

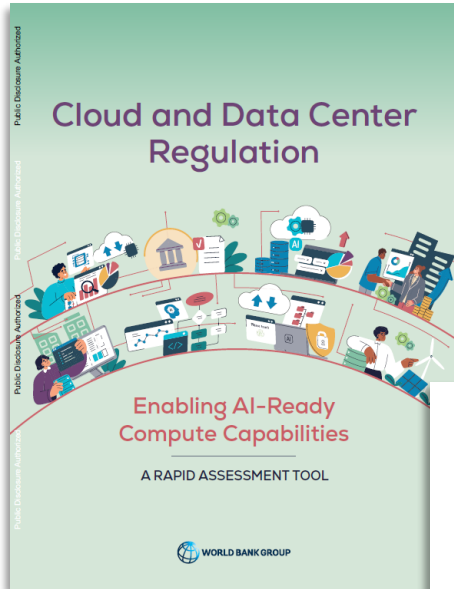
Cloud and Data Center Regulation: Enabling AI-Ready Compute Capabilities

22 July 2026

Slavina Pancheva, Digital Specialist, World Bank



New World Bank Report on Cloud and Data Center Regulation



An **analysis of core laws and regulations** to spur growth of cloud and data center markets, while promoting resilience and sustainability.

Rapid Assessment Tool allows countries to quickly assess their legal framework for cloud and data centers.

TABLE 1. Cloud and Data Center Regulation Rapid Assessment Tool

Subject Area	Core Criteria	Advanced Criteria
Demand: Promoting Government Cloud Adoption		
National digital strategy	☐ National digital strategy formally adopted <i>If yes:</i> ☐ Promotes cloud adoption by government	☐ National digital strategy promotes adoption of commercial cloud by government ☐ Promotes development of domestic cloud and data center markets ☐ Incorporates environmental sustainability targets for data infrastructure
Government cloud policy	☐ Whole-of-government government cloud policy formally adopted <i>If yes:</i> ☐ Adopts cloud-first principles ☐ Adopts risk-based approach to data governance and cybersecurity	Cloud policy: ☐ Promotes adoption of different types of cloud services in a hybrid cloud architecture ☐ Incorporates environmental sustainability targets
Data classification policy for public sector data <i>(Standalone or part of a data governance framework or cloud policy)</i>	☐ Data classification policy for public sector data formally adopted <i>If yes:</i> ☐ Public sector entities are mandated to classify data as per data classification policy	☐ Data classification policy is supported by a comprehensive security controls framework with minimum requirements for each category of data

- 1. Demand: Promoting Government Cloud Adoption**
Regulations to promote cloud adoption, specifically by increasing addressable demand, with a particular focus on demand from the public sector.
- 2. Supply: Attracting Private Capital**
Policies that create incentives for private investment in local and regional data center markets, that is, increasing supply and attracting private capital.
- 3. Ensuring Privacy, Security, and Sustainability**
Policy frameworks ensuring that cloud services and the underlying data centers provide adequate data privacy, cybersecurity, regulatory compliance, and operational and environmental sustainability.



Laws, policies and regulations: demand

1. Demand: Promoting Government Cloud Adoption. Regulations to promote cloud adoption, specifically by increasing addressable demand, with a particular focus on demand from the public sector.

 **1.1 National digital strategy** promotes cloud adoption and data center market development

 **1.2 Government cloud policy** with a risk-based approach is adopted and enforced

 **1.3 Data classification** framework mandated for use across government, linked to cloud policy and security controls frameworks

 **1.4 Procurement rules** optimized for cloud adoption (e.g., Opex spending, cloud marketplaces)

 **1.5 Standards, labels and certifications** used to evaluate cloud vendors and ensure compliance

 **1.6 Clear institutional framework** for government cloud adoption (mandates, roles, responsibilities, enforcement)

- Grow demand
- Aggregate demand nationally (e.g., within government)



