

Data sovereignty in the age of AI

Business control and individual rights in the
European Union, the United States and China

Victor A. Kiani
Jasmine Pacheco
Reya Sureshkumar



Contents

Executive summary	3
Power, institutions and distribution	4
Individuals and businesses	5
Control across the AI service	6
Market power and switching	7
Institutional evidence	8
China: the third market	9
European Union-United States cooperation	12
Rights, autonomy and cost	13
European Union and United States policy lessons	14
Testing the recommendation	15
Evidence and method	16
Appendix	17
References	21

Control that businesses and people can use

Enforceable control, a credible exit and personal rights must decide every AI purchase.

Domestic dependence

Domestic supply does not prevent dependence.

How can businesses control AI services, change suppliers and protect individuals' rights across the European Union (EU), the United States (US) and China? This report answers that question for business decision-makers and the policymakers who shape their choices. The EU and US form the core comparison. China is the third regulatory market: an international business must satisfy all three.

Each actor wants something different. A business protects sensitive records and avoids interruption. A person wants limits on how organisations use their information. Governments set rules while pursuing strategic goals and seeking data access. Every control faces the same test: whose choices improve, and who carries the costs?

Location and control

Storage location does not settle processing or access.

Businesses must secure enforceable control over data and a credible ability to change suppliers, and reserve stronger isolation for defined risks. Governments must make those choices practical and protect lawful data flows. Greater business control must also protect the customers and employees whose information makes the service useful.

Require evidence of the whole data route, a working exit and usable rights processes. The EU must make protections and alternatives easier to use; the US must strengthen consistent rights and practical customer choice. China applies its own rights and transfer rules, and separates developer origin from operation. Test every arrangement on the company's real workload before committing.

Distinct interests

Company autonomy does not protect personal rights by itself.

Domestic supply does not prevent dependence. Storage location does not settle processing or legal access. A company can gain independence from its supplier while giving people less say over their information. National strength, corporate autonomy and individual rights are different outcomes. [5-8,27]

Rules, power and the distribution of control

Markets rest on institutions

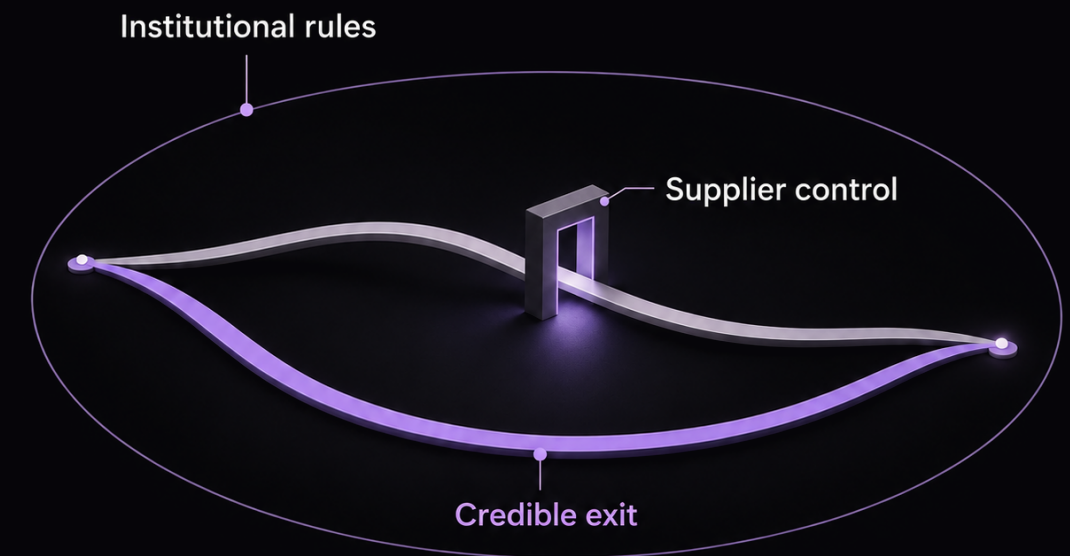
Stilwell treats markets as part of a wider institutional order: enforceable contracts, public rules and state decisions shape economic activity. Applied to data sovereignty, the questions become who can access data, which obligations govern the service and whether people and organisations can enforce them. A storage location answers none of these. The EU-US comparison therefore examines how each institutional setting turns a formal promise into an action a person or business can take. [41]

