

International Comparative Legal Guides

Digital Business 2026

A practical cross-border resource to inform legal minds

Seventh Edition

Contributing Editor:

James Gill

Lewis Silkin LLP



iclg

Expert Analysis Chapter

- 1** Digital Business Laws and Regulations Report 2026: Trends, The Future of Law and Technology, Navigating 2026 and Uncertainty!
James Gill, Lewis Silkin LLP

Q&A Chapters

- 4** **Argentina**
Diego Fernández & Alejo M. Gascón,
Marval O'Farrell Mairal
- 17** **France**
Catherine Mateu, Armengaud Guerlain
- 31** **Germany**
Dr. Lutz Keppeler, Markus Lennartz & Jutta Schumann,
Heuking Kühn Lüer Wojtek Part GmbH
- 40** **Greece**
Anastasia Dritsa, Andriani Tzamarou, Io Ligeraki &
Natalia Soulia, KYRIAKIDES GEORGOPOULOS
Law Firm
- 49** **India**
Rajat Prakash, Siddharth Mahajan, Naina Chandok &
Rishabh Sharma, Athena Legal
- 63** **Italy**
Fabiana Bisceglia, Donata Cordone,
Eleonora Curreli & Irene Picciano, Portolano Cavallo
- 76** **Kazakhstan**
Yelena Manayenko, Kirill Greshnikov &
Dinmukhamet Nurakhmet, AEQUITAS Law Firm
- 85** **Norway**
Kristin Haram Førde, Kristian Foss,
Hanna Beyer Olaussen & Jan Martin Fjellestad,
Bull & Co Advokatfirma AS
- 95** **Philippines**
Arjel P. de Guzman, Adrian B. Mayuga,
Christine P. De Vera & Cybele Iris S. Longcob,
de Guzman Mayuga
- 103** **Sweden**
Jim Runsten, Johan Toma & Hannah Hallgren, Synch
- 111** **Switzerland**
Jürg Schneider, Hugh Reeves, Emilia Rebetez &
Jérôme Heman, Walder Wyss Ltd
- 121** **Taiwan**
Robin Chang & Eddie Hsiung,
Lee and Li, Attorneys-at-Law
- 129** **Thailand**
John Formichella, Naytiwut Jamallsawat,
Onnicha Khongthon & Supitchaya Akeyati,
Formichella & Sritawat Attorneys at Law
- 137** **Ukraine**
Yaroslav Baienko, Oleksandr Melnyk &
Anastasiia Klian, GOLAW
- 147** **United Kingdom**
Andrew Maguire, Littleton Chambers
- 158** **USA**
Kyle R. Dull, Squire Patton Boggs
- 167** **Uzbekistan**
Zafar F. Vakhidov, Kamila Sharipova, Zhanibek Nurgali &
Dilshodbek Egamberdiev, Vakhidov & Partners
- 178** **Vietnam**
Son Dang, DNA Vietnam LLC

Kazakhstan



Yelena
Manayenko



Kirill
Greshnikov



Dinmukhamet
Nurakhmet

AEQUITAS Law Firm

1 E-Commerce Regulation

1.1 What are the key e-commerce legal requirements that apply to B2B e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register with regulatory bodies, as well as a summary of legal obligations specific to B2B e-commerce.

In the Republic of Kazakhstan, B2B e-commerce is governed by legislation that is generally applicable to non-e-commerce entities. However, specific requirements emerge in areas related to platform compliance, which are outlined below.

Registration and notification requirements

Entities engaging in e-commerce must register as a legal entity or individual entrepreneur. This requirement applies universally to all businesses engaged in commercial activity, including those operating through electronic platforms.

To register, an applicant must select an appropriate organisational-legal form (limited liability partnership (LLP), joint-stock company (JSC), etc.) and submit an application to the relevant registration authority. While the documentation may vary depending on the form of registration, the standard package typically includes:

- an application for registration;
- information about the founder (a copy of the extract from the company register or a passport for individuals); and
- a receipt of payment of the state fee.

Following registration, the entity must notify the tax authority of the commencement of e-commerce activity. This requirement is established by Article 95 of the Tax Code No. 214-VIII of the Republic of Kazakhstan dated July 18, 2025 (Tax Code).

Platform compliance

Operators of electronic trading platforms are obligated to ensure the confidentiality of user data, maintain transparency in operations, and adhere to content moderation standards. Law of the Republic of Kazakhstan dated May 21, 2013 No. 94-V “On Personal Data and Their Protection” (Law on Personal Data Protection), governs the collection, processing, and protection of personal data. Businesses must obtain consent from data subjects for processing their personal data and ensure appropriate security measures are in place. Platforms must also ensure that their services are available in the official languages of Kazakhstan: Kazakh and Russian.

Lastly, platforms with a daily user base exceeding 100,000 are mandated to appoint a legal representative within

Kazakhstan, in accordance with Law of the Republic of Kazakhstan dated July 10, 2023 No. 18-VIII “On online platforms and online advertising” (Law on Online Platforms and Advertising).

Taxation

E-commerce entities must comply with general tax obligations, including corporate income tax (CIT) and value-added tax (VAT) under the Tax Code.

CIT is set at 20% for local entities and foreign companies operating through a permanent establishment.

VAT is imposed at 16% on goods, services, and imports, with mandatory registration for businesses exceeding a turnover threshold. Certain goods and services are VAT-exempt. Excise taxes apply to specific products like alcohol, tobacco, fuel, and certain vehicles, with rates based on physical units.

Consumer protection

Even in B2B transactions, businesses must ensure transparency regarding product information, pricing, and return policies, in alignment with consumer protection laws. The primary regulation is prescribed by Law of the Republic of Kazakhstan dated May 3, 2010 No. 533-IV “On the protection of consumer rights” (Law on Consumer Rights Protection).

