Yekaterina Khamidullina

Partner, Head of Dispute Resolution,
AIFC Law and TMT Practices

Kirill Greshnikov

Senior Associate

AEQUITAS Law Firm

CURRENT ISSUES IN ARTIFICIAL INTELLIGENCE REGULATION IN KAZAKHSTAN: OBLIGATIONS, LIABILITY, AND PRACTICAL RECOMMENDATIONS FOR BUSINESS

(information valid as of 23 June 2026)

Introduction

As artificial intelligence continues to play an increasingly significant role across sectors, states have begun actively developing regulatory frameworks to govern this domain. Kazakhstan has taken a proactive stance in this process: on 17 November 2025, the Republic of Kazakhstan adopted the Law "On Artificial Intelligence" (hereinafter — the "Law"), which became the first specialized legislative act in this field within the EAEU space. The Law entered into force on 18 January 2026.

The adoption of the Law materially alters the legal environment for businesses that use or intend to use AI-based solutions. In this context, what is of key interest to business is not so much the formal legislative novelties as the practical questions of their application, including regulatory uncertainties, potential restrictions, emerging risks, and the challenges that the new regulatory framework presents for businesses, with a view to identifying possible directions for the further development of the legal environment.

This article focuses primarily on the core provisions of the Law and a number of problematic aspects associated with it.

Key Provisions of the Law

As with most legislative acts, the Law introduces a number of new terms that are unique to Kazakhstani legislation. These include "artificial intelligence" (hereinafter — "AI"), "data library", "data library producer", "AI system user", "authorized body in the field of artificial intelligence", and others. The Law contains 15 defined special terms.

The Law defines AI as the functional ability to imitate cognitive functions characteristic of humans, providing results comparable to or superior to the results of human intellectual activity. Despite its broad formulation, this definition has practical significance, as it enables AI systems to be

distinguished from other digital solutions and thereby determines the scope of application of the regulatory requirements.

At the same time, the Law contains significant gaps, in that it does not legislatively define such important concepts as AI system developer, AI system distributor, and AI system integrator. The absence of regulation and definitions for these actors makes it difficult to delineate liability among parties working with AI and, consequently, to identify those at fault and those bearing responsibility. The lack of a clear status distinction between transnational suppliers (such as OpenAI), local IT companies acting as AI system integrators, and Kazakhstani AI system owners creates serious difficulties in determining zones of responsibility and establishing liable parties in cases where damage is caused.

A key feature of the Law is the introduction of a risk-based approach. Artificial intelligence systems are classified into three risk levels depending on their degree of impact on the security of users, society and the state, with the primary burden of classification placed on the owner and/or possessor of the artificial intelligence system or the operator of the national artificial intelligence platform. Minimal-risk artificial intelligence systems are those whose disruption or termination of operation will have minimal impact on their users. Medium-risk artificial intelligence systems are those whose disruption or termination of operation may lead to a decrease in the efficiency and effectiveness of users' activities and cause moral harm or material damage. High-risk artificial intelligence systems are those whose disruption or termination of operation may lead to an emergency of a social and/or man-made nature and/or significant negative consequences for defence, security, international relations, the economy, individual sectors of the economy, users, the infrastructure of the Republic of Kazakhstan, and the life of individuals.

For high-risk artificial intelligence systems, the Law establishes a stricter regulatory regime. In particular, with respect to high-risk artificial intelligence systems classified as critical information and communications infrastructure facilities, the Law provides for mandatory audit involving specialized auditors, maintenance of extended technical documentation, including descriptions of architecture, algorithms and data used, as well as the implementation of a continuous risk management process throughout the entire life cycle of the system. Such systems are required to undergo compliance testing against information security requirements in accordance with the legislation of the Republic of Kazakhstan.

For businesses, this means the need to establish internal compliance procedures of the highest standard. Furthermore, the Law classifies artificial intelligence systems by degree of autonomy: from low autonomy, where the algorithm merely prepares decision options for a human, to high autonomy, where the correction or cancellation of decisions made by the machine by a human is completely excluded or technically impossible.

A separate section of the Law is dedicated to transparency in the use of AI technologies.

The Law establishes that the distribution of synthetic results of the activity of artificial intelligence systems shall be permitted only if they are marked in machine-readable form and accompanied by a visual or other form of warning that ensures the possibility of perception by the user without the use of methods that hinder such perception.

Companies using chatbots and generative models for interaction with clients/users are now required to expressly inform them of the procedure for and consequences of automated processing of personal data, of the possibility of objecting to automated processing, as well as of the procedure for protecting their rights, freedoms and legitimate interests.

Owners and holders of artificial intelligence systems are also subject to the following obligations:

1) implementation of risk management of artificial intelligence systems;

2) taking measures to ensure the security and reliability of artificial intelligence systems, including protection from unauthorized access and failures in their operation;

3) maintaining documentation on the artificial intelligence system depending on the degree of its impact on the security, rights, freedoms and legitimate interests of individuals, public order in accordance with the list of documentation on artificial intelligence systems;

4) providing support to users on issues related to the operation of artificial intelligence systems;

5) providing users with the opportunity to review the user agreement of the artificial intelligence system before using it.

First and foremost, the Law requires the establishment of a continuous risk management process, which must be carried out throughout the entire life cycle of the artificial intelligence system and shall include:

1) identification and analysis of known and predicted risks of the artificial intelligence system when used in accordance with its intended purpose;

2) assessment of the risks of the artificial intelligence system, carried out in accordance with its intended purpose and under conditions of foreseeable misuse;

3) the adoption of appropriate and targeted risk management measures designed to prevent and eliminate identified risks;

4) regular updating of risks, at least once a year.