Concentrated resources create power

Sackrey, Schneider and Knoedler connect concentrated economic resources with political power, including influence over regulation and competition. For supplier dependence, technical capability and contractual choice matter only alongside the buyer's practical ability to challenge terms, recover its records and leave. An alternative on a product list gives no leverage if the buyer cannot keep essential work running when it switches. Operating capability gives contractual choice its meaning. [42]

Benefits and burdens differ

Stilwell also asks who gains, who loses and who can act. That keeps individuals, workers, smaller firms and the public in view alongside buyers and providers. The assessment identifies who receives useful capabilities, who bears compliance and transition costs, and whether remedies work for those affected. Corporate autonomy alone is not success: a recommendation must preserve personal rights and keep disproportionate adjustment costs off workers, smaller firms and taxpayers. [41-42]



The same information creates different control problems

An individual

Information, rights
and a usable remedy

Consider a person using an AI assistant to improve a curriculum vitae (CV). They share a document and receive useful suggestions. Later, they want to know what remains, correct an error or request deletion. They need information, usable rights and a way to challenge misuse. Closing the chat answers none of this. [1,3-4,27]

The legal setting decides which tools they have. Within its scope, the General Data Protection Regulation (GDPR) sets a common EU framework for personal-data processing, individual rights and international transfers. The Data Act governs a separate relationship: switching between data-processing services. The US combines federal and sector-specific duties with state protections, and California supplies a concrete rights example. [1-4]

A business

A useful service
that survives a move

A right helps the CV user only when they can understand and exercise it. They cannot inspect a model or trace every retained copy, so the organisation's response to an access or correction request matters as much as any account setting. A clear process turns an abstract right into an action the person can take.

Both settings also govern cross-border activity. The Data Privacy Framework (DPF) covers qualifying transfers to participating US organisations. The US restricts specified sensitive-data transactions involving countries of concern. These mechanisms differ in purpose, coverage and remedies, so the buyer identifies the actual processing arrangement first. Supplier nationality does not settle that assessment. [15-16]

A company faces a broader decision. It wants an internal assistant to search confidential records and cite its answers, and some records hold customer or employee information. It must preserve permissions, protect people and keep the workflow running if it changes suppliers. The same task shows how EU and US rules shape the purchase.

Three purchasing questions connect these decisions. Whose information will the assistant use? What happens when that information crosses borders? What lets the customer change suppliers? Rules and contracts strengthen the buyer's position; operating evidence proves whether the company can act. That means looking beneath the interface at the organisations that make the assistant work.

Follow the data and the authority

Storage, processing, administration and continuity each need their own evidence.

One assistant depends on several organisations. The application decides which records and tools it can use. The model generates answers. Infrastructure supplies the computing, and contracts allocate duties across these relationships. Identify the infrastructure and model providers involved, such as Amazon Web Services (AWS), Microsoft, Google, OpenAI or Anthropic, and the exact service, operator, version and region. [8-13]

Suppose a provider promises to keep the company’s records in Europe. That commitment must state what it covers: storage, model processing, logs or calls to external tools. OpenAI’s application programming interface (API) documentation separates storage, regional processing and system data. Anthropic separates its direct service from partner-operated platforms. A regional label needs a precise scope. [8-11]

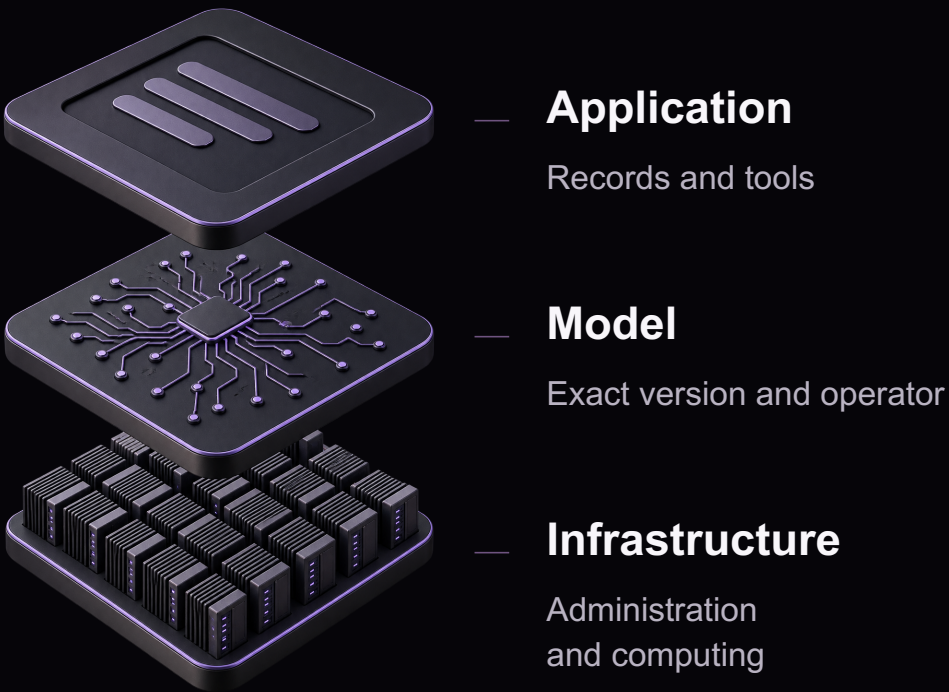
Follow the assistant as it retrieves a document, generates an answer and calls another tool. Each step creates another copy or dependency. Map the complete journey for the exact endpoint and features the buyer will use, so the assessment describes the service that will actually handle the records.