1.2 What are the key e-commerce legal requirements that apply to B2C e-commerce in your jurisdiction (and which do not apply to non-e-commerce business)? Please include any requirements to register with regulatory bodies, as well as a summary of legal obligations specific to B2C e-commerce.

General requirements mentioned in the previous response also applied to B2C. However, for B2C e-commerce, specific regulations are usually centred around consumer protection and dispute resolution.

The Law on Consumer Rights Protection establishes key obligations for businesses engaged in B2C e-commerce. Sellers are required to clearly define the terms of sale, which should include product descriptions, pricing, payment options, delivery terms, and return/refund policies. Consumers must also be informed of their right to withdraw from a purchase, typically within 14 days of receiving the goods. Additionally, businesses must provide warranties, ensuring that products meet quality standards and are free from defects.

When it comes to dispute resolution, B2C e-commerce businesses are generally free to choose any type of dispute resolution mechanism. However, in practice – particularly in Kazakhstan – there are a growing number of complaints

concerning the inclusion of arbitration clauses in B2C relationships, as consumers are typically considered the weaker party and may not fully understand the implications of waiving their right to access the courts.

1.3 Please explain briefly how the EU's Digital Services Act and Digital Markets Act and/or equivalent local legislation, such as the UK's Online Safety Act and Digital Markets, Competition and Consumers Act, are affecting digital business in your jurisdiction.

The EU's Digital Services Act (DSA), Digital Markets Act (DMA), as well as the UK's Online Safety Act and Digital Markets, Competition and Consumers Act, do not apply in Kazakhstan where digital services are provided exclusively to users located within Kazakhstan by local entities. In such cases, local legislation governs digital business activities, including but not limited to laws on consumer protection, personal data protection, competition, and electronic commerce.

1.4 Are there any new laws planned in your jurisdiction that will affect e-commerce going forward?

Yes. A major recent development is the adoption of the Digital Code of the Republic of Kazakhstan dated 9 January 2026 No. 255-VIII (Digital Code), which is expected to significantly affect e-commerce going forward. The Code establishes a comprehensive legal framework governing digital relations, including the creation, use, and circulation of digital data, and applies to both local and foreign businesses operating in Kazakhstan. It introduces enhanced requirements on personal data protection, digital identification, cybersecurity, and regulates technologies such as smart contracts and automated (AI-based) decision-making. Although already adopted, its provisions will be enacted in July 2026, meaning that e-commerce businesses will face increased compliance obligations but also benefit from greater legal certainty and a more structured digital regulatory environment.

2 Data Protection

2.1 How has the domestic law been developed in your jurisdiction in the last year?

Over the last year, domestic law in Kazakhstan has undergone significant development, primarily through the transition from fragmented regulation to a more consolidated framework for the digital economy. The key development was the adoption of the Digital Code, which introduces a unified legal regime governing digital data, digital technologies, and digital services, replacing the previously dispersed regulation across laws on informatisation, personal data, e-commerce, and competition. This reform did not emerge in isolation. In his 2025 State of the Nation Address, President Tokayev expressly called for the accelerated adoption of the Digital Code and described it as a document that should define the key directions of digitalisation, including AI, the platform economy, and the use of big data. That political direction was then followed by concrete legislation that emphasised digital transformation, AI, and the platform economy.

In parallel, Kazakhstan adopted Law of the Republic of Kazakhstan dated November 17, 2025 No. 230-VIII "On Artificial Intelligence" (Law on AI), establishing a dedicated legal framework for the development and use of AI systems

based on principles such as transparency, safety, and accountability. Accompanying amendments expanded regulation in related areas, including allowing the broader circulation of unsecured digital assets beyond the Astana International Financial Centre (AIFC). At the same time, personal data protection and cybersecurity requirements were strengthened, including the introduction of mandatory multi-factor (including biometric) authentication for large-scale personal data processing and stricter testing and certification requirements for ICT infrastructure.

Further developments in e-commerce and trade regulation focused on increasing transparency and state oversight, including new reporting obligations for logistics and delivery operators involved in e-commerce and the adoption of a Trade Policy Concept prioritising digital trade and analytics. Overall, the past year reflects a shift toward a more structured, technology-specific, and compliance-oriented legal environment, increasing regulatory obligations for digital businesses while providing greater legal certainty and a clearer framework for innovation.

2.2 What privacy challenges are organisations facing when it comes to fintech, retail, AI and digital health?

In Kazakhstan, privacy challenges in fintech, retail, AI, and digital health are increasingly evidenced by real-world incidents involving data leaks and weak access controls, particularly in relation to state and quasi-state databases. A recurring issue has been the leakage of large volumes of personal data, including national ID numbers, phone numbers, and addresses, which have appeared in public online sources and messaging platforms. These incidents are often linked not to external cyberattacks but to insider access or insufficient control over contractors, which directly affects fintech companies relying on the same datasets for customer identification and onboarding.

In the fintech sector, risks are further amplified by integration with government digital infrastructure, such as eGovernment systems, where vulnerabilities in one component may impact multiple market participants. In retail and e-commerce, the widespread use of behavioural analytics and targeted advertising raises concerns around excessive data collection and lack of transparency in obtaining user consent, issues that have already attracted regulatory scrutiny. In digital health, the sensitivity of medical data and its centralised storage in digital systems increase exposure to breaches and require heightened security measures.

