

Cloud Strategy & Data Localization

Türkiye's Policy Options

AUTHORS

Ulaş Akkaya · Sinan Ülgen

EXECUTIVE SUMMARY

Data has become a strategic determinant of economic welfare, state capacity, and national security. Dependence on cloud services controlled by non-domestic providers creates vulnerabilities for sensitive digital systems, yet a broad, inflexible localization regime would impose substantial costs, hinder productivity, and stifle innovation. This paper argues against a protectionist or blanket localization regime for Türkiye. A more suitable approach is selective, risk-based, and compatible with international data flows: hard localization reserved for a limited set of critical data and systems, conditional cross-border transfers for most personal and commercial data under strong safeguards, and an aggressive domestic datacenter and sovereign-cloud strategy.

The trade-off is high-value sovereignty versus low-value sovereignty — and Türkiye should aim for the first.

CONTENTS

I	Overview
II	The Logic of Localization
III	Legal and Regulatory Architecture
IV	Türkiye's Infrastructure Position
V	Costs, Benefits, and Strategic Trade-Offs
VI	Policy Models for Türkiye
VII	Policy Recommendations for Türkiye



Overview

Data has become a strategic determinant of economic welfare but also state capacity and national security. From the perspective of policy making, dependence on cloud services controlled by non-domestic cloud providers can create dependencies and vulnerabilities for most sensitive digital systems that can possibly be weaponized in times of crises. However, a broad and inflexible localization regime would impose substantial costs on firms and hinder economic productivity. It could also stifle innovation and the scaling up of novel business models. Several authoritative studies support a similar conclusion.¹

This paper argues against a protectionist or blanket localization regime for Türkiye. A more suitable approach would be selective, risk-based, and compatible with international data flows. Hard localization should be reserved for a limited set of critical data and systems. Most personal and commercial data should continue to move across borders under stronger safeguards, including encryption, audits, enforceable contracts, and regulatory oversight. In parallel, Türkiye should pursue a clear datacenter and sovereign-cloud strategy. Ankara should attract hyperscale and colocation investment, strengthen domestic providers, improve legal predictability, use energy and permitting policy as competitive tools, and align with EU-style transfer logic where doing so improves market access.



The Logic of Localization

The current debate often reduces localization to a false choice between openness and strict control. The real policy question should be whether a state can preserve strategic autonomy over the data and digital systems without cutting itself off from the interoperability benefits of the global internet. Governments dwell on this question because cloud infrastructure is concentrated in a small number of firms. AI is increasing demand for low-latency compute and massive storage capacity. At the same

time, digital public services hold large volumes of sensitive administrative, financial, and biometric data. These trends have increased concern over cross-border legal access by foreign authorities, specifically after the EU-U.S. transfer disputes, the U.S. CLOUD Act, and China's state-centered data governance.

Data localization is a legal requirement that certain data be stored and processed domestically.² Data residency is a business choice regarding where data are hosted, without necessarily prohibiting cross-border flows. Data sovereignty concerns which legal authorities can reach the data, the operator, the personnel, or the keys. Cross-border data flows are the transfer, remote access, replication, or onward sharing of data between jurisdictions. Data-center localization concerns the physical siting of infrastructure and the incentives that shape that geography. Cloud localization requires the use of local cloud regions and local control features. Sovereign cloud refers to cloud systems designed to limit foreign legal, operational, and administrative control. It seeks to provide data residency, stronger operational control, compliance tools, and tighter restrictions on operator access without necessarily abandoning the economies of scale offered by hyperscale cloud providers.

Often times, the question "Where is the data?" does not have a simple answer. A dataset may be generated in Türkiye by a patient. It may then be transmitted through telecom backbones and content-delivery networks, processed in one cloud region, cached at the edge, and backed up in another jurisdiction. Even if the data are encrypted, the system may be administered by personnel employed by a company subject to another country's laws. From a policy standpoint, legal control, architectural control, and physical location only partially overlap. If the provider, parent company, or key-management chain remains subject to another jurisdiction the mere domestic placement of servers does not eliminate foreign-interference.

The modern data cycle reflects that complexity. Data are generated continuously by websites, apps, mobile networks, payment systems, industrial sensors, vehicles, hospitals, social platforms, public registries, and AI systems.³ Collection is performed by platforms, app developers, telecom operators, financial institutions, cloud providers,

analytics vendors, cybersecurity firms, public agencies, and, in some sectors, regulated intermediaries.⁴ Once collected, data move through access networks, backbone operators, internet exchange or peering points, CDNs⁵, application layers, and cloud control planes before reaching storage or compute resources. Storage may be on-premises, in colocation facilities, in public cloud, in hybrid architectures, on edge nodes, or in backup and disaster-recovery systems.⁶ Security depends on architecture of encryption, identity and access management, segmentation, redundancy, logging, key control, auditability, incident response, and zero-trust design. NIST's zero-trust architecture is explicit that trust should not be granted based on network location alone.

Therefore, states are competing over infrastructure power. The relevant infrastructure market now includes more than public cloud providers. It includes platform firms such as Meta, Apple, Alphabet, Amazon, and ByteDance; Chinese cloud actors such as Alibaba Cloud, Tencent Cloud, and Huawei Cloud; enterprise and AI firms such as Oracle, IBM, Salesforce, Palantir, OpenAI, Anthropic, and NVIDIA; and infrastructure actors such as Cloudflare, Akamai, Equinix, Digital Realty, and Telehouse.⁷

Different jurisdictions show the range of policy options. The United States combines global cloud dominance with a generally pro-flow position.⁸ However, its legal access mechanisms and restrictions on bulk sensitive-data transactions show that even an open-flow model contains targeted security controls. The EU has developed the world's most influential transfer-governance framework through GDPR, adequacy, SCCs, Schrems jurisprudence, and data-protection enforcement.⁹ However, it still lacks comparable hyperscale dominance and therefore often regulates from a position of market power rather than infrastructure power.¹⁰ China institutionalized a state-centered model through the Cybersecurity Law, Data Security Law, PIPL, and outbound-transfer controls, though it eased some cross-border requirements in 2024 to reduce friction for business.¹¹ India has taken a hybrid route which combining Broad privacy legislation with sector-specific localization in payments. Moreover, it has an ambition to build domestic digital and AI scale.¹² Russia represents the hard-localization end of the spectrum, where localization has also deepened surveillance and market-exit

pressures.¹³ At the other end, Japan and Singapore have pushed variants of trusted data flow rather than blanket localization.¹⁴ Brazil has recently shown that a middle power can strengthen transfer rules and still move toward interoperability including mutual adequacy with the EU in 2026.¹⁵

Türkiye is neither a hyperscale superpower nor a peripheral digital market. The country has a sizable domestic market, meaningful telecom and digital-services capabilities. It also faces large public-sector digitalization needs and has growing industrial-policy ambitions in AI and advanced technologies. Any data localization strategy must therefore preserve market access and investor confidence.¹⁶ That position argues for a calibrated model that more sovereignty where the risks justify it, more openness where the gains are larger, and more attention to infrastructure.

Legal and Regulatory Architecture

The international legal framework is becoming more structured. Under GDPR, transfers of personal data outside the EEA are lawful if the destination benefits from an adequacy decision or if the exporter uses approved safeguards such as standard contractual clauses or binding corporate rules.¹⁷ Schrems II invalidated Privacy Shield and made clear that contractual mechanisms alone are not enough if third-country law undermines "essentially equivalent" protection.¹⁸ Therefore, transfer impact assessments and supplementary measures became central to EU practice. Afterwards, the EU, while continuing to tighten guidance on requests from third-country public authorities under Article 48, rebuilt part of the transatlantic bridge through the EU-U.S. Data Privacy Framework in 2023.¹⁹ The logic is neither free-flow absolutism nor full localization. The goal is conditional interoperability backed by law, documentation, and enforcement.

The U.S. legal structure is important since cloud concentration gives U.S.-based firms an outsized role in global data handling.²⁰ The CLOUD Act permits certain forms of cross-border access through U.S. legal process and executive agreements and the DOJ presents it as a mechanism to reconcile privacy protections with law-enforcement needs.²¹ Moreover, the U.S. has moved beyond a purely liberal transfer posture. The 2025 Data Security Program restricts or prohibits certain transactions that could expose bulk sensitive personal data or government-related data to "countries of concern."²² In other words, even the leading pro-flow jurisdiction is now using targeted, security-based controls. That underscores an important policy point for Türkiye. Selective restrictions tied to specific risks are more defensible than a sweeping localization strategy untethered from threat models.

China represents a more control-oriented model. PIPL requires domestic storage for personal information processed by state organs and imposes domestic-storage obligations plus security-assessment triggers for critical information infrastructure operators and large processors.²³ The Data Security Law and related CAC rules add an "important data" layer and export controls.²⁴ However, China's 2024 regulations on cross-border data flows also remind policymakers that hard regimes often soften when compliance burdens threaten investment and operations.²⁵ That is a caution for Türkiye that it is easier to legislate localization than to calibrate it economically.

