after public consultation (Version 1.0: 2 December 2024; Version 2.1 of 20 June 2025 only improved an annex). (https://www.edpb.europa.eu/documents/guideline/guidelines-022024-on-article-48-gdpr_en)
7. Court of Justice of the European Union (2020). Judgment in Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems ("Schrems II"), Grand Chamber, ECLI:EU:C:2020:559; Press Release No 91/20. Court of Justice of the European Union, Luxembourg, 16 July 2020. (<https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf>)
8. European Data Protection Board (2021). Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0. EDPB, adopted 18 June 2021 (Version 1.0: 10 November 2020). (https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en)
9. European Commission (2021). Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679. *Official Journal of the European Union*, L 199, 7 June 2021, pp. 31–61 (CELEX 32021D0914). (https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj)

10. European Data Protection Board (2023). Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, Version 2.0. EDPB, final version adopted 24 February 2023.
(https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052021-interplay-between-application-article-3_en)
11. European Commission (2023). Commission Implementing Decision (EU) 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 on the adequate level of protection of personal data under the EU-US Data Privacy Framework. Official Journal of the European Union, L 231, 20 September 2023 (CELEX 32023D1795). (https://eur-lex.europa.eu/eli/dec_impl/2023/1795/oj)
12. General Court of the European Union (2025). Judgment of the General Court in Case T-553/23, Latombe v Commission – Press Release No 106/25 "Data Protection: the General Court dismisses an action for annulment of the new framework for the transfer of personal data between the European Union and the United States". Court of Justice of the European Union, Luxembourg, 3 September 2025.
(<https://curia.europa.eu/jcms/upload/docs/application/pdf/2025-09/cp250106en.pdf>)
13. European Commission (2024). Report from the Commission to the European Parliament and the Council on the first periodic review of the functioning of the adequacy decision on the EU-US Data Privacy Framework, COM(2024) 451 final. European Commission, Brussels, 9 October 2024 (transmitted as Council document ST 14403/24, 10 October 2024).
(<https://data.consilium.europa.eu/doc/document/ST-14403-2024-INIT/en/pdf>)
14. Council of the European Union, General Secretariat (2026). Proposal for a Regulation amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854, (EU) 2024/1689 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868 and Directive (EU) 2019/1024 (Digital Omnibus) – Mandate for negotiations with the European Parliament. Council document ST 10729/26 (LIMITE), interinstitutional file 2025/0360 (COD), 22 June 2026.
(<https://data.consilium.europa.eu/doc/document/ST-10729-2026-INIT/en/pdf>)
15. European Parliament and Council of the European Union (2023). Regulation (EU) 2023/2854 of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). Official Journal of the European Union, L series, 2023/2854, 22 December 2023. (<https://eur-lex.europa.eu/eli/reg/2023/2854/oj>)
16. European Union Agency for Cybersecurity (ENISA) (2020). EUCS – Cloud Services Scheme: EUCS, a candidate cybersecurity certification scheme for cloud services (draft for consultation under Article 49 of the Cybersecurity Act, Regulation (EU) 2019/881). ENISA, December 2020.
(<https://www.enisa.europa.eu/sites/default/files/publications/EUCS%20%E2%80%93%20Cloud%20Service%20candidate%20cybersecurity%20certification%20scheme.pdf>)
17. European Supervisory Authorities (EBA, EIOPA, ESMA) (2025). European Supervisory Authorities designate critical ICT third-party providers under the Digital Operational Resilience Act (press release), with Joint ESAs Q&A 2024_7096 on Article 31 of Regulation (EU) 2022/2554 (DORA). ESMA/EBA/EIOPA, 18 November 2025; Q&A final publication 11 December 2024. (<https://www.esma.europa.eu/press-news/esma-news/european-supervisory-authorities-designate-critical-ict-third-party-providers>)