An additional emerging challenge relates to the use of AI systems, particularly regarding the opacity of algorithms and the processing of personal data without sufficient user awareness. Overall, practice in Kazakhstan demonstrates that the main privacy risks stem from insider-driven data leaks, insufficient cybersecurity, reliance on state-linked infrastructure, and underdeveloped data governance frameworks, all of which create significant compliance and reputational risks for organisations operating in these sectors.

2.3 What support are the government and privacy regulators providing to organisations to facilitate the testing and development of fintech, retail, AI and digital health, such as, for example, sandboxes?

The most established mechanism is the regulatory sandbox operated within the AIFC by the Astana Financial Services Authority (AFSA). The AIFC FinTech Lab functions as a full regulatory sandbox, allowing companies to test innovative

financial and RegTech products in a controlled live environment with real clients under a simplified regulatory regime. Participants benefit from temporary relief from certain licensing, capital, and reporting requirements and can gradually transition to full regulation once their models are validated. The sandbox also supports experimentation with advanced technologies, including AI-driven financial services and digital asset products.

In addition, Kazakhstan has expanded sandbox-type support beyond traditional fintech. In 2025, the National Bank of Kazakhstan launched a dedicated regulatory sandbox for digital assets, enabling real-world testing of tokenisation, crypto-exchange models, and stablecoin-related services under regulatory supervision. This reflects a broader policy trend toward controlled experimentation in emerging areas such as blockchain and Web3.

Beyond sandboxes, the AIFC ecosystem provides complementary support through accelerators, innovation hubs, and cross-border testing initiatives, including participation in the Global Financial Innovation Network (GFIN), which allows companies to test solutions simultaneously in multiple jurisdictions. These mechanisms are designed to reduce entry barriers, facilitate market access, and align local innovation with international standards.

For sectors such as AI, retail, and digital health, Kazakhstan currently relies less on formal sandbox regimes and more on general digital policy instruments, including the Digital Code and the Law on Artificial Intelligence, which create a legal framework for innovation but do not yet provide dedicated testing environments comparable to fintech sandboxes. However, AI solutions may still be tested indirectly within the AIFC sandbox when embedded in financial services.

3 Cybersecurity Framework

3.1 Please provide details of any cybersecurity frameworks applicable to e-commerce businesses.

In Kazakhstan, cybersecurity requirements applicable to e-commerce businesses are derived from several key legislative acts and are now increasingly systematised under the Digital Code.

The main framework is established by Law of the Republic of Kazakhstan dated November 24, 2015 No. 418-V “On Informatization”, which sets general obligations to ensure information security, including protection of information systems, prevention of unauthorised access, and implementation of technical and organisational safeguards. In parallel, the Law on Personal Data Protection imposes specific requirements on the secure processing, storage, and transfer of personal data, which are directly relevant for e-commerce platforms handling customer information.

Additional cybersecurity obligations arise where systems are classified as critical information and communication infrastructure under Law of the Republic of Kazakhstan dated January 6, 2012 No. 527-IV “On National Security”, requiring enhanced security measures, mandatory testing, and incident response procedures, as well as interaction with the State Technical Service.

3.2 Please provide details of other cybersecurity legislation in your jurisdiction. If there is any, how is that enforced?

Key additional acts include:

- 1) The Rules for Ensuring Information Security of Critical Information and Communication Infrastructure of the Republic of Kazakhstan approved by Decree of the Government of the Republic of Kazakhstan dated December 31, 2020 No. 757 set specific security requirements for designated critical entities. These include conducting risk assessments, vulnerability management, mandatory cybersecurity audits, and incident reporting obligations.
- 2) Law of the Republic of Kazakhstan dated July 5, 2004 No. 567-II “On Communications” regulates the activities of telecommunications providers, including requirements to implement technical measures for the protection of communication networks against cyber threats.

Enforcement of cybersecurity legislation is carried out by the Committee for Information Security of the Ministry of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan. This authority monitors compliance, conducts inspections, and is empowered to impose administrative fines for violations. In cases involving critical infrastructure, the National Security Committee of the Republic of Kazakhstan may intervene under national security grounds.

4 Cultural Norms

4.1 What are consumers’ attitudes towards e-commerce in your jurisdiction? Do consumers embrace e-commerce and new technologies or do consumers still prefer shopping in person?

In Kazakhstan, consumers generally embrace e-commerce and new technologies, particularly in urban areas, where online marketplaces, mobile banking, and digital payments are widely used. The growth of shopping platforms and accessibility of delivery services has significantly accelerated adoption, making online shopping a routine part of daily life.

At the same time, a hybrid model persists: many consumers still prefer in-person shopping for certain categories, especially high-value goods, due to trust concerns, product verification, and delivery reliability. Overall, however, the trend clearly indicates increasing confidence in e-commerce, driven by convenience, expanding logistics infrastructure, and widespread use of digital payment systems.

4.2 Do any particular payment methods offer any cultural challenges within your jurisdiction? For example, is there a debit card culture, a direct debit culture, a cash on delivery-type culture?

In Kazakhstan, there are no significant cultural barriers to digital payments, but certain payment preferences shape the market. The dominant model is a mobile-first and debit-based culture, with widespread use of banking apps, Apple Pay, and QR payments, which have made cashless payments highly accessible.

At the same time, cash-on-delivery (COD) remains relevant, especially in smaller cities and rural areas, where trust in online transactions and delivery reliability may be lower. Credit card usage is comparatively less developed than in Western markets, and direct debit models are not widely used in retail e-commerce.

4.3 Do home state retailer websites/e-commerce platforms perform better in other jurisdictions? If so, why?

Generally, home-state e-commerce platforms from Kazakhstan do not systematically outperform local platforms in other jurisdictions. Their performance abroad depends on factors such as market similarity, regulatory environment, and level of competition. They may perform relatively well in neighbouring or comparable markets due to familiarity with similar consumer behaviour, payment preferences, and logistics conditions, but tend to face stronger competition and entry barriers in more developed or highly regulated markets.