India, by contrast, illustrates a more mixed path. The Digital Personal Data Protection Act 2023 does not amount to generalized hard localization but the Reserve Bank's rule that payment-system data be stored only in India remains one of the clearest sector-specific localization requirements anywhere.²⁶ Japan and Singapore have moved in a different direction, trying to operationalize "data free flow with trust" through regulatory interoperability, industry guidance, and trusted data-sharing frameworks.²⁷ Brazil's recent trajectory is also instructive rather than adopting maximalist localization.²⁸ It strengthened cross-border transfer regulation and then moved into mutual adequacy with the EU. These are closer to the kind of pragmatic middle-power strategies that Türkiye can learn from.

Türkiye's data governance is in transition. The backbone remains Law No. 6698 on the Protection of Personal Data, administered by the Personal Data Protection Authority.²⁹ Cross-border transfer rules under KVKK were often criticized as rigid and uncertain in practice. That changed materially in 2024 when Article 9 was amended and the new framework introduced adequacy decisions, standard contracts, binding corporate rules, and a clearer legal basis for transfers abroad.³⁰ At least on paper, the implementing by-law and the Authority's guidance make the Turkish transfer governance closer to the EU model than the old consent-heavy system. This is an improvement for regulatory credibility.

And yet Türkiye's framework remains fragmented rather than a single, harmonized localization code. Personal-data rules interact with information-systems regulation in banking and finance, public-sector cybersecurity rules, national security and critical-infrastructure logic, and sectoral governance in fields such as health and telecom-related services.³¹ The Banking Regulation and Supervision Agency has detailed rules on banks' information systems and electronic banking services.³² The national cybersecurity strategy elevates protection of critical infrastructures and public systems. In addition, the 2025 Cybersecurity Law and the creation of the Cybersecurity Presidency indicate a central-security architecture.³³

Türkiye's data governance oversight ecosystem is broad and fragmented. It includes the Information and Communication Technologies Authority, the Personal Data Protection Authority, the Banking Regulation and Supervision Agency, the Digital Transformation Office, the Ministry of Transport and Infrastructure, the Ministry of Industry and Technology, sectoral ministries, competition authorities, and the newly established Cybersecurity Presidency. This can be an advantage if it produces credible whole-of-government supervision. It becomes a liability if it produces duplication, unclear priorities, or de facto discretionary enforcement. The strongest criticism of Türkiye's current framework is that it still lacks a single, transparent operating logic that tells companies which data must stay, which may move, under what safeguards, and under whose authorization.

For public cloud and government systems, the situation remains cautious. Public digitalization is already massive. The e-Devlet gateway has more than 68 million users, over 1,000 institutions, and nearly 9,000 services.³⁴ That scale alone makes public-sector data governance a matter of state capacity. However, a sovereign-cloud policy for public workloads does not currently mean banning all international providers. It means specifying the conditions under which such providers can be used. These should include workload segmentation, domestic support requirements, screening rules for privileged personnel, local key management, independent security audits, resilience obligations, and emergency-operability standards. The remaining task in legal regulations, is to make those rules coherent and investment compatible.

The current framework has improved but uncertainty remains. On the positive side, the 2024 KVKK reform, the adoption of standard contracts and BCR pathways, the 2024-2028 cybersecurity strategy, the 2025 Cybersecurity Law, and the emergence of data-center incentives improve the policy toolkit.³⁵ On the negative side, the system still presents uncertainty through institutional overlap, incomplete harmonization between privacy and sectoral rules, and limited precedents on how major cross-border transfer and sovereign-cloud questions will be decided in practice. Therefore, Türkiye should avoid an abrupt shift to hard localization because it would magnify discretion before clarifying governance.

IV Türkiye's Infrastructure Position

Türkiye is not yet a first-tier regional hub on the scale of Frankfurt, London, Amsterdam, Paris, or major Gulf campuses. It has growing investment momentum but has not yet become a hyperscale cloud hub. Turkcell reports that it had seven data centers as of the end of 2024 and explicitly describes itself as Türkiye's largest data-center operator.³⁶ It also offers government cloud and multi-cloud services and its cloud

platform obtained ISO/IEC 27017 certification. Türk Telekom continues to present data centers as a part of its digital infrastructure build-out, with efficiency targets that include an annual average PUE goal of 1.2 in next-generation facilities.³⁷

Recent investment announcements show growing interest. Equinix opened its second IBX data center in Istanbul in 2024.³⁸ Khazna Data Centers announced an AI-ready project in Ankara with projected capacity of up to 100 MW.³⁹ A Trendyol-Castle partnership announced a 48 MW Ankara Data Hub.⁴⁰ A Vodafone-DAMAC venture announced a data-center investment in Izmir. And NGN's Star of Bosphorus data center in Istanbul had already signaled, well before the current AI wave, that domestic capital was willing to build at substantial scale.⁴¹ The most important signal came in late 2025, when Turkcell and Google Cloud announced a strategic partnership with plans to establish a Google Cloud region in Türkiye.⁴² Global cloud providers begun to see localized cloud capacity in Türkiye as commercially viable. Most recently AWS announced a Turkish public-cloud region. These projects show that investors view Türkiye as a place to serve regional demand.

Connectivity is the foundation of that transition. Türkiye sits at a critical junction between Europe, the Eastern Mediterranean, the Gulf, the Caucasus, and the Central Asia. It has extensive fixed and mobile networks, a large domestic demand base, and a geography that can support east-west and north-south digital transit. BTK publishes quarterly market data, and the country's leading telecom operators continue to emphasize fiber expansion and backbone investment.⁴³ This is enough to support remarkable domestic cloud and colocation growth. But becoming a regional hub requires more. It requires deeper peering, neutral interconnection ecosystems, more cross-border route diversity, lower latency to adjacent markets, and the credibility or market reputation that persuades global firms to place primary rather than merely secondary infrastructure in-country.

Geography inside Türkiye matters as much as geography outside it. Istanbul is the obvious commercial node. It concentrates enterprise demand, finance, connectivity, digital services, and international business attention. That makes Istanbul the natural

first landing point for carrier hotels, dense peering, and customer-proximate cloud. But it also faces the most acute trade-offs such as land cost, congestion, environmental pressures, and seismic risk. AFAD's current national earthquake-hazard map underscores that site selection in the Marmara basin cannot be treated casually.⁴⁴ An "Istanbul-only" strategy would therefore maximize demand proximity while concentrating physical risk.

Ankara is a different proposition. It is the center of public administration and therefore the natural location for sovereign public-cloud workloads, national registries, and security-sensitive state systems. It also offers inland diversification from Marmara, organized industrial zones, and growing large-scale investor interest. The city's climate is warmer than Eastern Anatolia but far less intense than some southern alternatives. Its long-period average temperatures reported by the meteorological service show that Ankara remains operationally manageable especially when combined with modern cooling design. Arguably, Ankara is Türkiye's most natural governance hub for sovereign workloads.

Izmir and the wider Aegean and western corridor have credible advantages as well such as port access, renewable-energy possibilities, and diversification away from a single overconcentrated digital axis. The announced Vodafone-DAMAC⁴⁵ investment is therefore important even though it does not by itself make Izmir a regional hub. It demonstrates that the "one city, one hub" logic is already giving way to a multi-node model. That is desirable for resilience. For policymakers, it means localization strategy should be spatially differentiated rather than nationally monolithic.

The inland and eastern options are also available. Cooler provinces and higher-altitude inland zones can reduce cooling burdens. The meteorological long-period averages for Erzurum, for example, show mean temperatures still below 20°C even in midsummer⁴⁶, which is materially more favorable for free cooling than much of western or southern Türkiye. Provinces such as Bayburt, Ardahan, and Nevşehir may offer combinations of cheaper land, inland security, and operational diversity. But they also raise questions about fiber density, latency to users, specialist labor, grid redundancy, and ecosystem

depth. In practice, these regions are better suited in the medium term to backup, disaster recovery, cold storage, AI training clusters with looser latency constraints, or selected specialized campuses.

Türkiye is already a meaningful domestic digital-infrastructure market and an increasingly visible destination for new data-center investment. It is not yet a fully consolidated regional hub due to remaining several gaps. Türkiye needs more predictable renewable-energy contracting, stronger legal certainty, better institutional coordination, and a deeper peering ecosystem. It also needs operational hyperscaler regions and a larger pool of specialized talent in data-center design, operations, and cybersecurity. But those are the kinds of gaps that policy can address. The country's aspiration is therefore plausible, provided it is pursued through competitiveness and trust.

v

Costs, Benefits, and Strategic Trade-Offs

The case for caution starts with cost. Modern data centers are expensive and difficult to deliver on schedule. JLL estimates that average global construction costs rose from \$7.7 million per MW in 2020 to \$10.7 million per MW in 2025, with a forecast of \$11.3 million per MW for 2026.⁴⁷ Arizton estimates Turkey-specific construction costs around \$9 million to \$10 million per MW.⁴⁸ Even before localization law enters the picture, this is a capital-heavy sector in which land, utility interconnection, generators, UPS, chillers, racks, security, fire suppression, and network equipment all face supply-chain and financing pressures. Localization rules that force redundant domestic builds for every class of data would therefore convert a strategic-infrastructure policy into a broad capex mandate for the private sector.