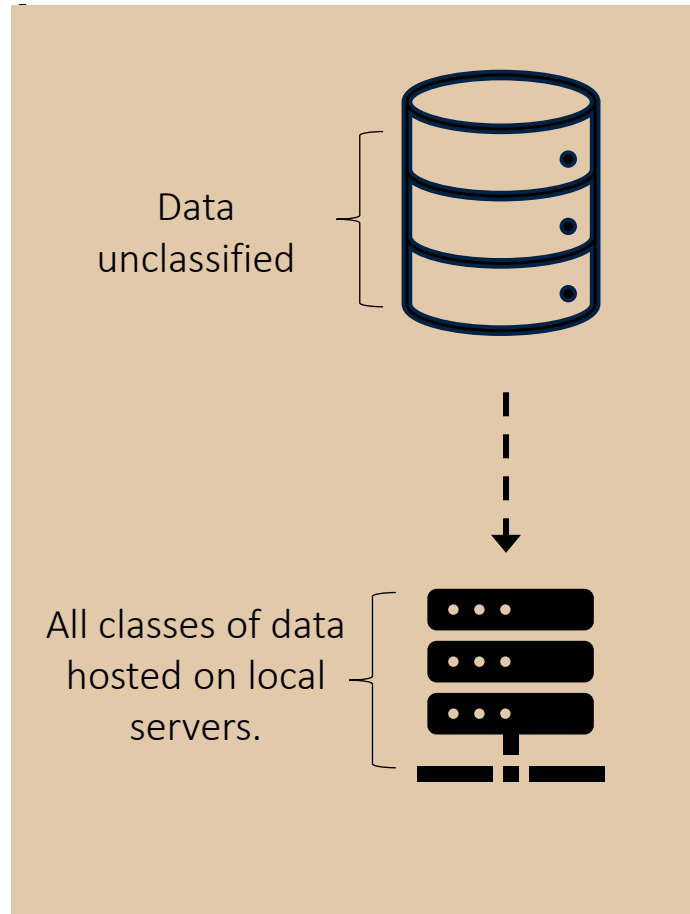
Cloud adoption to foster digital economy growth

1.3 Data Classification: Different Data for Different Hosting Needs

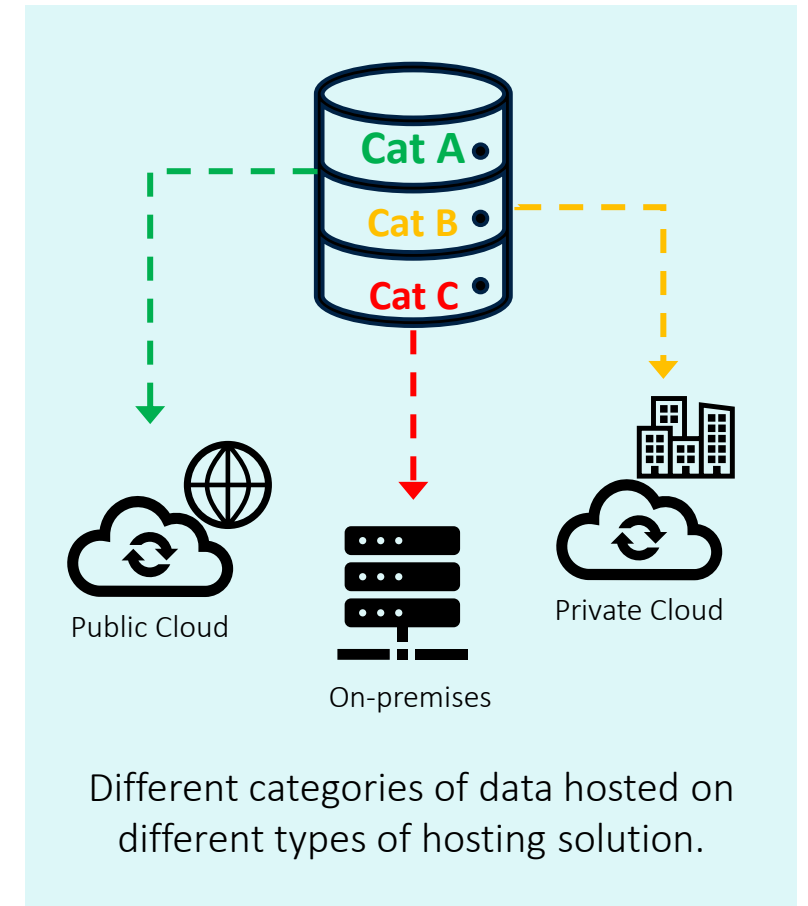
Implementing Data Classification

- ✓ Data to be classified according to key **requirements**, e.g., confidentiality, availability, and integrity.
- ✓ **UK Data Classification Framework:**
 - ✓ From 6 to 3 tiers
 - ✓ 90% of data “official” (lowest tier), can be stored freely in public cloud