4.4 Do e-commerce firms in your jurisdiction overcome language barriers to successfully sell products/services in other jurisdictions? If so, how and which markets do they typically target and what languages do e-commerce platforms support?

Yes, e-commerce firms in Kazakhstan often overcome language barriers by providing multiple language options, typically including Kazakh, Russian, and English. For international markets, they add local languages depending on the target region, such as Uzbek, Turkish, or more common European languages.

To expand their reach, platforms localise websites by translating product descriptions, adjusting currency, and offering relevant payment methods. They primarily target neighbouring Central Asian markets like Uzbekistan and Kyrgyzstan, as well as Russia, and are increasingly reaching Eastern Europe and Turkey.

Additionally, e-commerce businesses offer multilingual customer support and utilise localised marketing to connect with consumers more effectively.

4.5 Are there any particular web-interface design concepts that affect consumers' interactivity? For example, presentation style, imagery, logos, currencies supported, icons, graphical components, colours, language, flags, sounds, metaphors, etc.

Web-interface design greatly impacts consumer interactivity. A clean, intuitive layout with easy navigation enhances user engagement, while high-quality images and recognisable logos build trust. Supporting local currencies and popular payment methods simplifies transactions. Offering native language support and currency converters boosts accessibility. Subtle sounds and familiar metaphors like shopping carts improve user experience and make the site more engaging.

Designing with local cultural preferences in mind is essential for international success.

4.6 Has the COVID-19 pandemic had any lasting impact on these cultural norms?

Yes, the COVID-19 pandemic has had a lasting impact on cultural norms surrounding e-commerce. With lockdowns and social distancing measures, many consumers shifted to online shopping for the first time, and this behaviour has largely persisted even after restrictions eased. The pandemic accelerated the adoption of digital payment methods, mobile commerce, and online service platforms, with many consumers now preferring contactless options over cash or in-store visits.

Additionally, trust in e-commerce grew as consumers became more familiar with online transactions, although concerns around data privacy and payment security remain.

E-commerce websites also adapted by offering more flexible delivery options, including contactless delivery and same-day shipping, catering to changing expectations for convenience and safety.

Overall, the shift towards digital interactions and reliance on online shopping is likely to continue as consumers have grown accustomed to the convenience and safety it offers.

5 Brand Enforcement Online

5.1 What is the process for online brand enforcement in your jurisdiction?

In Kazakhstan, online brand enforcement begins with registering trademarks with the National Institute of Intellectual Property (NIIP), which provides legal protection against unauthorised use. Companies typically monitor online platforms for potential infringements, such as counterfeit goods or misuse of logos. If an infringement is found, a cease-and-desist letter is often sent to the infringing party.

Brands also collaborate with e-commerce platforms and social media sites to report violations, leading to the removal of unauthorised listings. If informal methods do not work, legal action may be pursued through the Economic Court or Customs Authorities for counterfeiting issues. Customs may also seize counterfeit goods if the trademark is registered with the Customs Union of the Eurasian Economic Union (EAEU), offering extra protection.

5.2 Are there any restrictions that have an impact on online brand enforcement in your jurisdiction?

Yes. Online brand enforcement in Kazakhstan faces several practical and legal limitations. There is no formal notice-and-takedown regime, so platforms are not legally obliged to promptly remove infringing content, and enforcement often depends on their voluntary cooperation. The system is largely rights-holder driven, meaning brand owners must independently monitor infringements, collect evidence, and initiate action.

Additional challenges include cross-border issues, where infringing sellers or websites are located outside Kazakhstan, making enforcement more difficult, as well as the anonymity of online sellers, which complicates identification of the infringer. Court enforcement can also be time-consuming and procedurally demanding.

6 Data Centres and Cloud Location

6.1 What are the legal considerations and risks in your jurisdiction when contracting with third party-owned data centres or cloud providers?

In Kazakhstan, a key issue is data localisation expectations, as organisations are generally required to ensure that personal data of local users is stored within Kazakhstan. Using foreign cloud providers may therefore create compliance risks if data is transferred or hosted abroad without proper safeguards.

Another critical aspect is allocation of responsibility. Even when outsourcing infrastructure, the company remains responsible for how data is processed, stored, and protected.

This makes it essential to include detailed contractual provisions on data security, access controls, incident response, audit rights, and restrictions on subcontracting.

Cybersecurity is also a major concern, as businesses must ensure that providers implement adequate technical and organisational measures to prevent breaches and unauthorised access. At the same time, reliance on third-party infrastructure creates operational risks, including loss of control over data, service outages, and dependency on the provider.

Additional challenges include cross-border data transfers, enforceability of contracts with foreign providers, and limited visibility over how data is handled in complex cloud environments. Overall, careful due diligence and strong contractual safeguards are essential to mitigate these risks.

6.2 Are there any requirements in your jurisdiction for servers/data centres to be located in that jurisdiction?

Yes, Kazakhstan has data localisation requirements. According to the Law on Personal Data Protection, certain types of personal data must be stored within Kazakhstan's borders. This primarily applies to data related to Kazakh citizens, and the law mandates that data controllers ensure that such data is not transferred to foreign servers unless specific conditions are met, such as ensuring the destination country has equivalent data protection standards.

7 Trade and Customs

7.1 What, if any, are the technologies being adopted by private enterprises and government border agencies to digitalise international (cross-border) trade in your jurisdiction?