Energy availability and environmental constraints will shape the feasibility of Türkiye's data-centre strategy. The IEA reports that data-center electricity demand surged by 17% in 2025 and expects AI to continue pushing power demand upward.⁴⁹ Uptime surveys

show that operators face worsening power constraints, rising costs, and continuing pressure to improve efficiency. Water use is also a non-trivial issue in many cooling configurations, especially in drought-prone areas. For Türkiye a data-center strategy is inseparable from security policy. If Türkiye wants to attract large-scale cloud and AI facilities, it needs grid planning, credible renewable-energy sourcing mechanisms, and a regulatory stance that treats energy and environmental performance as competitiveness variables. The fact that Türkiye's own telecom operators are now advertising PUE improvements and low-PUE targets shows that this logic is already reaching the domestic market.

Compliance costs are subtler but just as important. Under contemporary transfer governances, firms increasingly need data inventories, classifications, transfer mapping, contractual controls, cryptographic design, logging, incident reporting, and, in the EU model, transfer impact assessments. Türkiye's 2024 KVKK reform makes cross-border transfers clearer.⁵⁰ It also formalizes governance work that many firms previously handled informally. In regulated sectors, those obligations stack on top of sectoral requirements. A poorly designed localization law would not replace those burdens, rather, it would add another layer, including local backups, local disaster recovery, local key custody, and local audit trails. Large firms can absorb some of this. SMEs generally cannot do so without losing access either to advanced services or to cost-efficient cloud economics.

The OECD-WTO's 2025 study concludes that more globally interoperable solutions, which balance free flows with trust, are more likely to deliver better economic outcomes than stricter localization.⁵¹ The study estimates that removing existing localization measures would increase exports by 0.26% and GDP by 0.18% on average, with larger gains for more restrictive low-income regimes.⁵² The earlier ECIPE estimate is directionally even starker. In the jurisdictions it modeled, recently proposed or enacted localization-related measures reduced GDP, investment, and exports, and economy-wide localization produced much deeper losses. These establish a presumption for Türkiye that broad localization acts as a tax on digital production.

The security case is equally two-sided. States seek localization because they want resilience, lawful access, sovereign control, and protection against foreign surveillance, which are not irrational. However, localization can also fragment infrastructure and weaken information sharing. It may push firms away from globally mature security stacks toward smaller providers with less scale. It can also create a false sense of sovereignty if foreign legal reach remains intact through parent-company jurisdiction or remote administration. CSIS's study⁵³ stresses that data localization can impair cybersecurity and information sharing even when adopted in the name of national security; it can be a tool of domestic digital authoritarianism, as the human-rights literature on Russia and other cases makes clear.

This means that the benefits of localization are conditional. Local infrastructure can reduce latency, improve service quality for domestic users, strengthen disaster recovery if replication is well designed, create domestic engineering and security jobs, improve policymakers' bargaining power with foreign providers, and support domestic sectors. Public-sector digitalization and AI strategy both make these benefits more valuable. The announced Google Cloud-Turkcell project⁵⁴, the HIT-30 datacenter and AI calls, and the rise of government cloud offerings show that Türkiye now has an opportunity to use regulation to attract infrastructure investment. But the vital phrase is "if properly designed." Local storage without strong encryption, staffing, audits, redundancy, and oversight does not create digital sovereignty.

The trade-off, then, is high-value sovereignty versus low-value sovereignty. High-value sovereignty protects the most sensitive systems, preserves flexibility for the wider economy, and attracts infrastructure investment. Low-value sovereignty mandates domestic storage too broadly, raises costs, and still fails to resolve deep control questions. Türkiye should aim for the first.

Risk Analysis

FIGURE 1 — STRATEGIC RISKS OF BROAD DATA LOCALIZATION		
RISK AREA	LIKELIHOOD	STRATEGIC IMPACT
False sovereignty	High	High
Higher business costs	High	High
Burden on SMEs and start-ups	High	High
Security fragmentation	Medium-High	High
Domestic concentration risk	Medium	High
Investor deterrence	Medium-High	High
Rights and surveillance risk	Medium	High
Trade and interoperability friction	Medium	Medium-High

Under a broad hard localization model, false sovereignty emerges as a high-likelihood and high-impact risk, as data may remain subject to foreign legal reach through provider ownership, remote administration, or key control. If Türkiye localizes selectively, this risk can be mitigated through local key management, privileged-access controls, audit logs, and jurisdiction-sensitive provider structures. Higher business costs also constitute a high-likelihood and high-impact risk, since forced domestic hosting reduces scale economies and duplicates infrastructure; mitigation would require limiting hard localization to narrow critical categories while allowing safeguarded transfers for most business data. Similarly, the SME and start-up burden is high in both likelihood and strategic impact, as smaller firms may lose access to cheaper global cloud tooling and advanced AI services. This can be addressed through safe-transfer pathways, cloud vouchers, and proportionate compliance rules. Security fragmentation represents a medium-high likelihood and high-impact risk, materializing through more facilities, greater complexity, weaker operators, and inconsistent controls; consolidation around qualified providers would be a necessary

mitigating measure. Domestic concentration risk carries medium likelihood but high strategic impact, as overconcentration in one metro or one provider increases systemic vulnerability; multi-region resilience, an Ankara-plus-secondary-region design, and vendor diversity would help reduce exposure. Investor deterrence is a medium-high-likelihood and high-impact risk, as unclear or excessive rules raise perceived political and compliance risks. Türkiye could mitigate this risk by publishing clear classification rules, standardized safeguards, predictable permitting procedures, and transparent enforcement practices. Rights and surveillance risk has medium likelihood but high strategic impact because localization simplifies domestic access without adequate checks. Therefore, judicial authorization, proportionality rules, transparency reports, and independent oversight are essential safeguards. Finally, trade and interoperability friction present medium likelihood and medium-high strategic impact, as restrictions complicate EU-facing services and digital trade. This risk can be mitigated by aligning transfer mechanisms with GDPR logic and trusted-jurisdiction models.

VI Policy Models for Türkiye

A coherent Turkish approach requires choosing among identifiable models. The seven models below are variants of all of them already exist somewhere in the international system. The comparison synthesizes the evidence from EU transfer law, U.S. government-access debates, China's control model, India's sectoral practice, OECD-WTO economic analysis, and Türkiye's own investment and cybersecurity trajectory.

