AMERICAN CHAMBER OF COMMERCE IN KAZAKHSTAN

15 May 2026

AMCHAM ISSUE BRIEF

DATA LOCALIZATION REQUIREMENTS AND PROPOSED AMENDMENTS

SUMMARY

This issue brief reflects a consensus among AmCham members including Google, Meta, Microsoft, Apple, Ericsson, Oracle, Cisco and more. Our companies want to help the country achieve its goals to become a regional digital hub, increase AI adoption and spur widespread digitalization, while supporting digital sovereignty and cybersecurity.

The Digitalization Committee of AmCham works on identifying barriers to achieving this goal. A persistent issue has been unclear governance of personal data collection and processing, comprised of:

1. A lack of distinction between:
    a. Sensitive data that must be stored in Kazakhstan;
    b. Data that can be stored and processed abroad, and
    c. Data where hybrid cloud or parallel storage is permissible,
2. Gaps in global security standards, certifications, and government, quasi-government and critical digital infrastructure contracts and
3. Expanding domestication and data registry requirements for global digital platforms.

Resolving these issues can unlock the potential for partnership with AmCham members Google, Meta, Microsoft, Apple, Ericsson, Oracle, Cisco and others to help Kazakhstan achieve its vision.

The draft decree *On Comprehensive Measures for the Development of the Data Processing and Storage Infrastructure and Ecosystem* addresses many of our concerns by:

1. Lifting requirements for mandatory storage of digital databases in Kazakhstan and allowing cross-border data transfer for most categories of personal data;
2. Adopting the Cloud First principle for government data processing, including conditionally including public cloud and private sector solutions; and
3. Simplifying security, compliance and operations requirements for the Data Centers Valley project participants.

CURRENT REGULATORY FRAMEWORK

Personal data collection and processing governance in the Republic of Kazakhstan is defined by a complex ecosystem of overlapping regulations.

The data localization clause in the foundational **Law on Personal Data** (№ 94-V, 21 May 2013) states that data storage shall take place on the territory of the Republic (Article 12). The localization clause has survived multiple revisions and has, at times, been further strengthened by the relevant Ministry's regulations, such as the Order № 395, 21 October 2020, "On rules of collecting and processing personal data" and its subsequent amendments. Moreover, the Law № 255-VIII ("On Amendments and Additions to Certain Legislative Acts of the Republic of Kazakhstan on Digitalization, Transport and Entrepreneurship"), signed on 09 January 2026, significantly broadened the definition of personal data to "*information, or a set of information, relating to a personal data subject and supplemented by one or more personal data identifiers*".

The **Law on Informatization** (№ 418-V, 24 November 2015) has further entrenched data localization requirements for state, quasi-state and a broad range of '*critically important objects of information and telecommunications infrastructure*'. Even though the recent amendments (№ 256-VIII, 09 January 2026) repeal Article 36 "Electronic information resources containing personal information", they also reimpose Personal Data Law requirements, including data localization provisions, on an even wider range of 'digital objects', including digital records, systems, platforms, software and products. Similarly to the Personal Data Law, the Informatization Law neither delineates types of data when such storage is required (for instance, sensitive data or data processed by critical infrastructure or services operators), nor includes provision for parallel storage, data synchronization, identification of primary vs. secondary databases etc.

The significant additions to the regulatory landscape in the last 12 months - namely, the **Digital Code** (№ 255-VIII, 09 January 2026) and the **Law on Artificial Intelligence** (#№ 230-VIII, 17 November 2025) - contain provisions further strengthening the localization approach. The Digital Code explicitly requires the owners of 'digital resources' (Article 24), to adhere to Kazakhstan's regulations on personal data and its protection, i.e. the Personal Data Law, in particular. Articles 30 and 31 impose additional restrictions on cross-border transfer of 'digital data products', including the outcomes of data processing operations. Adherence to personal data protection laws - and hence the localization clause - is also explicitly required by Articles 11 and 17 of the AI Law.

Policies currently under discussion would further tighten the localization requirement. The draft **Online Platforms Bill** would further extend requirements to companies outside Kazakhstan by requiring them to open local representative offices. Proposed amendments to several laws would tighten limits on data extraction from state

databases, and in April mandatory biometric identification for operators of large databases was introduced.