Authority raises further questions. Who administers the service? Which legal process reaches covered data? Who can revoke access or stop the system? Section 2713 of US law reaches records in a provider’s possession, custody or control through applicable legal process, regardless of where they are stored. [7]

A buyer can restrict access to stored documents and still depend on the provider’s authentication or updates to keep operating. Another arrangement offers strong recovery but leaves an unacceptable administration path. Assessing confidentiality and continuity together stops one attractive feature from standing in for the whole control assessment.

A storage promise meets one requirement and leaves others open. Buyers demand evidence on administrators, keys, updates and termination. Stronger isolation is justified when existing controls cannot address a defined exposure. The resulting service must still work securely and usefully; confidentiality and continuity require different investments.

THE SERVICE ARCHITECTURE



Contracts allocate responsibilities across the layers.

A credible alternative changes the buyer’s position

The market behind these contracts has unequal financing. Stanford’s 2026 AI Index reports 2025 private AI investment of about US\$285.9 billion in the United States, US\$20.9 billion in Europe and US\$12.4 billion in China. The US total is about 13.7 times Europe’s. These figures frame the options buyers can investigate. [24]

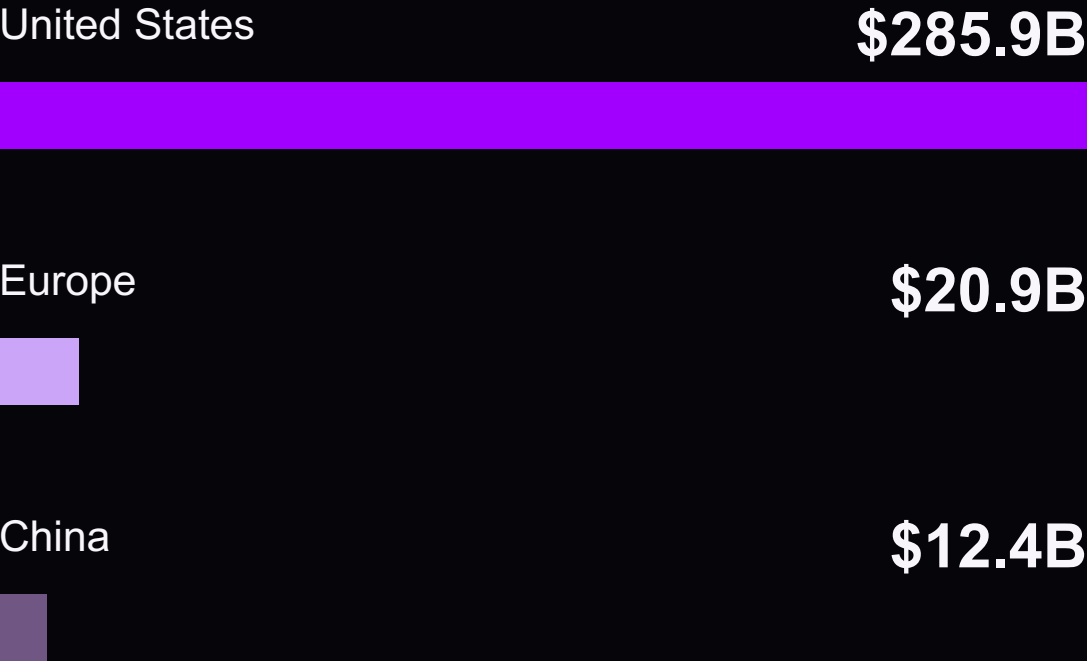
A buyer discovers its dependencies when it tries to leave. Downloading records is the easy part; rebuilding search indexes, permissions and application connections takes far more work. Staff also need a replacement that keeps the essential routine running. A useful service running elsewhere is the real test of independence, not an export button.