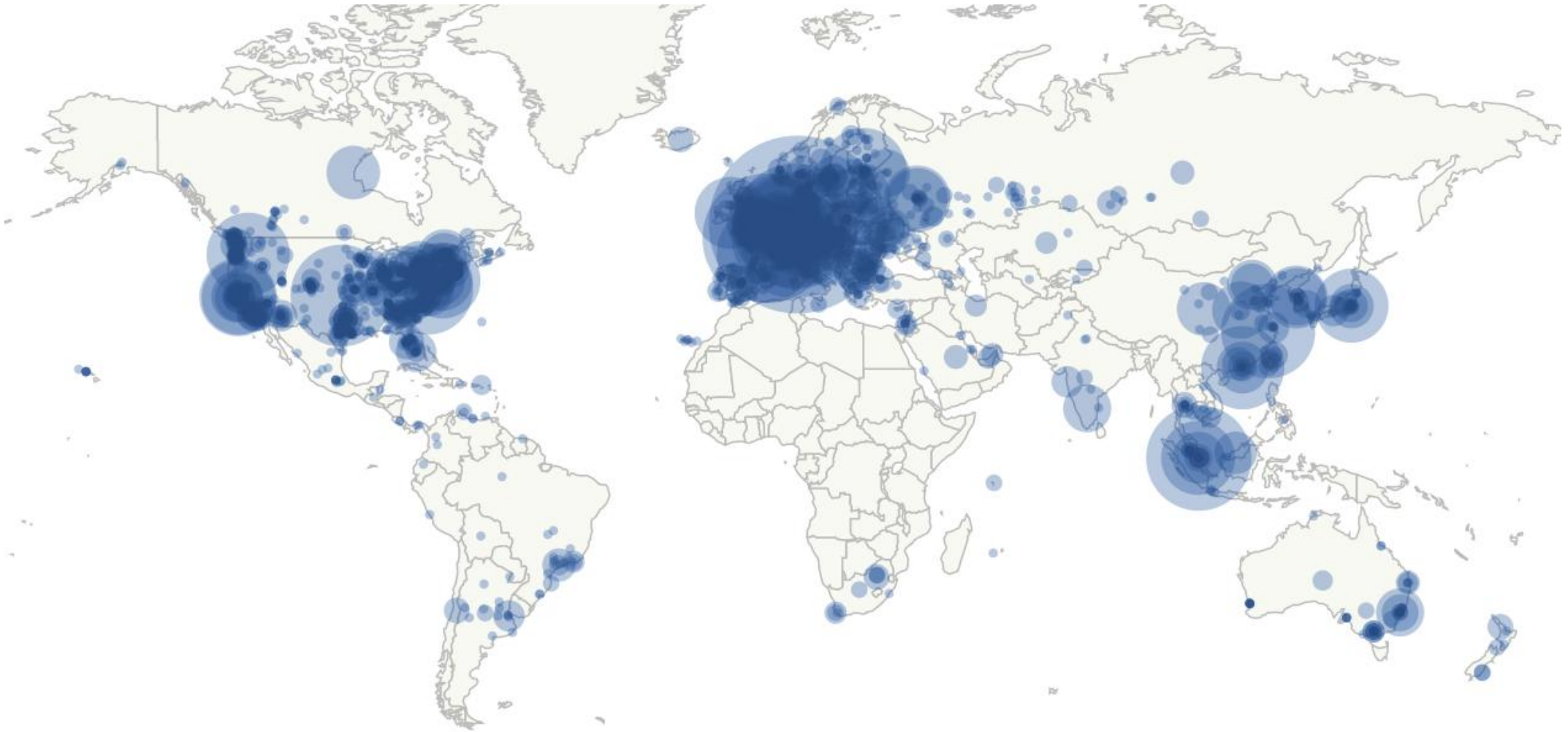
Low-maturity contexts



High-maturity contexts



Supply: uneven distribution of data infrastructure



Laws, policies and regulations: supply

2. Supply: Attracting Private Capital. Policies that create incentives for private investment in local and regional data center markets, that is, increasing supply and attracting private capital.



2.1 Appropriate **online intermediary protection** and no general obligation to monitor content (especially for infrastructure intermediaries, like CSPs or data center operators)



2.2 **Licensing and permit requirements** are clear, proportionate, without undue discretion and necessary to achieve objectives



2.3 **Competition and business climate** rules are predictable and non-discriminatory (e.g., score on World Bank Business Ready Index)



2.4 **Tax policy** is clear and does not impede foreign direct investment



2.5 **National PPP framework** promotes data center and cloud partnerships

- Create incentives to attract data center investments nationally (or regionally)



Grow supply of cloud and data center services (nationally or regionally)

2.5 PPPs for data centers



Government data hosting: Within a risk-based approach, DC PPPs could be used for hosting more sensitive data that doesn't flow to the public cloud (e.g., sensitive or top-secret data) within a hybrid or private cloud configuration.