18. United Arab Emirates (2021). Federal Decree-Law No. 45 of 2021 Regarding the Protection of Personal Data (PDPL), incl. Articles 22–23 on cross-border transfer. UAE federal legislation portal (uaelegislation.gov.ae, legislation 1972), issued 20 September 2021, in force 2 January 2022. (<https://uaelegislation.gov.ae/en/legislations/1972>)
19. Dubai International Financial Centre Authority, Commissioner of Data Protection (n.d., page current October 2026). Data Export and Sharing (guidance page on transfers under DIFC Data Protection Law, DIFC Law No. 5 of 2020, Articles 26–27, and DIFC Data Protection Regulations, Regulation 5). DIFC, Dubai. (<https://www.difc.com/business/registrars-and-commissioners/commissioner-of-data-protection/data-export-and-sharing>)
20. Abu Dhabi Global Market, Office of Data Protection (2021). Guidance on the Data Protection Regulations 2021 – Part 6: International Transfers (VER2.0, 14 September 2021), under the ADGM Data Protection Regulations 2021, Part V (sections 41–45). ADGM, Abu Dhabi. (<https://assets.adgm.com/download/assets/ADGM+DPR+2021+Guidance+Part+6.pdf/e743e728595711ef80b936e29b0f3a63>)
21. Kingdom of Saudi Arabia (2021, amended 2023). Personal Data Protection Law, issued by Royal Decree No. M/19 of 9/2/1443H (16 September 2021), amended by Royal Decree No. M/148 of 5/9/1444H (27 March 2023); with its Implementing Regulation (September 2023). Saudi Data & Artificial Intelligence Authority (SDAIA), National Data Management Office / Data Governance Platform. (<https://dgp.sdaia.gov.sa/wps/portal/pdp/knowledgecenter>)
22. Saudi Data & Artificial Intelligence Authority (SDAIA) (2024). Regulation on Personal Data Transfer Outside the Kingdom (amended version), with Standard Contractual Clauses for Personal Data Transfer (four modules) and Guidelines for Binding Common Rules; plus Guideline for Assessing Risks of Transferring Personal Data Outside the Kingdom (February 2025). SDAIA, amended regulation published 1 September 2024. (<https://dgp.sdaia.gov.sa/wps/portal/pdp/knowledgecenter>)
23. Arab Republic of Egypt (2020; Executive Regulations 2025). Law No. 151 of 2020 Promulgating the Personal Data Protection Law; Executive Regulations issued by Minister of Communications and Information Technology Decree No. 816 of 2025. Official Gazette (Al-Jarida Al-Rasmiya), Executive Regulations dated 1 November 2025. Official text not opened; as reported by Soliman, Hashish & Partners (Legal 500 / Mondaq, 6 April 2026) and Clyde & Co (21 January 2026).
24. Google Cloud (2026). Restrict resource locations (Resource Manager organization policy, `gcp.resourceLocations`). Official documentation, accessed October 2026. (<https://docs.cloud.google.com/resource-manager/docs/organization-policy/defining-locations>)
25. Google Cloud (2026). Data residency | Assured Workloads | Google Cloud Documentation. Official documentation, accessed October 2026. (<https://docs.cloud.google.com/assured-workloads/docs/data-residency>)
26. Microsoft (2025). Pattern: Field properties in a policy definition - Azure Policy (reproduces the built-in "Allowed locations" definition). Official documentation, accessed October 2026. (<https://learn.microsoft.com/en-us/azure/governance/policy/samples/pattern-fields>)
27. Amazon Web Services (2026). Configure the Region deny control (AWS Control Tower User Guide). Official documentation, accessed October 2026. (<https://docs.aws.amazon.com/controltower/latest/userguide/region-deny.html>)