FIGURE 2 — COMPARATIVE ASSESSMENT OF DATA LOCALIZATION POLICY MODELS

Broad hard localization

SOVEREIGNTY GAIN

Superficially high, but often overstated

COST

Very high

INVESTMENT IMPACT

Negative

SME IMPACT

Negative

ADMINISTRATIVE BURDEN

Very high

GEOPOLITICAL EFFECT

Signals digital protectionism

CYBERSECURITY GAIN

Mixed; can fragment defenses

FEASIBILITY

Low-Medium

EU COMPATIBILITY

Low

AI & INNOVATION IMPACT

Negative

ABUSE RISK

High

Sector-specific hard localization

SOVEREIGNTY GAIN

High where truly critical

COST

Medium

INVESTMENT IMPACT

Manageable

SME IMPACT

Limited outside regulated sectors

ADMINISTRATIVE BURDEN

Medium

GEOPOLITICAL EFFECT

Defensible if narrowly drafted

CYBERSECURITY GAIN

High if paired with standards

FEASIBILITY

High

EU COMPATIBILITY

Medium-High

AI & INNOVATION IMPACT

Limited damage

ABUSE RISK

Medium

Soft localization and mirroring

SOVEREIGNTY GAIN

Moderate

COST

Medium

INVESTMENT IMPACT

Mildly positive if flexible

SME IMPACT

Low-Medium

ADMINISTRATIVE BURDEN

CYBERSECURITY GAIN

Moderate

FEASIBILITY

High

EU COMPATIBILITY

High

AI & INNOVATION IMPACT

Low-Medium

ABUSE RISK

Medium

GEOPOLITICAL EFFECT
Interoperable

Medium

Conditional cross-border transfer

SOVEREIGNTY GAIN

Moderate

COST

Medium

INVESTMENT IMPACT

Positive

SME IMPACT

Low

ADMINISTRATIVE BURDEN

Medium

GEOPOLITICAL EFFECT

Supports trusted integration

CYBERSECURITY GAIN

Moderate-High

FEASIBILITY

High

EU COMPATIBILITY

High

AI & INNOVATION IMPACT

Positive

ABUSE RISK

Lower

Sovereign-cloud partnership

SOVEREIGNTY GAIN

High for designated workloads

COST

Medium-High

INVESTMENT IMPACT

Positive

SME IMPACT

Low for users, higher for public buyers

ADMINISTRATIVE BURDEN

Medium-High

GEOPOLITICAL EFFECT

Balances autonomy and openness

CYBERSECURITY GAIN

High if key and operator controls are real

FEASIBILITY

Medium-High

EU COMPATIBILITY

Medium-High

AI & INNOVATION IMPACT

Positive

ABUSE RISK

Medium

Data-center investment hub

SOVEREIGNTY GAIN

Indirect, but economically valuable

COST

Medium

INVESTMENT IMPACT

Strongly positive

SME IMPACT

Positive

CYBERSECURITY GAIN

Indirect

FEASIBILITY

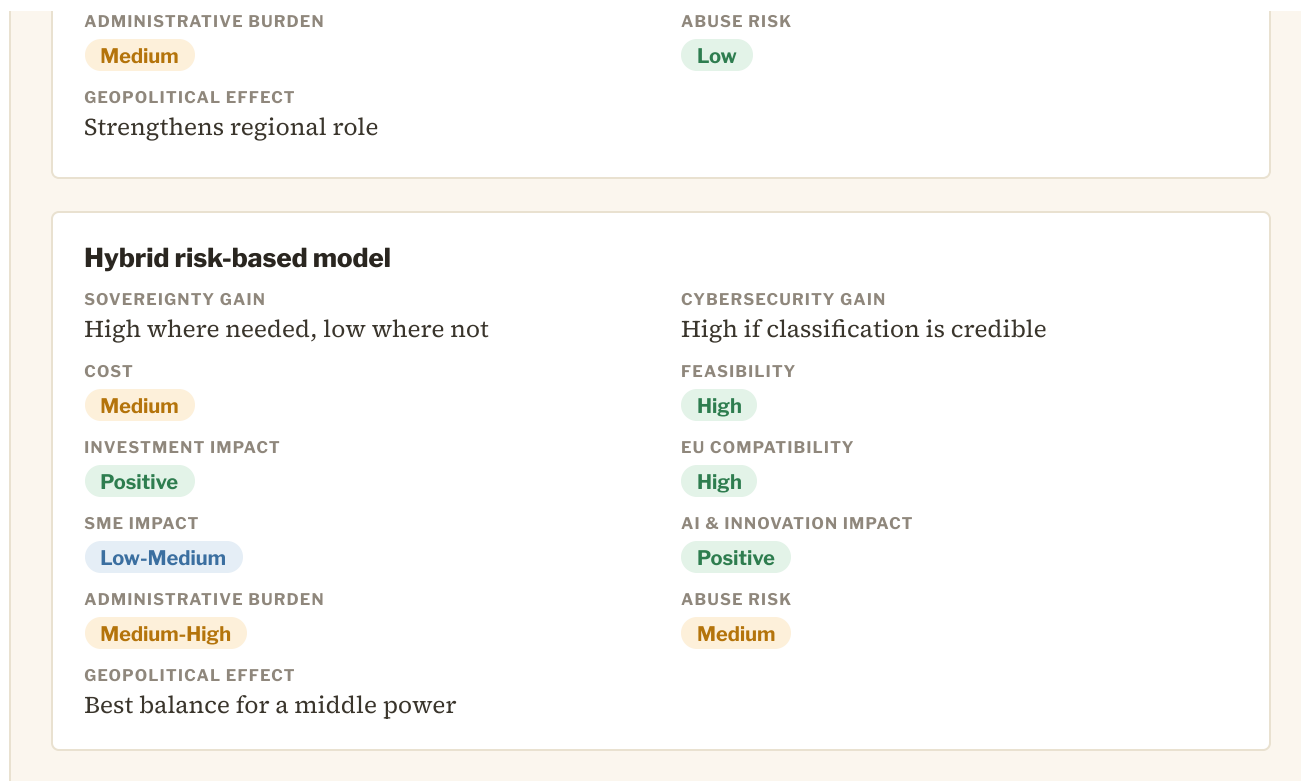
High

EU COMPATIBILITY

High

AI & INNOVATION IMPACT

Positive



Broad hard localization is the least attractive option for Türkiye, because it confuses visible territorial control with actual control, imposes high costs on the economy, and would be difficult to reconcile with the country's ambition to attract global cloud investment while deepening digital trade with Europe. A pure investment-hub model, by contrast, would underperform in national-security terms because it would not define which data and systems must remain operationally sovereign. The two strongest options are therefore the sovereign-cloud partnership model and the hybrid risk-based model. The first is especially useful for public sector, defense-adjacent, and regulated workloads. The second provides the best whole-economy architecture because it differentiates among data categories and risk profiles instead of assuming all data carry the same strategic value. Türkiye should therefore adopt a hybrid, risk-based, and investment-oriented model with three pillars. First, narrowly defined hard localization for a small set of critical categories. Second, conditional cross-border transfers for most personal and commercial data under strong safeguards. Third, an aggressive domestic

infrastructure strategy designed to make localization a competitive choice for many workloads even when it is not a legal mandate. This model is more likely to advance sovereignty, cybersecurity, competitiveness, and regional-hub ambition.

VII

Policy Recommendations for Türkiye

Establishing a National Data-Classification Framework

Türkiye should begin by creating a single national classification framework. At minimum, the categories should include: 1) public data, 2) ordinary personal data, 3) sensitive personal data, 4) critical public-sector registries, 5) defense and intelligence data, 6) critical-infrastructure operational data, 7) health and biometric data, 8) financial and payment-system data, 9) industrial and IoT data, and 10) non-personal commercial data. The purpose is to stop using "data" as if it were a single regulatory object. A birth registry, a hospital image archive, a smart-factory sensor stream, a tax filing, a retail CRM database, and a machine-learning training corpus do not create the same public risks.

Limiting Localization to Clearly Justified Cases

Hard localization should be reserved for narrowly defined categories in which operational sovereignty genuinely is vital. Even here, the rule should not be phrased as "all related data must always remain in Türkiye" without qualification. It should specify the protected function, the operational environment, the recovery requirements, the personnel requirements, and the audit chain. That creates a standards-based system. The 2024-2028 cybersecurity strategy and the 2025 Cybersecurity Law provide the institutional opening for this more exact approach.

Conditional transfers for personal and commercial data

For the overwhelming majority of personal and commercial data, Türkiye should preserve cross-border transfers under a strengthened legal architecture modeled on conditional trust. The 2024 KVKK reform already provides the legal tools such as adequacy-style decisions, standard contracts, BCRs, and a clearer transfer system. Cross-border moves should be allowed where firms can demonstrate legal basis, contract, encryption, auditable access controls, and a risk assessment proportionate to the transfer. This would move Türkiye closer to the logic of GDPR interoperability without copying the EU.

A Turkish sovereign-cloud strategy

Türkiye should define sovereign cloud as a policy and technical standard. A Turkish sovereign-cloud framework should allow participation by both domestic providers and trusted international firms, but only under objective controls such as local key management or customer-held keys for designated workloads, domestically vetted privileged-access personnel, transparent subcontracting rules, independent audits, logging and localization of administrative telemetry where necessary, and clear incident-reporting obligations to the relevant authorities. This is an area where global hyperscalers are already adapting to sovereignty demands in Europe; Türkiye should use that shift to its advantage.

Attracting Investment

Türkiye should pair legal reform with a targeted investment package for cloud regions and data centers. Current policy tools such as HIT-30 have created data-center and AI calls, with a \$30 billion support envelope for high-tech investment by 2030. Existing incentive rules already recognize data centers meeting TS EN 50600 and white-space thresholds. The next step is to turn these initiatives into an operational policy package,

including land zoning, faster utility interconnection, renewable-energy access, transparent permitting, customs predictability, and a published sovereign-cloud investment framework.

Energy and Environmental Governance

If energy policy is treated as an unrelated topic, no Turkish data-center strategy will perform well. Data centers should be integrated into grid planning and clean-power procurement. New large campuses should be expected to demonstrate renewable-energy sourcing plans, realistic PUE targets, water-efficiency measures, and site-specific environmental assessments. Heat reuse should be encouraged where the urban and industrial context makes it viable, but it should not become a formal requirement that blocks investment. The goal is to make sustainability a competitive advantage rather than an ex-post compliance burden. That is consistent both with global operator practice and with the IEA's warning that energy, water, and climate constraints are now inseparable from digital infrastructure.

Regional data-center zoning inside Türkiye

Türkiye should use a differentiated geography strategy. Istanbul should remain the primary commercial interconnection and customer-proximity node. Ankara should be developed as the principal sovereign-public-cloud and continuity node. Izmir and the western corridor could help diversify large private investment and strengthen Aegean connectivity. Inland and cooler regions merit feasibility studies for backup, disaster recovery, cold storage, and selected AI or HPC workloads with lower latency sensitivity. This is where provinces like Erzurum, Bayburt, Ardahan, Konya, Kayseri, and Nevşehir deserve serious feasibility work rather than rhetorical overpromotion. The point is not to force a "hub" into every region; it is to match regional characteristics to workload types.