Benefits for the government: use of private sector expertise, access to private sector financing, decreased CapEx requirements, optimal task and risk allocation, public sector demand alone might be insufficient for large capacity data center



Benefits for private sector: offset demand risk through government demand anchor (e.g. offtake agreement), may enable market entry in otherwise unattractive market



Challenges: risks of vendor lock-in, technological obsolescence, high up-front costs. Requires careful selection of PPP model and may require cloud-specific PPP guidance.



Examples: Crown Hosting Data Centers (UK), US GovCloud, EU AI Gigafactory Initiative, Armenia Firebird project

Laws, policies and regulations: privacy, security and sustainability

3. Ensuring Privacy, Security, and Sustainability. Policy frameworks ensuring that cloud services and the underlying data centers provide adequate data privacy, cybersecurity, regulatory compliance, and operational and environmental sustainability.

Cross-border interoperability



3.1 Personal data protection law clearly defines obligations, and a data protection authority enforces these



3.2 Data localization rules are minimal to what is necessary to achieve legitimate objectives (e.g., apply only to certain well-defined classes of data, such as top secret data; least restrictive requirements)



3.3 Cybersecurity law exists and places clear obligations on cloud service providers



3.4 Government policy addresses environmental sustainability of cloud and data centers (e.g., Cloud Policy specifies efficiency standards to be met by solutions used by the public sector)

- Cross-cutting enablers and safeguards

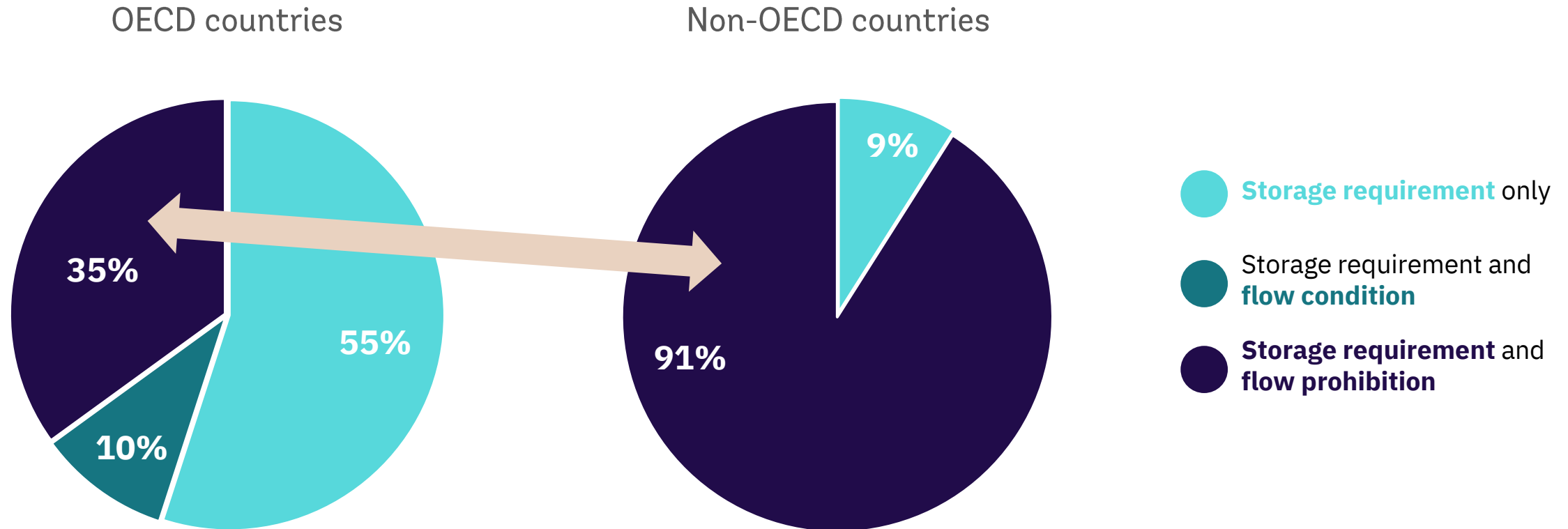


Ensure responsible use of cloud and data center solutions

Safeguard sensitive data and build trust

Promote both demand and supply of cloud and data center services

3.2 Lower income countries are imposing the strictest localization requirements



Gains for low-income countries would be around 1% of GDP following removal of data localization measures.

Key Takeaways

- **Laws and regulations** are a **key enabler** of cloud adoption and data center market growth.
- On the **demand side**, a favorable legal environment helps to **grow and aggregate demand** and facilitates **cloud adoption** to support digital transformation across the economy.
- On the **supply side**, a favorable legal environment helps to **attract cloud and data center investments** to serve local and regional markets.
- Legal framework puts in place **vital safeguards** that guarantee **privacy, security and sustainability**, that build trust and boost both demand and supply.

Thank you!