Kazakhstan is implementing a range of digital solutions to streamline foreign trade. In the customs domain, the "Astana-1" information system and the "single window" mechanism for electronic declarations are in operation, enabling online submission of documentation. Several international pilot projects are under way; for instance, Kazakhstan was the first country in the region to test the e-TIR electronic system for the transit of goods without paper-based TIR carnets; and has introduced electronic phytosanitary certificates (e-Phyto).

The national postal operator, Kazpost, is conducting a pilot project aimed at expediting customs clearance for cross-border e-commerce exports and enhancing the statistical tracking of international parcels.

Blockchain technologies are also being deployed – specifically, a blockchain-based information system is being developed for the administration of VAT, enhancing the transparency of fiscal transactions. Major online marketplaces are expanding their domestic infrastructure (such as fulfilment centres and logistics networks) and are integrating with government systems.

7.2 What do you consider are the significant barriers to successful adoption of digital technologies for trade facilitation and how might these be addressed going forward?

Despite significant progress, substantial challenges to digital trade remain in Kazakhstan:

- 1) Existing procedures are often complex. For example, burdensome customs processes create barriers for e-commerce exporters. Until recently, there were no tax

incentives or other policy measures to support the development of e-commerce, which deterred investment in the sector.

- 2) Insufficient coordination between government agencies and the private sector has led to fragmented initiatives. The government is addressing this through strategic programmes – such as Digital Kazakhstan and the E-Commerce Development Plan through 2027 – which aim to modernise legislation and foster collaboration between public authorities and the National Chamber of Entrepreneurs (Atameken).
- 3) Limited internet connectivity and underdeveloped logistics infrastructure in remote areas hinder business participation in digital trade. In response, the government is expanding broadband internet access and developing regional logistics hubs. In parallel, Kazakhstan is working to harmonise its regulatory framework with international standards (including those of the World Trade Organization (WTO), the EAEU, and bilateral agreements). For instance, the country has signed a Digital Trade Agreement under the auspices of the Organization of Turkic States.

8 Tax Treatment for Digital Businesses

8.1 Please give a brief description of any relevant tax incentives for digital businesses in your jurisdiction. These could include investment reliefs, research and development credits and/or beneficial tax rules relating to intellectual property.

Kazakhstan has established special tax regimes to incentivise the IT sector and promote innovation. The principal regime is the preferential tax treatment available to participants of the Astana Hub technology park. Residents of Astana Hub benefit from comprehensive tax exemptions, including 0% CIT (compared to the standard rate of 20%), exemption from VAT (16%) on the sale of IT services, 0% personal income tax on employee salaries, reduced social tax, among other benefits. These incentives are provided by law and are codified in the Tax Code.

In addition, a general framework of tax preferences is available to all investors in priority projects. Under an investment contract for the establishment of new production facilities, investors may be eligible for 100% exemption from CIT, land tax, and property tax for the duration of the contract. This regime is particularly relevant for priority sectors such as data centres and electronics manufacturing.

As of 2024, new incentives have been introduced to stimulate intellectual property (IP) development. Amendments to the Tax Code provide for an additional 50% deduction of eligible expenses incurred on research and development (R&D) activities, provided they are conducted within Kazakhstan and result in patentable or otherwise protectable outcomes.

Furthermore, the taxable base is reduced by 50% when acquiring IP rights for the purpose of implementing R&D results.

8.2 What areas or points of tax law do you think are most likely to lead to disputes between digital businesses and the tax authorities, either domestically or cross-border?

The rapid growth of the digital economy has given rise to new tax challenges, often leading to disputes between IT

businesses and tax authorities. One of the most pressing issues is the application of VAT to electronic services provided by foreign companies. As of January 1, 2022, amendments to the Tax Code of Kazakhstan require foreign suppliers of digital goods and services delivered online to Kazakhstani consumers to register with the tax authorities and remit 16% VAT. This so-called “Google Tax” obligates major international companies – such as Google, Apple, and Netflix – to comply with local VAT rules for sales to individuals in Kazakhstan. Misinterpretation or non-compliance with these provisions may result in disputes regarding the existence of a tax liability or nexus in Kazakhstan for foreign entities.

Another contentious area concerns the determination of permanent establishment (PE) and the corporate taxation of foreign digital businesses. The tax authorities may seek to classify significant in-country operations – such as those of large marketplaces or services with local teams – as constituting a PE subject to CIT in Kazakhstan. Meanwhile, companies often argue that their business lacks a physical presence and therefore does not meet the threshold for PE under domestic law or applicable double tax treaties.

Disputes also frequently arise over withholding tax on cross-border payments. For instance, software licence fees are typically classified as royalties subject to a 15% withholding tax. However, IT companies may contend that such payments constitute fees for services, potentially subject to a different rate or exemption under applicable double taxation agreements.

Furthermore, transfer pricing is a recurring source of disagreement. Intra-group transactions – such as software payments to a parent company – are scrutinised for compliance with the arm’s-length principle. In the digital economy, where transactions often involve unique intangible assets, this can lead to complex and subjective assessments by tax authorities.

9 Employment Law Implications for an Agile Workforce

9.1 What legal and practical considerations should businesses take into account when deciding on the best way of resourcing work in your jurisdiction? In particular, please describe the advantages and disadvantages of the available employment status models.

When hiring personnel in Kazakhstan, a company may choose between establishing employment relationships or engaging individuals under civil law contracts (such as contracts for services or work).

The choice of model involves several legal and practical considerations. An employment contract provides the individual with protections under labour legislation, including entitlement to paid leave, limits on working hours, and statutory guarantees upon dismissal. For the employer, this entails various obligations, such as withholding and remitting income tax and social contributions, ensuring safe working conditions, and compliance with overtime rules. However, an employment contract also enables the employer to define internal work regulations, determine the working schedule, and exercise direct control over the employee.