Test four steps: export the records and their context; rebuild a minimum useful service; revoke old access; and verify remaining data obligations. Measuring time, labour, interruption and replacement quality exposes dependencies an export button conceals. A credible alternative strengthens bargaining power before the company ever leaves. [2,5-6,25]

A credible exit does not need every feature on day one. Define the minimum useful service and acceptable interruption before comparing suppliers. Those requirements keep the exercise tied to the business and set the basis for judging the fallback’s cost. The aim is enough capability to keep a real choice, not a claim of complete independence.

The EU Data Act removes covered switching charges from 12 January 2027. That removes a defined obstacle; migration, rebuilding and staff time still cost money. US cloud customers report transfer-cost and licensing barriers. Policy and operating capacity meet here: removing a barrier pays off when the customer can use the resulting choice. [2,5]

Private AI investment, 2025



US dollars. Stanford AI Index 2026. [24]

Enforceable terms and operating capacity work together

Public-sector cases show enforcement at work and the practical limits of supplier choice.

A public agency carries extra responsibilities. Take an assistant searching policy and administrative records: the agency must justify the purchase, protect the information and maintain continuity. As major customers, governments also shape supplier behaviour through the terms they demand. Two institutional cases show enforcement and purchasing at work.

In July 2025, the European Data Protection Supervisor (EDPS) reported that the Commission had brought its examined Microsoft 365 use into compliance after corrective work. Scrutiny changed the arrangement: buyer and supplier had to fix the identified problems. Enforceable obligations produce concrete changes in the service relationship. [22]

The Government Accountability Office (GAO) interviewed 24 selected US agencies about cloud procurement. Seventeen reported cost-management challenges; eleven reported technical issues with adopting multiple vendors, including interoperability. Having several suppliers did not remove the work of managing costs or connecting systems. [23]

Together, the cases establish two conditions of usable choice: enforceable terms and the operating capacity to use alternatives. Neither delivers the other. A company assessing an AI service tests both against its own workload instead of inferring readiness from a contract or a count of suppliers.

Government influence goes beyond procurement. An enforcer makes obligations effective; a purchaser negotiates the arrangement; a policymaker shapes the protections. One institution can hold several roles, each with its own mechanism. Commercial autonomy improves when those mechanisms give buyers usable options.

Governments must use purchasing to demand clear data routes, understandable terms and realistic recovery and exit plans. Reusable evidence from those purchases helps commercial customers demand the same assurances. [31]

Cloud procurement challenges

Cost-management challenges



Multi-vendor technical issues



GAO interviews with 24 selected US agencies. [23]

China: the third market

An international business must satisfy EU, US and Chinese rules at the same time.



Three markets, one business

An international business must satisfy all three regimes at once.

Obligation	European Union	United States	China
Core framework	General Data Protection Regulation (GDPR), with the Data Act for switching between data-processing services [1-2]	Federal and sector-specific duties combined with state protections [3-4]	Personal Information Protection Law and cross-border data provisions [14,36]
Personal rights	Access, correction and deletion within the GDPR’s scope [1]	Set by state and sector; California gives residents rights against covered businesses [4]	Access, correction and conditional deletion [36]
Data leaving the jurisdiction	Transfer safeguards; the Data Privacy Framework (DPF) covers qualifying transfers to participating US organisations [1,16]	Restrictions on specified sensitive-data transactions involving countries of concern [15]	Exemption, standard contract, certification or security assessment, set by exporter, data, volume and purpose [14,39-40]

One AI service answers to all three regimes. Map each obligation to the exact data route before deployment.