28. Brill, J. and Lorimer, P. / Microsoft (2025). Microsoft completes landmark EU Data Boundary, offering enhanced data residency and transparency. Microsoft On the Issues blog (official vendor announcement), 26 February 2025. (<https://blogs.microsoft.com/on-the-issues/2025/02/26/microsoft-completes-landmark-eu-data-boundary-offering-enhanced-data-residency-and-transparency/>)
29. Microsoft (2026). What is the EU Data Boundary? (Microsoft Privacy, Microsoft Learn; page dated 21 July 2026, content "last updated February 26, 2025"). Official documentation, accessed October 2026. (<https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-learn>)
30. Amazon Web Services (2026). AWS Launches AWS European Sovereign Cloud and Announces Expansion Across Europe. Amazon press release (official vendor announcement), Potsdam, 15 January 2026. (<https://press.aboutamazon.com/aws/2026/1/aws-launches-aws-european-sovereign-cloud-and-announces-expansion-across-europe>)
31. Google Cloud (2026). Dammam region access. Official documentation, accessed October 2026. (<https://docs.cloud.google.com/docs/dammam-region-access>)
32. Barker, E. / NIST (2020). Recommendation for Key Management: Part 1 – General (NIST SP 800-57 Part 1 Rev. 5). NIST Special Publication 800-57 Part 1 Rev. 5, May 2020. (<https://doi.org/10.6028/NIST.SP.800-57pt1r5>)
33. Google Cloud (2026). Cloud External Key Manager (Cloud KMS documentation). Official documentation, accessed October 2026. (<https://docs.cloud.google.com/kms/docs/ekm>)
34. Amazon Web Services (2026). External key stores (AWS Key Management Service Developer Guide). Official documentation, accessed October 2026. (<https://docs.aws.amazon.com/kms/latest/developerguide/keystore-external.html>)
35. Microsoft (2026). Azure Key Vault Managed HSM Overview. Official documentation (Microsoft Learn, page dated 9 October 2026), accessed October 2026. (<https://learn.microsoft.com/en-us/azure/key-vault/managed-hsm/overview>)
36. Confidential Computing Consortium (2022). A Technical Analysis of Confidential Computing, v1.3. Confidential Computing Consortium (Linux Foundation) white paper, November 2022. (https://confidentialcomputing.io/wp-content/uploads/sites/10/2023/03/CCC-A-Technical-Analysis-of-Confidential-Computing-v1.3_unlocked.pdf)
37. Birkholz, H., Thaler, D., Richardson, M., Smith, N. and Pan, W. (2023). Remote ATtestation procedureS (RATS) Architecture. IETF RFC 9334 (Informational), January 2023. (<https://www.rfc-editor.org/rfc/rfc9334.html>)
38. Sardar, M. U. and Fetzer, C. (2023). Confidential computing and related technologies: a critical review. Cybersecurity (Springer/SpringerOpen), 6(1), article 10. (<https://doi.org/10.1186/s42400-023-00144-1>)
39. Fei, S., Yan, Z., Ding, W. and Xie, H. (2021). Security Vulnerabilities of SGX and Countermeasures: A Survey. ACM Computing Surveys, 54(6), 1–36. (<https://doi.org/10.1145/3456631>)
40. Bertani, A., Caraccio, D., Zanero, S. and Polino, M. (2025). Confidential Computing: A Security Overview and Future Research Directions. Joint National Conference on Cybersecurity (ITASEC & SERICS 2025), CEUR Workshop Proceedings (ISSN 1613-0073), CC BY 4.0. (<https://ceur-ws.org/Vol-3962/paper70.pdf>)

41. Schlüter, B., Sridhara, S., Kuhne, M., Bertschi, A. and Shinde, S. (2024). HECKLER: Breaking Confidential VMs with Malicious Interrupts. 33rd USENIX Security Symposium (USENIX Security 24), pp. 3459–3476.
(<https://www.usenix.org/conference/usenixsecurity24/presentation/schl%C3%BCter>)
42. Singh, J., Cobbe, J., Quoc, D. L. and Tarkhani, Z. (2021). Enclaves in the clouds: Legal considerations and broader implications. *Communications of the ACM*, 64(5), 42–51.
(<https://doi.org/10.1145/3447543>)
43. Beedkar, K., Quiané-Ruiz, J.-A. and Markl, V. (2021). Compliant Geo-distributed Query Processing. *Proceedings of the 2021 International Conference on Management of Data (ACM SIGMOD 2021)*, pp. 181–193. (<https://doi.org/10.1145/3448016.3453687>)
44. Beedkar, K., Brekardin, D., Quiané-Ruiz, J.-A. and Markl, V. (2021). Compliant Geo-distributed Data Processing in Action. *Proceedings of the VLDB Endowment*, 14(12), p. 2843ff (demonstration). (<https://doi.org/10.14778/3476311.3476359>)
45. Starburst (2026). Starburst Stargate connectors — Starburst Enterprise. Official documentation, accessed October 2026.
(<https://docs.starburst.io/latest/connector/starburst-stargate.html>)
46. Starburst (2026). Cross-region support (Starburst Galaxy documentation). Official documentation, accessed October 2026. (<https://docs.starburst.io/starburst-galaxy/security-and-compliance/manage-cluster-connectivity/cross-region-support>)
47. Amazon Web Services (2026). Replicating objects within and across Regions (Amazon S3 User Guide). Official documentation, accessed October 2026.
(<https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication.html>)
48. OpenLineage project / LF AI & Data Foundation (2026). About OpenLineage; Naming Conventions (OpenLineage specification). Official documentation, accessed October 2026. (<https://openlineage.io/docs/spec/naming>)
49. Google Cloud (2026). Overview of Access Transparency. Official documentation, accessed October 2026. (<https://docs.cloud.google.com/assured-workloads/access-transparency/docs/overview>)
50. van der Marel, E. & Ferracane, M. F. (2021). Do data policy restrictions inhibit trade in services? *Review of World Economics*, 157(4), 727–776, November 2021, doi:10.1007/s10290-021-00417-2. (<https://doi.org/10.1007/s10290-021-00417-2>)

Product and project names are trademarks of their respective owners. Their mention describes publicly documented technology and does not imply a business relationship, except where Bassirah names a Strategic Technology Partner.