By contrast, a civil law contract (e.g., a services agreement) concluded with an individual is governed by the Civil Code and not subject to labour law. Under such arrangements, the contractor is responsible for organising their own work and

assumes the associated risks. This model offers greater tax efficiency and operational flexibility, particularly for short-term projects or freelance arrangements.

However, there are legal risks: if the actual working relationship exhibits the characteristics of employment – such as fixed working hours, subordination to company rules, personal and regular performance of work, etc. – then regulatory authorities or courts may reclassify the contract as an employment relationship. In such cases, the company may be required to pay all due taxes and social contributions retroactively and may also face administrative liability for violating labour laws.

9.2 Are there any specific regulations in place in your jurisdiction relating to carrying out work away from an organisation’s physical premises?

Kazakhstan’s labour legislation, in line with modern employment trends, establishes specific rules governing remote (telecommute) work. The Labor Code of the Republic of Kazakhstan dated November 23, 2014 No. 414-V (Labor Code) defines “remote work” as the performance of job duties outside the location of the employer, host party, or their facilities, using information and communication technologies in the course of employment.

The terms of remote work must be formalised either in the employment contract or in a supplementary agreement thereto. The Labor Code imposes additional obligations on the employer in the context of remote employment. In particular, the employer is required to either provide the employee with the necessary communication tools (e.g., a computer, software, etc.) or reimburse the employee for the use of their own equipment and internet connection.

Furthermore, the employer must comply with occupational health and safety requirements by issuing a regulatory act on safety protocols for remote work and by providing appropriate safety instructions to the employee.

9.3 What long-term effects or changes are likely to result from the COVID-19 pandemic?

The COVID-19 pandemic had a significant impact on the labour sector in Kazakhstan, accelerating its transformation. The mass shift to remote work in 2020 prompted the legislature to rapidly adapt the legal framework. As a result, amendments to the Labor Code concerning remote work were adopted as early as May 2020.

These amendments established the employer’s occupational health and safety obligations toward remote employees and effectively legalised permanent remote employment, thereby eliminating the existing legal vacuum.

10 Top ‘Flags’ for Doing Business as a Digital Business in Different Jurisdictions

10.1 What are the key legal barriers faced by a digital business operating in your jurisdiction?

Digital businesses in Kazakhstan face both general and sector-specific regulatory constraints. One of the key barriers is the data localisation requirement, previously mentioned. This mandates that global IT service providers must either host their servers within Kazakhstan or enter into agreements with local data centres. Such requirements increase operational

costs and may deter the entry of foreign online services into the Kazakhstani market.

Another significant barrier is the relatively strict regulation of online content. In 2023, Kazakhstan adopted the Law on Online Platforms and Online Advertising, which requires major social networks and messaging services with a daily user base exceeding 100,000 in Kazakhstan to establish an official representative office in the country. These platforms must also remove prohibited content upon request of Kazakhstani authorities, under the threat of being blocked. For digital companies, this represents an additional legal and compliance burden.

10.2 Are there any notable advantages for a digital business operating in your jurisdiction?

Alongside regulatory barriers, Kazakhstan also offers a number of significant advantages for IT companies:

- 1) A favourable tax and legal regime for technological enterprises (as described earlier).
- 2) Government authorities are implementing financial support programmes and sectoral development initiatives. As of 2024, direct support measures for e-commerce have been introduced: the government subsidises interest rates on loans and provides guarantee instruments for e-commerce entities. In collaboration with business associations, nationwide e-commerce training centres have been launched, and grants are awarded for IT projects through the Digital Kazakhstan fund, TechOrda competitions, and other initiatives.
- 3) Kazakhstan benefits from a well-developed digital infrastructure and strong consumer demand. The country has a large youth population and over 8 million internet users; cashless payments and mobile banking are widely adopted. These factors create a robust domestic market for digital services, offering opportunities for rapid business growth.

10.3 What are the key areas of focus of the regulator in your territory for those operating digital business in your territory?

Kazakh government authorities focus on several key areas of oversight related to the digital economy:

- 1) Government authorities strictly enforce personal data protection laws, requiring local data storage and the safeguarding of citizens' information. The Cybersecurity Concept "Cyber Shield of Kazakhstan" has been adopted, and measures are actively implemented to counter cyber threats. In the financial and digital sectors, the National Bank of Kazakhstan has mandated that all banks and payment organisations deploy fraud monitoring systems and report all incidents to a dedicated anti-fraud centre.
- 2) Government authorities conduct inspections and provide guidance to ensure that local IT companies correctly apply tax incentives, such as those under the Astana Hub regime, and prevent misuse of such benefits.
- 3) The National Bank promotes innovation, including the implementation of a central bank digital currency (CBDC) known as the digital tenge, and has adopted the Open Banking concept for 2023–2025. At the same time, it has tightened oversight of unlicensed payment services and cryptocurrency operations. Since 2023, the crypto-asset industry has been placed under regulatory

supervision, with licensing requirements introduced for crypto exchanges and mining data centres, along with restrictions on their energy consumption.

- 4) Government authorities monitor the service quality of marketplaces, handle consumer complaints related to cross-border platforms, and are developing regulations to ensure safe e-commerce practices.

11 Online Payments

11.1 What regulations, if any, apply to the online payment sector in your jurisdiction?

The legal framework for electronic payments and settlements in Kazakhstan is primarily established by Law of the Republic of Kazakhstan dated July 26, 2016 No. 11-VI "On Payments and Payment Systems". This law comprehensively regulates the organisation and operation of payment systems, the payment services market, and the procedures for executing payments and money transfers within Kazakhstan.