[1] [2] [3] [4] [14] [15] [16] [36] [39] [40]

Origin, operator and data route answer different questions

Rights and hosted use

China combines personal rights, state authority and model supply. Its Personal Information Protection Law grants rights including access, correction and conditional deletion. Outbound-transfer rules separate specified exemptions from transfers that need a contract, certification or security assessment. Separate rules set privacy and content obligations for generative AI offered to the public in China. [14,36-37]

Take the CV user choosing DeepSeek's hosted chatbot. Its privacy policy states that inputs and uploaded files are subject to collection and that personal data is processed and stored in China. It offers a training opt-out and rights under applicable law. A training opt-out does not settle retention or deletion, so the user needs the exact service relationship. [38]

Outbound transfers

A company's China subsidiary wants to send employee records to overseas headquarters for an internal AI workflow. It classifies the information, purpose and transfer before choosing a route. Specified cross-border human resources (HR) activities qualify for an exemption under stated conditions; convenience alone does not establish eligibility. Other transfers need a contract, certification or security assessment. [14,39-40]

The route depends on the exporter, data categories and volume as well as purpose. The HR exemption excludes important data, and certification cannot replace a legally required security assessment. Underlying duties continue to apply under any exemption, and the receiving EU or US operation meets its own obligations separately. [14,39-40]

Local operation

A buyer can also run locally operated weights. Qwen3.8-27B provides Apache 2.0 weights and local-serving instructions. When the complete workflow stays in the buyer's environment, prompts do not go to the Chinese developer. The buyer then owns the checks on connections, telemetry, tools, updates and remote administration, plus hardware, skills and security. [12,26]

These cases separate origin from operation. DeepSeek's hosted service and locally operated Qwen are different configurations. Developer nationality establishes neither the data route nor who can act on the service. EU and US buyers apply the same rights, quality and exit tests to each exact arrangement. Local operation removes one dependence and moves other responsibilities to the buyer.

Cooperation continues alongside disagreement

Transfer safeguards



2016

Privacy Shield

Invalidated in 2020



2023

Data Privacy Framework

Qualifying transfers

Businesses need evidence about each service while governments negotiate the conditions for international activity. The transatlantic record shows engagement, disruption and changing institutions. Obama-era Privacy Shield created a transfer route in 2016; in 2020 the Court of Justice invalidated its adequacy decision. Durability depends on safeguards and legal foundations. [16-17]

Under Biden, the EU and US established the Trade and Technology Council (TTC) and adopted the 2023 Data Privacy Framework. The council coordinated technical work on AI; the framework covers qualifying transfers to participating US organisations. Political and technical cooperation supports business activity, and each customer stays responsible for its own arrangement. [16,18]

Cooperation channels

2021-2024

Trade and Technology Council

AI and technical coordination

2025-2026

Trade and digital dialogue

2025 framework; dialogue sought in 2026

The Trump administration’s 2025 trade framework included digital commitments and AI-chip intentions. In July 2026, the Office of the United States Trade Representative (USTR) sought dialogue over regulatory disputes. The Commission describes the TTC format as inactive. Engagement continues alongside conflict and changing channels. [19-21]

Businesses need clear responsibility when provider terms or transfer channels change, with lawful contingencies that protect the essential workflow and personal rights. Governments reduce uncertainty through durable safeguards and remedies, and technical coordination makes evidence easier to compare. Political announcements do not make a transfer lawful or a supplier’s controls adequate. Cooperation supports buyer autonomy when governments preserve lawful options and customers keep the evidence and capacity to use, challenge or leave a service. [16-21]

Business independence must preserve personal rights



Required controls

Rights, access and lawful use

Supplier independence shifts power without improving everyone's position. A company can run its own model while expanding employee monitoring. Customers and workers need understandable limits and usable rights processes. Limit unnecessary collection, fund training and involve workers before changing performance monitoring. Smaller firms need shared testing and contract resources to manage fixed costs. [1,4,27]

The operating arrangement decides who carries the work. A managed service reduces the burden of running a model. A regional or sovereign offering adds boundaries the buyer verifies. Buyer-operated weights put responsibility for the environment on the customer. These arrangements overlap, so assess the actual service against the task, not the label.



Useful task quality

Same task and quality target

No label settles suitability. A regional offering can omit a needed feature, and an open license supplies neither hardware nor qualified staff. A managed service can satisfy the controls without local operation. The question is which exact configuration meets the company's requirements and protects the people involved. [8-13,26]

Apply three decision gates. First, meet every mandatory control, including applicable personal rights: carry access, correction or deletion requests through the relevant records, indexes and logs. Next, meet a pre-set quality threshold on the same documents and access rules. Finally, compare full costs, including integration, staff, maintenance, interruption and exit. [1,4,26-27]



Compare full cost

Compute, people, upkeep and exit

Full cost puts these choices on a common basis. A local model shifts spending toward hardware, staff and maintenance; a hosted service still requires integration and migration work. Counting only the subscription or equipment purchase hides those responsibilities. Compare what it takes to sustain acceptable service and an eventual exit.