Alignment with the European Union

Türkiye should pursue compatibility with EU transfer governance. The EU will remain central to Türkiye's digital-investment environment. The more credible and operationally capable Türkiye's transfer tools become, the more plausible future adequacy-like or equivalence-like arrangements become in specific contexts. At minimum, closer alignment lowers transaction costs for firms serving EU markets and reduces the perception that Turkish digital regulation is unpredictable. In digital regulation, credibility is a competitiveness asset.

Institutional coordination and market governance

The institutional architecture should be clarified through a formal coordination mechanism. The Personal Data Protection Authority should lead on personal-data transfer and privacy safeguards. The Information and Communication Technologies Authority should lead on telecom and interconnection issues. The Banking Regulation and Supervision Agency should continue to lead in regulated finance. The Cybersecurity Presidency and Ministry of Transport and Infrastructure should lead on critical-infrastructure resilience and cybersecurity standards. The Ministry of Industry and Technology should anchor investment, incentives, and industrial policy. The competition authority should monitor market concentration and anticompetitive self-preferencing in cloud and colocation markets. A state that wants digital sovereignty must first be administratively coherent.

Domestic capability and protection of rights

Türkiye should support domestic providers. The better way to do so is through certification, public procurement reform, and targeted support for cybersecurity and cloud engineering. The public sector can help create demand by using "sovereign by design" procurement criteria for eligible workloads. Localization must also not become a shortcut to unchecked state access: judicial oversight, proportionality, necessity tests,

ex-post transparency reporting, and independent audit mechanisms are essential if the sovereignty agenda is to retain domestic legitimacy and international credibility. Ultimately, localization without the proper judicial redress and constraints regime is a serious hindrance for the effective development of a cloud enabled technology innovation ecosystem and digital economy.

Roadmap

In the short term, within 12 months, Türkiye should publish a binding classification framework, issue KVKK implementation guidance for the new transfer governance, establish a sovereign-cloud pilot for selected public workloads, launch a formal interagency coordination mechanism, and publish a transparent pipeline of data-center incentive and permitting rules. These actions are low-cost relative to full infrastructure build and would immediately reduce regulatory uncertainty.

Over the medium term, sector-specific localization rules should be introduced only for clearly identified high-risk categories. The aim should be operationalizing a cloud and cybersecurity certification governance, building renewable-procurement and utility-interconnection pathways for large campuses, supporting multi-region public-sector cloud migration, and expanding workforce programs in cloud operations, data-center engineering, and security. This is also the window in which sovereign-cloud partnerships with international providers and domestic operators should move from memoranda and announcements into audited operational practice.

Over the longer term, the objective should be a multi-node digital-infrastructure system capable of supporting public-sector sovereignty, private-sector innovation, and regional hub functions. That means at least one operational hyperscale cloud region, deeper interconnection, geographically diversified resilience, stronger domestic cloud and security firms, and a legal governance framework trusted enough that firms choose Türkiye because they want to. That is the difference between a defensive localization policy and a successful digital-state strategy.

Ultimately, Türkiye should determine what kind of sovereignty it wants to buy, for which data, at what cost, under what safeguards, and to what strategic end. A narrow, risk-based, standards-driven localization governance offers the best answer. Everything else is either insufficiently sovereign or excessively restrictive.

SOURCES

- Al Thehaiban, Abdul Rahman, and Önder Güler. "A New Google Cloud Region Is Coming to Türkiye as Part of \$2 Billion Investment." Google Cloud Blog, November 20, 2025. <https://cloud.google.com/blog/products/infrastructure/new-google-cloud-region-coming-to-turkiye>.
- Amazon Web Services. "AWS Digital Sovereignty." Accessed May 18, 2026. <https://aws.amazon.com/compliance/digital-sovereignty/>.
- Arizton Advisory and Intelligence. "Turkey Data Center Market: Investment Analysis." Accessed May 21, 2026. <https://www.arizton.com/market-reports/turkey-data-center-market-investment-analysis>.
- Banking Regulation and Supervision Agency. "Regulation on Banks' Information Systems and Electronic Banking Services." March 2020. <https://www.bddk.org.tr/Mevzuat/DokumanGetir/1063>.
- Bauer, Matthias, Hosuk Lee-Makiyama, Erik van der Marel, and Bert Verschelde. "The Costs of Data Localisation: Friendly Fire on Economic Recovery." ECIPE Occasional Paper no. 3/2014. European Centre for International Political Economy, 2014. <https://ecipe.org/publications/dataloc/>.
- Bradford, Anu. *The Brussels Effect: How the European Union Rules the World*. Oxford University Press, 2020.
- Cloudflare. "What Is a CDN?" Cloudflare Learning Center. Accessed May 21, 2026. <https://www.cloudflare.com/learning/cdn/what-is-a-cdn/>.
- Court of Justice of the European Union. "The Court of Justice Invalidates Decision 2016/1250 on the Adequacy of the Protection Provided by the EU-US Data Protection Shield." Press release no. 91/20, July 16, 2020. <https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf>.
- Creemers, Rogier, and Graham Webster, trans. "Translation: Data Security Law of the People's Republic of China." DigiChina, Stanford University, June 29, 2021. <https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/>.
- Creemers, Rogier, and Graham Webster, trans. "Translation: Personal Information Protection Law of the People's Republic of China — Effective Nov. 1, 2021." DigiChina, Stanford University, November 1, 2021. <https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/>.

Cyberspace Administration of China. "Provisions on Promoting and Regulating the Cross-Border Flow of Data." Translated by China Law Translate, March 25, 2024.
<https://www.chinalawtranslate.com/en/Provisions-on-Promoting-and-Regulating-the-Cross--Border-Flow-of-Data/>.

Dağıstanlı, Hüseyin Cem. "e-Devlet Kapısı'na Kayıtlı Kullanıcı Sayısı 68 Milyonu Aştı." Anadolu Agency, February 1, 2026. <https://www.aa.com.tr/tr/gundem/e-devlet-kapisina-kayitli-kullanici-sayisi-68-milyonu-asti/3816815>.

Digital Agency of Japan. "Data Free Flow with Trust." Last updated October 16, 2024.
<https://www.digital.go.jp/en/policies/dfft>.

Disaster and Emergency Management Authority of Türkiye. "Türkiye Deprem Tehlike Haritası." Accessed May 21, 2026. <https://www.afad.gov.tr/turkiye-deprem-tehlike-haritasi>.

Equinix. "Equinix Opens New Data Center in Türkiye, Establishing Vital Interconnection Hub between Europe and Asia." October 31, 2024. <https://newsroom.equinix.com/2024-10-31-Equinix-Opens-New-Data-Center-in-Turkiye,-Establishing-Vital-Interconnection-Hub-between-Europe-and-Asia>.

European Commission. "Data Protection Adequacy for Non-EU Countries."
https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

European Commission. "Data Protection: European Commission Adopts New Adequacy Decision for Safe and Trusted EU-US Data Flows." July 10, 2023.
https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721.

European Commission. "EU-Brazil Data Adequacy Agreement." January 26, 2026.
https://ec.europa.eu/commission/presscorner/detail/en/ip_26_229.

European Commission. "Standard Contractual Clauses." June 4, 2021.
https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

European Data Protection Board. "Guidelines 02/2024 on Article 48 GDPR." Version 2.1, June 4, 2025.
https://www.edpb.europa.eu/system/files/2025-06/edpb_guidelines_202402_article48_v2_en.pdf.

Freedom House. "Freedom on the Net 2024: Russia." 2024.
<https://freedomhouse.org/country/russia/freedom-net/2024>.

Funk, Allie, and Jennifer Brody. "The Human Rights Costs of Data Localization Around the World." Tech Policy Press, March 26, 2024. <https://techpolicy.press/the-human-rights-costs-of-data-localization-around-the-world>.

Gartner. "Gartner Says Worldwide IaaS Public Cloud Services Market Grew 22.5 Percent in 2024." August 6, 2025. <https://www.gartner.com/en/newsroom/press-releases/2025-08-06-gartner-says-worldwide-iaas-public-cloud-services-market-grew-22-point-5-percent-in-2024>.

Google Cloud. "Sovereign Cloud." Accessed May 18, 2026. <https://cloud.google.com/sovereign-cloud>.

Government of India, Ministry of Electronics and Information Technology. "The Digital Personal Data Protection Act, 2023." August 11, 2023. <https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf>.

Infocomm Media Development Authority. "Trusted Data Sharing Framework." <https://www.imda.gov.sg/how-we-can-help/data-innovation/trusted-data-sharing-framework>.

Information and Communication Technologies Authority. "Electronic Communications Sector Quarterly Market Data Report: 2024 Q4." 2025.

International Energy Agency. "Data Centre Electricity Use Surged in 2025, Even with Tightening Bottlenecks Driving a Scramble for Solutions." April 16, 2026. <https://www.iea.org/news/data-centre-electricity-use-surged-in-2025-even-with-tightening-bottlenecks-driving-a-scramble-for-solutions>.