Under the law, only resident legal entities – banks and payment organisations established as LLPs – may provide money transfer services, subject to authorisation for payment services. A non-banking payment organisation must register with the National Bank of Kazakhstan and be included in the official register.

The National Bank issues regulatory acts that detail the implementation of the law, including rules on the issuance and use of electronic money, the procedure for opening and maintaining electronic wallets, and limits on anonymous transactions, among others.

The law also requires merchants and service providers to install payment terminals or integrate instant payment systems, thereby encouraging the development of e-commerce.

In addition to the core legislation, online payments are also subject to foreign exchange regulations – notably, Law of the Republic of Kazakhstan dated July 2, 2018 No. 167 "On Currency Regulation and Currency Control" governs cross-border transactions – and to AML and counter-terrorist financing (CFT) legislation, which imposes customer identification requirements for electronic transfers exceeding certain thresholds.

11.2 What are the key legal issues for online payment providers in your jurisdiction to consider?

Companies providing internet payment services (internet acquiring, e-wallets, transfers) should take into account a number of legal risks in Kazakhstan. First of all, the risk of non-compliance with regulatory requirements. Operating without the necessary licence or registration is fraught with prohibition and administrative liability. The law requires a payment organisation to operate strictly within the limits of authorised services, and if it engages agents to accept payments, it is jointly and severally liable to customers for their actions.

The second significant risk is violation of AML/CFT requirements. Payment providers are obliged to identify users, monitor suspicious transactions and report them to authorised bodies. Failure to comply with these obligations threatens sanctions up to and including licence revocation.

The third risk is the protection of personal data. The processing of customer financial data (card numbers, personal information) falls under the Law on Personal Data Protection, and leaking or storing data abroad without consent will violate

the law and result in fines. In addition, regarding cybersecurity, in case of a hacker attack on the payment system and theft of funds, the company may be subject to lawsuits from customers and control by authorised bodies.

The fourth risk is currency and sanctions compliance: when processing international payments, it is important to comply with currency rules (for example, residents are prohibited from receiving payment in foreign currency for intra-Kazakhstan sales) and international sanctions. Violations here may lead to problems with correspondent accounts.

12 Digital and the Green Economy

12.1 With the current global emphasis on the environment and sustainability, will current or anticipated legislation in that area affect digital business in your jurisdiction?

Although digital companies are not major polluters, environmental regulation in Kazakhstan is increasingly affecting their operations – particularly in high energy-consumption sectors.

The Environmental Code of the Republic of Kazakhstan dated July 1, 2021, is focused on reducing greenhouse gas emissions and promoting the adoption of best available technologies (BAT). Over time, this may lead to stricter energy efficiency requirements for data centres and IT infrastructure.

The most prominent example is the regulation of the cryptocurrency mining industry. Mining data centres consumes vast amounts of electricity, primarily generated by coal-fired power plants, thereby contributing significantly to the country's carbon footprint.

In 2022–2023, Kazakhstan introduced specific regulatory provisions. Under the Law of the Republic of Kazakhstan “On Digital Assets”, cryptocurrency mining companies are allowed to consume electricity from the national grid only if there is excess capacity available, and without compromising the energy needs of the population or industrial sectors.

In practice, mining operations are prohibited during periods of energy shortages, incentivising miners to develop their own renewable energy sources or to purchase green electricity. The law also requires mining entities to obtain a government licence, introducing transparency and regulatory oversight to the sector – measures that are closely tied to Kazakhstan's environmental objectives, particularly the goal of reducing uncontrolled energy consumption.

12.2 Are there any incentives for digital businesses to become ‘greener’?

Although there are currently few environmental incentives specifically targeted at the IT sector, digital companies in Kazakhstan can benefit from general “green” initiatives and programmes.

Kazakhstan is actively developing its green finance market, primarily through the AIFC, which supports the issuance of green bonds and provides preferential loans for sustainable

projects. If an IT company implements an energy efficiency initiative (e.g., upgrading a data centre to improve energy performance) or a project related to e-waste recycling, it may qualify for green financing from the Development Bank of Kazakhstan or international institutions such as the European Bank for Reconstruction and Development (EBRD) or the World Bank under favourable terms.

Kazakhstan is also introducing general tax incentives to reduce environmental impact. For example, companies that implement BAT in place of outdated processes are exempt from emission fees during the investment payback period. While such incentives may not directly apply to IT firms, indirect benefits may arise – such as reduced emission-related payments by telecom operators that upgrade to energy-efficient equipment, thereby lowering the carbon emissions associated with electricity consumption.

The government also encourages the transition to renewable energy. While there are no direct consumer subsidies, any company in Kazakhstan can enter into a power purchase agreement (PPA) with a renewable energy producer at a fixed “green” tariff, which may prove to be more cost-effective than market rates in the long term.

12.3 What do you see as the environmental and sustainability challenges facing digital businesses?

As Kazakhstan's IT sector expands, it increasingly faces environmental challenges that businesses must take into account.

One of the main concerns is energy sustainability and carbon footprint. Energy-intensive segments – such as data centres, cryptocurrency mining farms, and large-scale server facilities – consume substantial amounts of electricity, a significant portion of which is generated from coal-fired power plants. This presents not only an environmental issue, but also a business risk: disruptions or restrictions in energy supply (as occurred in 2021–2022 due to an influx of crypto miners) can severely impact the continuity of digital services.

The rapid expansion of IT infrastructure also leads to a growing volume of decommissioned electronic equipment, ranging from computers to networking devices. Kazakhstan currently has limited capacity for electronic waste recycling, forcing companies to either store outdated equipment or export it to countries with established recycling systems, facing regulatory hurdles related to the export of hazardous waste.