A failed mandatory control blocks deployment. If no arrangement qualifies, redesign the task or service. Where several qualify, choose the simplest suitable option. This ties stronger isolation to a defined need and keeps the decision grounded in evidence.

Make protections usable and alternatives credible

EU policy

EU policymakers must help businesses use existing rights through reusable evidence, proportionate assurance and migration support. They should also learn from US cloud providers' scale and service breadth while backing credible alternatives. The European Investment Bank (EIB) describes the strong US infrastructure position and the narrower service range of many European and Chinese providers. The goal: more useful choices, with quality and workable exits intact. [1-2,35]

Costs and adjustment

These recommendations carry costs as well as benefits. Assurance demands weigh most on smaller firms, and subsidies can protect a favoured supplier without improving customer choice. Shared testing and contract resources cut repeated work; funded training and consultation help workers adapt. Public support must carry transparent performance conditions and periodic review, so taxpayers do not fund alternatives customers cannot use or leave.

US policy

US policymakers should learn from the EU's enforceable personal-data rights and switching protections. A clearer baseline reduces fragmented protection. Competition scrutiny must examine dependence across applications, models and infrastructure. Hosting successful suppliers does not guarantee that ordinary customers can negotiate terms or leave. [1-6,25]

Government roles

Governments shape the market as negotiators, enforcers and customers. Durable transfer safeguards and credible remedies support lawful activity. Public purchases must demand clear terms, common evidence and tested exits, setting practices commercial buyers can also demand. Each buyer remains responsible for its particular service. [16,18-21,25,31]

Testing the recommendation

Test rights, service quality and a workable exit before committing.

Start with the company’s document-search task. Classify the records, map data routes and identify access restrictions and applicable rights. Assign responsibility for the service and set quality and interruption thresholds before assessing results. A separate review team examines the evidence; the accountable business leader decides whether the arrangement meets the requirements. [26-27]

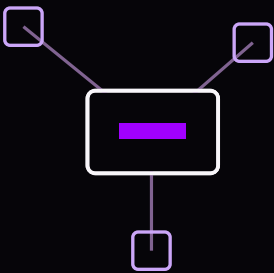
Compare feasible configurations on common documents and access rules. Record answer quality, citation support, permission failures, response times and full operating costs. Each option must sustain a useful service under the required controls. Failures feed directly into the purchasing decision, including redesign of the task or arrangement.

Test the exit as part of that decision. Export records and context, rebuild a minimum useful service elsewhere, revoke old credentials and check remaining data and obligations. Measure the effort, disruption and replacement quality. If the alternative cannot sustain the essential workflow, document the dependency and the measures that manage it. [2,5-6,25-27]

Keep the comparison consistent. Use the same documents, permissions and service requirements, and record real differences instead of forcing unlike configurations into one score. A lower price never compensates for a failed mandatory control. Cost or quality shortfalls trigger reassessment before the decision to proceed.

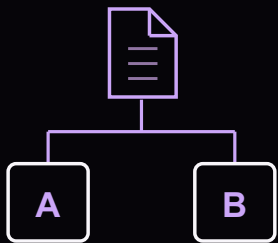
Let the evidence set the level of isolation. When a managed option meets the requirements, its lower complexity wins; a defined risk justifies local operation and its extra expense. Where no feasible alternative exists, disclose the dependency and negotiate proportionate mitigations. Reject or redesign any arrangement that fails mandatory requirements.

The standard is usable business choice that protects people. EU and US rules shape rights and supplier relationships; China adds a third rulebook and separates a model’s origin from its operation. Testing proves whether a buyer can exercise the control it seeks: a tested exit proves control, and a defined risk justifies stronger isolation.



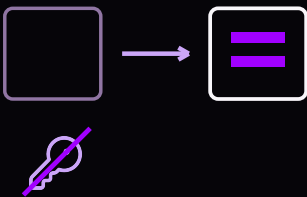
Map the service

Routes, rights and responsibility



Compare options

Same task.
Controls, quality and cost.



Test the exit

Rebuild elsewhere.
Revoke and verify.

Evidence and method

Evidence base

The analysis rests on documented law, official guidance, published service terms and institutional studies from the European Union, the United States and China, current to October 2026. Primary legal texts and regulator publications anchor every legal claim; provider documentation anchors every service claim.