Investment Office of the Presidency of the Republic of Türkiye. "Khazna to Establish AI-Ready Facility in Ankara, Expanding Investment Footprint in Türkiye." May 3, 2025. <https://www.invest.gov.tr/en/news/news-from-turkey/pages/khazna-to-establish-ai-ready-facility-in-ankara-expanding-investment-footprint-in-turkiye.aspx>.

Investment Office of the Presidency of the Republic of Türkiye. "NGN Group Opens Data Center in Istanbul." July 4, 2019. <https://www.invest.gov.tr/en/news/news-from-turkey/pages/ngn-group-opens-data-center-in-istanbul.aspx>.

Investment Office of the Presidency of the Republic of Türkiye. "Trendyol and Castle Investments Partner on USD 500M Data Center in Ankara." June 2, 2025. <https://www.invest.gov.tr/en/news/news-from-turkey/pages/trendyol-and-castle-investments-partner-on-usd-500m-data-center-in-ankara.aspx>.

Investment Office of the Presidency of the Republic of Türkiye. "Turkcell and Google Cloud to Establish Türkiye's First Hyperscale Regional Data Center." November 24, 2025. <https://www.invest.gov.tr/en/news/news-from-turkey/pages/turkcell-and-google-cloud-to-establish-turkiyes-first-hyperscale-regional-data-center.aspx>.

Investment Office of the Presidency of the Republic of Türkiye. "Vodafone and DAMAC to Invest USD 100 Million in Data Center in Türkiye." February 22, 2024. <https://www.invest.gov.tr/en/news/news-from-turkey/pages/vodafone-and-damac-to-invest-usd-100-million-in-data-center-in-turkiye.aspx>.

JLL. "2026 Global Data Center Market Outlook." January 5, 2026. <https://www.jll.com/en-us/insights/market-outlook/data-center-outlook>.

- Mattoo, Aaditya, and Joshua P. Meltzer. "International Data Flows and Privacy: The Conflict and Its Resolution." Policy Research Working Paper no. 8431. World Bank, May 2018.
<https://documents.worldbank.org/en/publication/documents-reports/documentdetail/881561526852796804/international-data-flows-and-privacy-the-conflict-and-its-resolution>.
- Mell, Peter, and Timothy Grance. "The NIST Definition of Cloud Computing." National Institute of Standards and Technology, Special Publication 800-145, September 2011.
<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>.
- Microsoft. "Discover Microsoft Sovereign Cloud." Accessed May 18, 2026.
<https://www.microsoft.com/en-us/industry/sovereignty/cloud>.
- Ministry of Transport and Infrastructure of the Republic of Türkiye. "National Cyber Security Strategy and Action Plan 2024–2028." 2024. <https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/national-cyber-security-strategy-2024-2028.pdf>.
- National People's Congress of the People's Republic of China. "Data Security Law of the People's Republic of China." June 10, 2021.
- NGN. "Star of Bosphorus Data Center." Accessed May 21, 2026. <https://www.ngn.com.tr/en/star-of-bosphorus-data-center/>.
- OECD and World Trade Organization. Economic Implications of Data Regulation: Balancing Openness and Trust. Paris and Geneva: OECD Publishing and World Trade Organization, 2025.
https://www.oecd.org/en/publications/economic-implications-of-data-regulation_aa285504-en.html;
https://www.wto.org/english/res_e/booksp_e/data_regulation_e.pdf.
- Office of the United States Trade Representative. "Key Barriers to Digital Trade." March 2017.
<https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2017/march/key-barriers-digital-trade>.
- Panday, Jyoti, and Jeremy Malcolm. "The Political Economy of Data Localization." *Partecipazione e Conflitto* 11, no. 2 (2018): 511–27.
- Personal Data Protection Authority of Türkiye. "Kişisel Verilerin Yurt Dışına Aktarılması Rehberi." 2024.
<https://www.kvkk.gov.tr/Icerik/8142/Kisisel-Verilerin-Yurt-Disina-Aktarilmasi-Rehberi>.
- Personal Data Protection Authority of Türkiye. "Personal Data Protection Law." Published January 6, 2020. <https://www.kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law>.
- Personal Data Protection Authority of Türkiye. "Yurt Dışına Aktarım." Accessed May 21, 2026.
<https://www.kvkk.gov.tr/Icerik/2053/Yurtdisina-Aktarim>.
- Reserve Bank of India. "Storage of Payment System Data." June 26, 2019.
<https://www.rbi.org.in/commonman/english/scripts/FAQs.aspx?Id=2995>.

- Republic of Türkiye. "Cybersecurity Law." Law No. 7545. Official Gazette no. 32846, March 19, 2025.
- Rose, Scott, Oliver Borchert, Stu Mitchell, and Sean Connolly. "Zero Trust Architecture." National Institute of Standards and Technology, Special Publication 800-207, August 2020.
<https://csrc.nist.gov/pubs/sp/800/207/final>.
- Sheppard, Lindsey R., Erol Yayboke, and Carolina G. Ramos. "The Real National Security Concerns over Data Localization." Center for Strategic and International Studies, July 23, 2021.
<https://www.csis.org/analysis/real-national-security-concerns-over-data-localization>.
- Turkish State Meteorological Service. "Resmi İklim İstatistikleri: Erzurum." Accessed May 21, 2026.
<https://www.mgm.gov.tr/veridegerlendirme/il-ve-ilceler-istatistik.aspx?k=H&m=ERZURUM>.
- Turkcell İletişim Hizmetleri A.Ş. "2024 Annual Report." Form 20-F, April 29, 2025.
<https://s.turkcell.com.tr/SiteAssets/Hakkimizda/yatirimci-iliskileri/documents/pdf/20F2024.pdf>.
- Türk Telekom. "Energy Management and Environmental Investments." Accessed May 21, 2026.
<https://www.ttyatirimciiliskileri.com.tr/en-us/socially-responsible-investing/pages/energy-management-and-environmental-investments>.
- Uptime Institute. "Uptime Institute Global Data Center Survey Results 2025." July 2025.
<https://uptimeinstitute.com/resources/research-and-reports/uptime-institute-global-data-center-survey-results-2025>.
- U.S. Department of Justice. "Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern." Federal Register 90, no. 5, January 8, 2025.
<https://www.federalregister.gov/documents/2025/01/08/2024-31486/preventing-access-to-us-sensitive-personal-data-and-government-related-data-by-countries-of-concern>.
- U.S. Department of Justice. "The Purpose and Impact of the CLOUD Act." April 2019.
<https://www.justice.gov/criminal/media/999601/dl?inline=>.

ENDNOTES

1. OECD and World Trade Organization, Economic Implications of Data Regulation: Balancing Openness and Trust (Paris and Geneva: OECD Publishing and World Trade Organization, 2025), https://www.oecd.org/en/publications/economic-implications-of-data-regulation_aa285504-en.html; Matthias Bauer, Hosuk Lee-Makiyama, Erik van der Marel, and Bert Verschelde, "The Costs of Data Localisation: Friendly Fire on Economic Recovery," ECIPE Occasional Paper no. 3/2014, European Centre for International Political Economy, 2014, <https://ecipe.org/publications/dataloc/> ↩

2. Lindsey R. Sheppard, Erol Yayboke, and Carolina G. Ramos, "The Real National Security Concerns over Data Localization," Center for Strategic and International Studies, July 23, 2021, <https://www.csis.org/analysis/real-national-security-concerns-over-data-localization> ↩
3. Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, Special Publication 800-145, September 2011, <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>. ↩
4. Jyoti Panday and Jeremy Malcolm, "The Political Economy of Data Localization," Partecipazione e Conflitto 11, no. 2 (2018): 511–27; Aaditya Mattoo and Joshua P. Meltzer, "International Data Flows and Privacy: The Conflict and Its Resolution," Policy Research Working Paper no. 8431, World Bank, May 2018, <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/881561526852796804/international-data-flows-and-privacy-the-conflict-and-its-resolution> ↩
5. Cloudflare, "What Is a CDN?," Cloudflare Learning Center, accessed May 21, 2026, <https://www.cloudflare.com/learning/cdn/what-is-a-cdn/>; Scott Rose, Oliver Borchert, Stu Mitchell, and Sean Connelly, "Zero Trust Architecture," National Institute of Standards and Technology, Special Publication 800-207, August 2020, <https://csrc.nist.gov/pubs/sp/800/207/final> ↩
6. Amazon Web Services, "AWS Digital Sovereignty," accessed May 18, 2026, <https://aws.amazon.com/compliance/digital-sovereignty/>; Microsoft, "Discover Microsoft Sovereign Cloud," accessed May 18, 2026, <https://www.microsoft.com/en-us/industry/sovereignty/cloud>; Google Cloud, "Sovereign Cloud," accessed May 18, 2026, <https://cloud.google.com/sovereign-cloud> ↩
7. Gartner, "Gartner Says Worldwide IaaS Public Cloud Services Market Grew 22.5 Percent in 2024," August 6, 2025, <https://www.gartner.com/en/newsroom/press-releases/2025-08-06-gartner-says-worldwide-iaas-public-cloud-services-market-grew-22-point-5-percent-in-2024>; Equinix, "Equinix Opens New Data Center in Türkiye, Establishing Vital Interconnection Hub between Europe and Asia," October 31, 2024, <https://newsroom.equinix.com/2024-10-31-Equinix-Opens-New-Data-Center-in-Turkiye,-Establishing-Vital-Interconnection-Hub-between-Europe-and-Asia> ↩
8. Office of the United States Trade Representative, "Key Barriers to Digital Trade," March 2017, <https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2017/march/key-barriers-digital-trade>; U.S. Department of Justice, "Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern," Federal Register 90, no. 5, January 8, 2025, <https://www.federalregister.gov/documents/2025/01/08/2024-31486/preventing-access-to-us-sensitive-personal-data-and-government-related-data-by-countries-of-concern> ↩
9. European Commission, "Standard Contractual Clauses," June 4, 2021, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en; Court of Justice of the European Union, "The Court

of Justice Invalidates Decision 2016/1250 on the Adequacy of the Protection Provided by the EU-US Data Protection Shield," press release no. 91/20, July 16, 2020, <https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf> ↪