IMPLICATIONS OF DATA LOCALIZATION ON BUSINESSES

The current enforcement regime along with certain lack of regulatory clarity have so far allowed global data platforms to help drive digitalization and AI adoption efforts among individual users in particular. At the same time, to avoid legal risk, state and quasi-state organizations as well as many corporations often overinterpret these laws as limiting the use of the world's best cybersecurity, ERP, CRM and other solutions across a variety of industries, from mining to education.

Data localization also limits access to advanced data management models for sensitive data, such as hybrid and distributed cloud needed for speed, scalability, security and resilience of data and software, increasing cybersecurity risk. Compliance with the requirements is difficult as they are spread across multiple laws and regulations, yet lack practical and legal clarity.

Particularly for advanced AI products, localization of data storage and processing is not feasible. The advanced high-load compute required for AI deployments is enabled by the extensive use of cloud technologies and requires constant uninterrupted access to hyperscalers' infrastructure in regional clusters.

The trend toward greater requirements, is also on a different course than the EU and United States, which are seeking to reduce regulatory complexity.

THE DRAFT DECREE PROVISIONS

The draft decree *On Comprehensive Measures for the Development of the Data Processing and Storage Infrastructure and Ecosystem* contains three key provisions:

1. Lifting requirements for mandatory storage of digital databases in Kazakhstan and allowing cross-border data transfer for most categories of personal data
2. Adopting the Cloud First principle for government data processing, including conditionally including public cloud and private sector solutions
3. Simplifying security, compliance and operations requirements for the Data Centers Valley project participants

The first provision is a major step forward from the localization policy under the Personal Data Law. It allows cross-border transfer for most types of personal data to jurisdictions with adequate level of protection, or if the operator adheres to binding corporate rules, has standard contractual clauses, and obtains recognized security certification for data protection. Special categories of personal data are allowed to be

stored in the cloud if a Kazakhstan-based entity retains encryption keys and controls. This will spur adoption of advanced cloud and AI products in Kazakhstan.

The second provision revises the data localization approach outlined by the Informatization Law. It prioritizes the Cloud First principle for government sector data and under specific conditions allows government data processing in the public cloud. The specifics will be developed by the authorities but it highlights that the "digital government" platform (the existing domestic ecosystem of data centers, services and operators) shall be prioritized. This provision will give state and state-owned entities access to leading-edge data storage and processing.

The third provision lifts a number of restrictions for Data Valley participants with foreign ownership. They will no longer have to comply with numerous security requirements, such as mandatory use of the single backbone, use of local security certificates and cryptography, installation of surveillance equipment and providing security services access. Operators are given free hand in designing and routing their data flows, infrastructure and processes, on the condition they do not serve users in Kazakhstan. This provision is key to Kazakhstan becoming a Eurasia data transit and processing hub.

RECOMMENDATIONS

In our view, several recommendations, however, are in order for the Decree to fulfill its objective of accelerating the adoption of cloud and AI products in Kazakhstan and support the development of Data Center Valley project:

1. Distinguish sensitive personal data that must be stored in Kazakhstan, data that can be stored and processed abroad, and data where hybrid cloud or parallel storage scenarios are permissible, in clear and consistent regulations and future legislation.
2. Adopt globally-recognized security standards, certifications, and best practices, as well as advancing sector-specific domestic regulations for data processing in government, quasi-government and critical digital infrastructure sector contracts.
3. Withdraw the domestication and data registry requirements for global digital platforms in the Online Platforms Bill, and adopt subsequent regulations to AI Law and the Digital Code to avoid automatic imposition of processing and storage localization clauses on a wider range of datasets and data processing outcomes.

It is also worth noting that the removing multiple security obligations for Data Center Valley participants not servicing users in Kazakhstan does not resolve the underlying issue of imposing those obligations on digital companies providing services in the

country. In our view, these companies require analogous regulatory reform to enable provision of cutting-edge solutions to users in Kazakhstan.

Enacting policies outlined by the Decree will require changes to several interwoven laws and regulations, as well as in secondary regulation and bylaws. We strongly believe that the Ministry and relevant bodies should involve private enterprise during this process.

We are ready to share our international expertise and engage in a constructive dialogue with the Government of Kazakhstan to ensure requirements are technically and operationally feasible and aligned with both the national digitalization goals and global technological standards, allowing our companies to increase their participation in Kazakhstan’s digital future.