Comparative design

One business task runs through the whole comparison: an internal assistant that searches confidential records and cites its answers. Holding the task constant isolates how each jurisdiction's rules, the provider arrangement and the buyer's operating capacity change control. The individual and public-institution cases test the same questions from two other positions.

Institutional evidence

Two observed cases ground the argument. The European Data Protection Supervisor's Microsoft 365 finding shows enforcement changing a live arrangement. The Government Accountability Office's interviews with 24 agencies show the operating cost of multi-vendor cloud. Each case answers a different question; together they establish that usable choice needs both enforceable terms and operating capacity. [22-23]

Course framework

Stilwell's institutional view and Sackrey, Schneider and Knoedler's account of economic power structure the analysis around three questions: who holds rights, who holds leverage and who carries the costs. Every recommendation answers all three. [41-42]

From evidence to recommendation

Recommendations follow from the combined evidence: the legal mechanisms each system provides, the gaps the institutional cases expose and the costs the stakeholder analysis identifies. The testing sequence turns each recommendation into steps a buyer applies to its own workload, with mandatory controls, quality thresholds and full costs set in advance. [26-27]

Key definitions

Data sovereignty here means control a person or business can exercise: enforceable rights, a mapped data route and a working exit. Europe follows the AI Index's regional definition, and the investment figures cover private investment. China's human resources exemption covers necessary employee-information transfers and excludes important data. [14,24,39-40]

Checking provider claims

Provider route	Offering examined	Question for the exact service
Amazon Web Services (AWS)	European Sovereign Cloud / Bedrock	Which models, regions and retention modes apply?
Microsoft	Sovereign Cloud / local operation	Which control and update dependencies remain?
Google	Cloud AI / Distributed Cloud	Which processing, support and connectivity rules apply?
OpenAI / Anthropic	Direct and partner services	Whose terms govern this endpoint and feature?
European alternatives	OVHcloud, Scaleway and other award participants	What evidence supports this workload?

Verify each provider’s contract, configuration and controls for the intended workload. Suitability comes from evidence, not announcements or procurement awards.

[8] [9] [10] [11] [28] [29] [30] [31]

A common purchasing scorecard

Dimension	Observable evidence	Decision criterion
Data control	Tested route and administrative permissions	All mandatory boundaries met
Personal rights	Completed access, correction or deletion exercise	Applicable rights operational
Task quality	Supported answers and source citations	Threshold set before testing
Exit and continuity	Export plus rebuild on an alternative	Fits disruption tolerance
Total cost	Staff, compute, integration, upkeep and exit	Within the full-life budget

Purchasing criteria. Set task requirements and thresholds in advance, and apply the legal requirements of each jurisdiction.

[1] [2] [4] [26] [27]

Open-weight model candidates

The task, data sensitivity and operating capacity decide the model.

Model example	Developer / license	What to assess
gpt-oss 20B / 120B	OpenAI / Apache 2.0 [32]	Size, quantization and task quality
Gemma 4	Google / Apache 2.0 [33]	Variant, languages and tools
Mistral Small 4	Mistral / Apache 2.0 [34]	Memory and serving requirements
Qwen3.8-27B	Qwen / Apache 2.0 [12]	Local controls, license and task fit
DeepSeek-V4.1-Flash	DeepSeek / MIT [13]	Infrastructure, security and support

Candidates, not a ranking. Test representative tasks for answer quality, response time, data controls and full cost on configurations the buyer can support.

Massachusetts Institute of Technology (MIT) license. [12] [13] [32] [33] [34] [26]

Benefits, burdens and responses

Who	Gain	Burden	Response
Individuals	Control over data	Expanded monitoring	Minimise collection. Make rights usable.
Workers	Better tools	Retraining and role changes	Fund training and worker participation.
Smaller firms	Supplier choice	Fixed compliance costs	Share testing and contract resources.
The public	Greater resilience	Subsidies and public costs	Tie support to results and usable exits.

Each response targets the burden beside it. Apply the relevant rights and review whether each response reduces that burden.

[1] [4] [27]

References

[1]

European Parliament and Council (2016). General Data Protection Regulation, Arts. 3, 5, 12-22, 28, 44-49.

[2]

European Commission (n.d.). Data Act explained, Chapters VI-VII.

[3]

Federal Trade Commission (n.d.). Privacy and security: business guidance.

[4]

California Department of Justice (2026). California Consumer Privacy Act: rights and coverage.