10. Gartner, "Gartner Says Worldwide IaaS Public Cloud Services Market Grew 22.5 Percent in 2024"; Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press, 2020). ↪
11. Rogier Creemers and Graham Webster, trans., "Translation: Personal Information Protection Law of the People's Republic of China — Effective Nov. 1, 2021," DigiChina, Stanford University, November 1, 2021, <https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/>; Rogier Creemers and Graham Webster, trans., "Translation: Data Security Law of the People's Republic of China," DigiChina, Stanford University, June 29, 2021, <https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/> ↪
12. Government of India, Ministry of Electronics and Information Technology, "The Digital Personal Data Protection Act, 2023," August 11, 2023, <https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf>; Reserve Bank of India, "Storage of Payment System Data," June 26, 2019, <https://www.rbi.org.in/commonman/english/scripts/FAQs.aspx?Id=2995> ↪
13. Allie Funk and Jennifer Brody, "The Human Rights Costs of Data Localization Around the World," Tech Policy Press, March 26, 2024, <https://techpolicy.press/the-human-rights-costs-of-data-localization-around-the-world>; Freedom House, "Freedom on the Net 2024: Russia," 2024, <https://freedomhouse.org/country/russia/freedom-net/2024> ↪
14. Digital Agency of Japan, "Data Free Flow with Trust," last updated October 16, 2024, <https://www.digital.go.jp/en/policies/dfft>; Infocomm Media Development Authority, "Trusted Data Sharing Framework," <https://www.imda.gov.sg/how-we-can-help/data-innovation/trusted-data-sharing-framework> ↪
15. European Commission, "EU-Brazil Data Adequacy Agreement," January 26, 2026, https://ec.europa.eu/commission/presscorner/detail/en/ip_26_229 ↪
16. Anadolu Agency, "e-Devlet Kapısı'na Kayıtlı Kullanıcı Sayısı 68 Milyonu Aştı," February 1, 2026, <https://www.aa.com.tr/tr/gundem/e-devlet-kapisina-kayitli-kullanici-sayisi-68-milyonu-asti/3816815>; Information and Communication Technologies Authority, "Electronic Communications Sector Quarterly Market Data Report: 2024 Q4," 2025; Investment Office of the Presidency of the Republic of Türkiye, "Turkcell and Google Cloud to Establish Türkiye's First Hyperscale Regional Data Center," November 24, 2025, <https://www.invest.gov.tr/en/news/news-from-turkey/pages/turkcell-and-google-cloud-to-establish-turkiyes-first-hyperscale-regional-data-center.aspx> ↪

17. European Commission, "Data Protection Adequacy for Non-EU Countries," https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en; European Commission, "Standard Contractual Clauses," June 4, 2021, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en ↩
18. Court of Justice of the European Union, "The Court of Justice Invalidates Decision 2016/1250 on the Adequacy of the Protection Provided by the EU-US Data Protection Shield," press release no. 91/20, July 16, 2020, <https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf> ↩
19. European Commission, "Data Protection: European Commission Adopts New Adequacy Decision for Safe and Trusted EU-US Data Flows," July 10, 2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721; European Data Protection Board, "Guidelines 02/2024 on Article 48 GDPR," version 2.1, June 4, 2025, https://www.edpb.europa.eu/system/files/2025-06/edpb_guidelines_202402_article48_v2_en.pdf ↩
20. Gartner, "Gartner Says Worldwide IaaS Public Cloud Services Market Grew 22.5 Percent in 2024"; U.S. Department of Justice, "The Purpose and Impact of the CLOUD Act," April 2019, <https://www.justice.gov/criminal/media/999601/dl?inline=> ↩
21. U.S. Department of Justice, "The Purpose and Impact of the CLOUD Act," April 2019, <https://www.justice.gov/criminal/media/999601/dl?inline=> ↩
22. U.S. Department of Justice, "Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern," Federal Register 90, no. 5, January 8, 2025, <https://www.federalregister.gov/documents/2025/01/08/2024-31486/preventing-access-to-us-sensitive-personal-data-and-government-related-data-by-countries-of-concern> ↩
23. Rogier Creemers and Graham Webster, trans., "Translation: Personal Information Protection Law of the People's Republic of China — Effective Nov. 1, 2021," DigiChina, Stanford University, November 1, 2021, <https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/> ↩
24. Creemers and Webster, trans., "Translation: Data Security Law of the People's Republic of China"; National People's Congress of the People's Republic of China, "Data Security Law of the People's Republic of China," June 10, 2021 ↩
25. Cyberspace Administration of China, "Provisions on Promoting and Regulating the Cross-Border Flow of Data," translated by China Law Translate, March 25, 2024, <https://www.chinalawtranslate.com/en/Provisions-on-Promoting-and-Regulating-the-Cross--Border-Flow-of-Data/> ↩

26. Government of India, Ministry of Electronics and Information Technology, "The Digital Personal Data Protection Act, 2023"; Reserve Bank of India, "Storage of Payment System Data." ↩
27. Digital Agency of Japan, "Data Free Flow with Trust"; Infocomm Media Development Authority, "Trusted Data Sharing Framework." ↩
28. European Commission, "EU-Brazil Data Adequacy Agreement." ↩
29. Personal Data Protection Authority of Türkiye, "Personal Data Protection Law," published January 6, 2020, <https://www.kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law> ↩
30. Personal Data Protection Authority of Türkiye, "Kişisel Verilerin Yurt Dışına Aktarılması Rehberi," 2024, <https://www.kvkk.gov.tr/Icerik/8142/Kisisel-Verilerin-Yurt-Disina-Aktarilmasi-Rehberi>; Personal Data Protection Authority of Türkiye, "Yurt Dışına Aktarım," accessed May 21, 2026, <https://www.kvkk.gov.tr/Icerik/2053/Yurtdisina-Aktarim> ↩
31. Personal Data Protection Authority of Türkiye, "Personal Data Protection Law"; Banking Regulation and Supervision Agency, "Regulation on Banks' Information Systems and Electronic Banking Services," March 2020, <https://www.bddk.org.tr/Mevzuat/DokumanGetir/1063>; Ministry of Transport and Infrastructure of the Republic of Türkiye, "National Cyber Security Strategy and Action Plan 2024–2028," 2024, <https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/national-cyber-security-strategy-2024-2028.pdf> ↩
32. Banking Regulation and Supervision Agency, "Regulation on Banks' Information Systems and Electronic Banking Services," March 2020, <https://www.bddk.org.tr/Mevzuat/DokumanGetir/1063> ↩
33. Ministry of Transport and Infrastructure of the Republic of Türkiye, "National Cyber Security Strategy and Action Plan 2024–2028"; Republic of Türkiye, "Cybersecurity Law," Law No. 7545, Official Gazette no. 32846, March 19, 2025. ↩
34. Hüseyin Cem Dağıstanlı, "e-Devlet Kapısı'na Kayıtlı Kullanıcı Sayısı 68 Milyonu Aştı," Anadolu Agency, February 1, 2026, <https://www.aa.com.tr/tr/gundem/e-devlet-kapisina-kayitli-kullanici-sayisi-68-milyonu-asti/3816815> ↩
35. Personal Data Protection Authority of Türkiye, "Kişisel Verilerin Yurt Dışına Aktarılması Rehberi"; Ministry of Transport and Infrastructure of the Republic of Türkiye, "National Cyber Security Strategy and Action Plan 2024–2028"; Republic of Türkiye, "Cybersecurity Law," Law No. 7545. ↩
36. Turkcell İletişim Hizmetleri A.Ş., "2024 Annual Report," Form 20-F, April 29, 2025, <https://s.turkcell.com.tr/SiteAssets/Hakkimizda/yatirimci-iliskileri/documents/pdf/20F2024.pdf> ↩
37. Türk Telekom, "Energy Management and Environmental Investments," accessed May 21, 2026, <https://www.ttyatirimciiliskileri.com.tr/en-us/socially-responsible-investing/pages/energy-management-and-environmental-investments> ↩