Under the country's Extended Producer Responsibility (EPR) rules, companies must pay utilisation fees when importing electronics, thereby increasing the cost of IT infrastructure components. Moreover, public pressure for environmental accountability is growing; larger companies are increasingly expected to safely dispose of batteries and smartphones and reduce plastic usage in their operations.

Tightening environmental regulations may also compel telecom operators and data centres to transition to energy-efficient equipment and adopt renewable energy sources, such as solar panels at communication sites. These shifts will require additional capital investment to meet new standards and societal expectations.



Yelena Manayenko's areas of specialisation are corporate and commercial law, subsoil use law, construction, infrastructure and anti-trust legislation. Yelena's experience in the subsoil use sphere encompasses support of major transactions and projects, including production, processing and transportation of oil and gas, mining production, construction of large production, recreation and infrastructure facilities. Yelena advises clients on the issues of structuring local and international transactions, drafting and coordination of commercial contracts, including sale and purchase agreements, as well as services, supply, construction, lease, franchise and distribution agreements, and represents clients' interests in relations with counterparties and governmental agencies.

Yelena has many times participated in the support of M&A transactions and due diligence of major Kazakhstan companies from different sectors of the economy.

AEQUITAS Law Firm

47 Abai Ave., Office 2
Almaty
Kazakhstan

Tel: +7 727 3 968 968

Email: y.manayenko@aequitas.kz

LinkedIn: www.linkedin.com/in/yelena-manayenko-11985a77



Kirill Greshnikov's areas of specialisation are information and digital, corporate and commercial law with a particular focus on TMT and financial sectors. A major part of his work is focused on legal support for FinTech projects and clients facing different issues of regulation of the digital economy, digitalisation, cross-border payments, blockchain, cryptocurrency, digital assets, software, data management, information processing, intellectual property, and antitrust legislation. Kirill is experienced in conducting comprehensive research in the sphere of intellectual property, commercial activities and technology-related transactions.

He actively advises clients on the issues of setting up, registration and doing business in Kazakhstan in the Astana International Financial Centre (AIFC) jurisdiction and regularly participates in the support of M&A transactions and due diligence of major companies from different sectors of economy.

As a part of AEQUITAS's membership in the European Business Association of Kazakhstan (EUROBAK), Kirill was elected as a member of the executive team of the Digital Committee for 2023 and will act as a co-chairman to deal with the issues of development of innovations based on technologies, cybersecurity, electronic commerce, cloud technologies and many other issues discussed by the Digital Committee.

AEQUITAS Law Firm

47 Abai Ave., Office 2
Almaty
Kazakhstan

Tel: +7 727 3 968 968

Email: k.greshnikov@aequitas.kz

LinkedIn: www.linkedin.com/in/kirill-greshnikov-b0a870216



Dinmukhamet Nurakhmet works on projects involving corporate and civil legislation issues, dispute resolution, M&A, and other issues pertaining to the laws of the AIFC.

While being a student, he actively participates in academic conferences and develops theoretical knowledge.

When acquiring vocational education, he participated in competitions on consideration of disputes by the International Commercial Arbitration (William C. Vis Moot) in Hong Kong, PRC (2023–2024), and the international judicial competition of the AIFC (6th AIFC Court & IAC Moot, 2023).

Dinmukhamet is a member of the Kazakh Vis Alumni Association responsible for scientific activities (2024).

AEQUITAS Law Firm

47 Abai Ave., Office 2
Almaty
Kazakhstan

Tel: +7 727 3 968 968

Email: d.nurakhmet@aequitas.kz

LinkedIn: www.linkedin.com/in/dinmukhamet-nurakhmet-6a7543274

AEQUITAS is one of Kazakhstan's leading law firms acknowledged in the global legal services market. For many years, authoritative legal guides, including *Chambers and Partners*, *Who's Who Legal*, *The Legal 500*, *Asialaw Profiles*, *Best Lawyers* and *IFLR1000*, have been rating AEQUITAS and its partners and associates as the country's most recommended in Energy & Natural Resources, Corporate & Finance, M&A, Dispute Resolution and other areas. Many publications specifically acclaim the firm's Labour, Environmental and Healthcare & Pharmaceuticals practice. AEQUITAS has been recognised as the "Firm of the Year" in Kazakhstan by *Lexology Index* (WWL Awards) between 2021–2024.

AEQUITAS's clients are companies active in the leading sectors of the economy from more than 50 countries, including major international corporations, companies representing world famous brands, banks and financial institutions, most of them working with AEQUITAS for

years. According to rating agencies and the firm's clients and business partners, AEQUITAS is one of the most client-oriented law firms in Kazakhstan. Alongside providing legal services of invariably high quality, AEQUITAS is regularly informing its clients of the business-relevant changes in legislation and practice, organising training and seminars and annually holding a Client Day.

www.aequitas.kz

AEQUITAS
— LAW FIRM —



The **International Comparative Legal Guides** (ICLG) series brings key cross-border insights to legal practitioners worldwide, covering 59 practice areas.

Digital Business 2026 features one expert analysis chapter and 18 Q&A jurisdiction chapters covering key issues, including:

- E-Commerce Regulation
- Data Protection
- Cybersecurity Frameworks
- Cultural Norms
- Brand Enforcement Online
- Data Centres and Cloud Location
- Trade and Customs
- Tax Treatment for Digital Businesses
- Employment Law Implications for an Agile Workforce
- Top 'Flags' for Doing Business as a Digital Business in Different Jurisdictions
- Online Payments
- Digital and the Green Economy