[5]

Federal Trade Commission (2023). Cloud computing request for information (RFI): What we heard and learned.

[6]

Federal Trade Commission (2025). Partnerships between cloud service providers and AI developers, §5.2.

[7]

United States Congress (2024 ed.). Title 18, United States Code, §2713: required preservation and disclosure.

[8]

OpenAI (n.d.). Data controls in the OpenAI platform: data residency and limitations.

[9]

Anthropic (n.d.). Data residency: direct and partner-operated platforms.

[10]

Amazon Web Services (n.d.). Amazon Bedrock data retention.

[11]

Google Cloud (n.d.). Generative AI data governance and retention documentation.

[12]

Qwen Team (2026). Qwen3.8-27B: model card and Apache 2.0 license.

[13]

DeepSeek-AI (2026). DeepSeek-V4.1-Flash: model card and Massachusetts Institute of Technology (MIT) license.

[14]

Cyberspace Administration of China (CAC) (2024). Provisions on promoting and regulating cross-border data flows, Arts. 3-8, 10-11.

[15]

U.S. Department of Justice (2025). Data Security Program implementation announcement.

[16]

European Commission (n.d.). EU-US data transfers: Data Privacy Framework.

[17]

Court of Justice of the EU (2020). Schrems II, C-311/18, press release 91/20.

[18]

European Commission (n.d.). EU-US Trade and Technology Council, 2021-2024.

[19]

The White House (2025, August 21). EU-US trade framework, paras. 5, 13, 17, 19.

[20]

USTR (2026, July 23). Statement on EU regulation and transatlantic trade dialogue.

[21]

European Commission (2026, August 7). Update on the closing of the TTC Futurium Community.

References

[22] European Data Protection Supervisor (2025, July 28). Commission’s Microsoft 365 use brought into compliance.

[23] U.S. GAO (2026, June 23). Cloud computing: Federal government needs to address procurement challenges, GAO-26-107530.

[24] Stanford Institute for Human-Centered Artificial Intelligence (2026). AI Index Report: Economy and Technical Performance. 2025 investment data.

[25] Organisation for Economic Co-operation and Development (OECD) (2025). Competition in the provision of cloud computing services. Roundtables on Competition Policy Papers, 323.

[26] Autio, C., et al. (2024). Artificial intelligence risk management framework: Generative AI profile. National Institute of Standards and Technology (NIST), AI 600-1.

[27] European Data Protection Board (n.d.). Respect individuals’ rights: guide for small and medium-sized enterprises.

[28] Microsoft (2026, February 24). Sovereign Cloud: governance and disconnected operation.

[29] Amazon Web Services (2026, January 15). AWS European Sovereign Cloud launch.

[30] Google Cloud (2026, April 22). New innovations in Google Distributed Cloud.

[31] European Commission (2026, April 17). Cloud sovereignty through strategic procurement.

[32] OpenAI (2025, August 5). Introducing gpt-oss: Apache 2.0 open weights.

[33] Google (2026, April 2). Gemma 4: model release and Apache 2.0 license.

[34] Mistral AI (2026, March 16). Introducing Mistral Small 4.

[35] European Investment Bank (2026). Investment Report 2025/2026, Chapter 5, Box B, pp. 217-218: cloud infrastructure scale and service breadth.

[36] National People’s Congress (2021). Personal Information Protection Law, Arts. 3 and 44-50. Official Chinese text.

[37] CAC et al. (2023). Interim Measures for Generative AI Services, Arts. 2, 4 and 11. Official Chinese text.

[38] DeepSeek (2026, February 10). Privacy Policy: inputs, rights, training choices and storage. Published terms.

[39] CAC and State Administration for Market Regulation (2025). Certification measures for outbound personal information, Arts. 5-6. Effective January 2026.

[40] CAC (2026, September 11). Data export security management questions and answers, questions 1-3. Official Chinese text.

[41] Stilwell, F. (2012). Political Economy: The Contest of Economic Ideas (3rd ed.). Oxford University Press. Ch. 1, pp. 3-4; ch. 5, pp. 42-43. Assigned reading.

[42] Sackrey, C., Schneider, G., & Knoedler, J. (2016). Introduction to Political Economy (8th ed.). Economic Affairs Bureau. Ch. 1, pp. 15-17. Assigned reading.

Usable choice. Meaningful rights.



A tested exit
proves control.



Defined risk justifies
stronger isolation.