38. Equinix, "Equinix Opens New Data Center in Türkiye, Establishing Vital Interconnection Hub between Europe and Asia," October 31, 2024, <https://newsroom.equinix.com/2024-10-31-Equinix-Opens-New-Data-Center-in-Turkiye,-Establishing-Vital-Interconnection-Hub-between-Europe-and-Asia> ↩
39. Investment Office of the Presidency of the Republic of Türkiye, "Khazna to Establish AI-Ready Facility in Ankara, Expanding Investment Footprint in Türkiye," May 3, 2025, <https://www.invest.gov.tr/en/news/news-from-turkey/pages/khazna-to-establish-ai-ready-facility-in-ankara-expanding-investment-footprint-in-turkiye.aspx> ↩
40. Investment Office of the Presidency of the Republic of Türkiye, "Trendyol and Castle Investments Partner on USD 500M Data Center in Ankara," June 2, 2025, <https://www.invest.gov.tr/en/news/news-from-turkey/pages/trendyol-and-castle-investments-partner-on-usd-500m-data-center-in-ankara.aspx> ↩
41. NGN, "Star of Bosphorus Data Center," accessed May 21, 2026, <https://www.ngn.com.tr/en/star-of-bosphorus-data-center/>; Investment Office of the Presidency of the Republic of Türkiye, "NGN Group Opens Data Center in Istanbul," July 4, 2019, <https://www.invest.gov.tr/en/news/news-from-turkey/pages/ngn-group-opens-data-center-in-istanbul.aspx>. ↩
42. Investment Office of the Presidency of the Republic of Türkiye, "Turkcell and Google Cloud to Establish Türkiye's First Hyperscale Regional Data Center," November 24, 2025, <https://www.invest.gov.tr/en/news/news-from-turkey/pages/turkcell-and-google-cloud-to-establish-turkiyes-first-hyperscale-regional-data-center.aspx> ↩
43. Information and Communication Technologies Authority, "Electronic Communications Sector Quarterly Market Data Report: 2024 Q4," 2025; Turkcell İletişim Hizmetleri A.Ş., "2024 Annual Report," Form 20-F, April 29, 2025, <https://s.turkcell.com.tr/SiteAssets/Hakkimizda/yatirimci-iliskileri/documents/pdf/20F2024.pdf> ↩
44. Disaster and Emergency Management Authority of Türkiye, "Türkiye Deprem Tehlike Haritası," accessed May 21, 2026, <https://www.afad.gov.tr/turkiye-deprem-tehlike-haritasi> ↩
45. Investment Office of the Presidency of the Republic of Türkiye, "Vodafone and DAMAC to Invest USD 100 Million in Data Center in Türkiye," February 22, 2024, <https://www.invest.gov.tr/en/news/news-from-turkey/pages/vodafone-and-damac-to-invest-usd-100-million-in-data-center-in-turkiye.aspx> ↩
46. Turkish State Meteorological Service, "Resmi İklim İstatistikleri: Erzurum," accessed May 21, 2026, <https://www.mgm.gov.tr/veridegerlendirme/il-ve-ilceler-istatistik.aspx?k=H&m=ERZURUM> ↩
47. JLL, "2026 Global Data Center Market Outlook," January 5, 2026, <https://www.jll.com/en-us/insights/market-outlook/data-center-outlook> ↩

48. Arizton Advisory and Intelligence, "Turkey Data Center Market: Investment Analysis," accessed May 21, 2026, <https://www.arizton.com/market-reports/turkey-data-center-market-investment-analysis> ↩
49. International Energy Agency, "Data Centre Electricity Use Surged in 2025, Even with Tightening Bottlenecks Driving a Scramble for Solutions," April 16, 2026, <https://www.iea.org/news/data-centre-electricity-use-surged-in-2025-even-with-tightening-bottlenecks-driving-a-scramble-for-solutions>; Uptime Institute, "Uptime Institute Global Data Center Survey Results 2025," July 2025, <https://uptimeinstitute.com/resources/research-and-reports/uptime-institute-global-data-center-survey-results-2025> ↩
50. Personal Data Protection Authority of Türkiye, "Kişisel Verilerin Yurt Dışına Aktarılması Rehberi"; Personal Data Protection Authority of Türkiye, "Yurt Dışına Aktarım." ↩
51. OECD and World Trade Organization, Economic Implications of Data Regulation: Balancing Openness and Trust (Paris and Geneva: OECD Publishing and World Trade Organization, 2025), https://www.oecd.org/en/publications/economic-implications-of-data-regulation_aa285504-en.html ↩
52. OECD and World Trade Organization, Economic Implications of Data Regulation, https://www.wto.org/english/res_e/booksp_e/data_regulation_e.pdf ↩
53. Lindsey R. Sheppard, Erol Yayboke, and Carolina G. Ramos, "The Real National Security Concerns over Data Localization," Center for Strategic and International Studies, July 23, 2021, <https://www.csis.org/analysis/real-national-security-concerns-over-data-localization>; Allie Funk and Jennifer Brody, "The Human Rights Costs of Data Localization Around the World," Tech Policy Press, March 26, 2024, <https://techpolicy.press/the-human-rights-costs-of-data-localization-around-the-world> ↩
54. Abdul Rahman Al Thehaiban and Önder Güler, "A New Google Cloud Region Is Coming to Türkiye as Part of \$2 Billion Investment," Google Cloud Blog, November 20, 2025, <https://cloud.google.com/blog/products/infrastructure/new-google-cloud-region-coming-to-turkiye>; Investment Office of the Presidency of the Republic of Türkiye, "Turkcell and Google Cloud to Establish Türkiye's First Hyperscale Regional Data Center," November 24, 2025, <https://www.invest.gov.tr/en/news/news-from-turkey/pages/turkcell-and-google-cloud-to-establish-turkiyes-first-hyperscale-regional-data-center.aspx>; Turkcell İletişim Hizmetleri A.Ş., "2024 Annual Report." ↩

AUTHORS

Ulaş Akkaya

RESEARCHER / ANALYST

Ulaş Akkaya graduated in 2025 at the top of his department with high honors from the Department of International Relations at Kadir Has University and studied as an exchange student at Sciences Po Lille.

During his undergraduate studies, he served as the principal investigator for the TÜBİTAK 2209-A project titled “A Roadmap for Turkey in Space Diplomacy” and as a researcher for the two-year TÜBİTAK 1001 project on “The Role of Sports in Turkey’s Foreign Relations.” He is the Founder and Director of the International Relations Youth Platform, where he has directed the Foreign Policy and Youth Summit and the Youth and Security Summit, bringing together young professionals in diplomacy and international affairs.

Akkaya also gained professional experience through voluntary internships at the Istanbul Metropolitan Municipality Department of Foreign Relations, Global Academy, Kadir Has University Center for International and European Studies (CIES), and the IKV EU Information Centre. He is a fellow of the Konrad-Adenauer-Stiftung & EDAM Political Leadership Excellence Program (PLEP 2025). His research interests include foreign policy analysis and the intersection of emerging technologies and international security.

Sinan Ülgen

DIRECTOR

Sinan Ülgen graduated in 1987 from the University of Virginia with a double major in computer sciences and economics. He undertook graduate studies at the College of Europe in Bruges, Belgium where he received, in 1990, a master's degree in European economic integration. He then joined the Turkish Foreign Service as a career diplomat. In 1992, he was posted to the Turkish Permanent Delegation to the European Union in Brussels where he became part of the team that negotiated the Turkey-EU customs union.

Ülgen is the founder and managing partner of Istanbul Economics. The consultancy specializes in market entry strategies for international companies, political and economic risk analysis related to Turkey and regulatory affairs.

Ülgen is also the director of the Istanbul based think tank, Center for Economics and Foreign Policy Studies (EDAM) and a visiting scholar at Carnegie Europe in Brussels. His research and opinion pieces have been published by the Carnegie Endowment for International Peace, Center for European Policy Studies, Center for European Reform, the Atlantic Council, German Marshall Fund, Brookings and the World Economic Forum as well as newspapers such as Le Figaro, Financial Times, Wall Street Journal, European Voice, Project Syndicate and the International New York Times. He is also the co-author of a book on Turkey-EU relations with Kemal Derviş and a frequent commentator on Turkish affairs in the international press. Ülgen served on the academic advisory board of the NATO Defence College in Rome. He was a member of the Europe Council of the World Economic Forum. He was also a member of the international policy experts group set up by the NATO Secretary General Rasmussen.

edam Centre for Economics and Foreign Policy Studies



Cloud Strategy and Data Localization — Türkiye's Policy Options

Centre for Economics and Foreign Policy Studies
Hare Sok. No:16, Akatlar · İstanbul / TÜRKİYE

+90 (212) 823 66 47 · info@edam.org.tr · edam.org.tr