Particular attention is paid to preventive measures for ensuring the security and reliability of artificial intelligence systems. The operation of such systems must be conducted in a secure environment that excludes unauthorized access, critical software failures, and the possibility of abuse.

A certain administrative burden on artificial intelligence system developers is associated with the rules governing the maintenance of technical documentation. It is submitted that a risk-based approach should apply in this regard, under which the scope and depth of information disclosed are directly proportional to the degree of the artificial intelligence system's potential impact on public order, as well as on the fundamental rights and freedoms of individuals. Consequently, for high-risk solutions, clients will be required to maintain comprehensive technical files and audit logs.

For the purposes of protecting the rights of end users, the Law also establishes an obligation to provide continuous technical support. This requires owner companies to allocate resources for the establishment of a support service whose functionality enables users to receive timely explanations regarding the operational logic of the artificial intelligence system, as well as to promptly report system errors or incorrect data output.

An equally important obligation is the requirement to provide the user with the opportunity to review the user agreement prior to the actual commencement of use of the artificial intelligence system. As a rule, such a document sets out limitations on the liability of the artificial intelligence system owner, rules for the processing of submitted text requests, the scope of applicability of the technology, and other matters. Notwithstanding the foregoing, the legislator has reasonably refrained from requiring the disclosure of source code, thereby allowing commercial secrets to be preserved.

At the same time, the Law introduces a strict list prohibiting the creation and operation of artificial intelligence systems possessing any of the following functional capabilities:

1) the use of subconscious, manipulative or other methods that distort the behaviour of an individual and limit the ability to make informed decisions or force them to make decisions that may cause harm or create a threat of harm;

2) exploitation of the moral and/or physical vulnerability of an individual due to age, disability, social status and any other circumstances to cause or create a threat of causing harm to the individual;

3) assessment and classification of individuals or groups of individuals over a certain period of time based on their social behaviour or known, assumed or predicted personal characteristics, except in cases provided for by the legislation of the Republic of Kazakhstan;

4) collection and processing of personal data in violation of the legislation of the Republic of Kazakhstan on personal data and its protection;

5) classification of individuals based on their biometric data to conclude their race, political views, religious affiliation, and any other circumstances (criteria) for the purpose of using them for any discrimination against an individual;

6) determination of emotions of an individual without his/her consent, except in cases provided for by the legislation of the Republic of Kazakhstan;

7) creation and distribution of results of artificial intelligence systems prohibited by the laws of the Republic of Kazakhstan.

In their essence, these prohibitions are broadly consistent with the approaches enshrined in European regulation and reflect the general international trend towards restricting the most sensitive use cases of artificial intelligence.

The entry into force of the new regulations has entailed systemic changes in related areas of law as well. In the sphere of consumer protection, a new requirement has emerged applicable to sellers (manufacturers, contractors) working with goods (services) containing AI components. With the adoption of the Law, such persons are now under an obligation to inform consumers of potential risks and conditions for the safe use of goods (works, services) containing AI components (produced, performed and/or provided by an artificial intelligence system), by indicating the necessary information in the documentation accompanying the goods (works, services), on consumer packaging, labels, or by other means customary for particular types of goods (works, services).

In the area of personal data protection, a prohibition has been established on automated processing that alters the legal rights of a data subject without their explicit consent. With the introduction of the Law, the collection and processing of personal data for the purpose of creating or expanding databases through the non-targeted extraction of personal data from publicly available sources is prohibited.

Of particular practical interest is the establishment of the institution of trusted high-risk artificial intelligence systems, the lists of which are compiled by industry-specific government agencies to disseminate best practices in the relevant sector. Inclusion in such a list requires the completion of a mandatory audit, within the framework of which not only information security is assessed, but also the quality and legitimacy of the use of data libraries for the training of artificial intelligence models.

Risks and Opportunities for Business

The introduction of dedicated regulation in the field of artificial intelligence has a direct and immediate impact on the operations of Kazakhstani companies using AI in operational, marketing, managerial, or other business processes. The Law creates a new legal and compliance environment for business, in which the use of artificial intelligence requires not only technological, but also legal and regulatory maturity. Companies that are able to integrate regulatory requirements into their business processes will be positioned not only to minimise risks, but also to derive additional advantages from the growing AI market. In this regard, the Law gives rise not

only to additional restrictions and obligations, but also creates certain opportunities associated with increased market transparency and enhanced trust on the part of consumers and counterparties.

The key risk that can be identified in connection with the Law is the new regulatory burden imposed on business. Companies applying AI-based solutions effectively become subjects of a dedicated regulatory regime and are required to structure their internal processes in accordance with the requirements of the Law. This refers, in the first instance, to the need to classify the artificial intelligence systems in use by risk level, to maintain technical documentation, to implement risk management procedures, and in certain cases to undergo an audit. For many companies, particularly small businesses, this means the need to establish new, or to adapt existing, internal compliance procedures, entailing additional organisational and financial costs.

At the same time, the level of administrative fines is not significant for medium and large businesses. However, it cannot be excluded that enforcement practice in this area will, in all likelihood, be accompanied by heightened scrutiny from regulators, the public and the media, which further increases costs for business. For companies operating in the public domain, including banks, telecommunications operators and digital platforms, such risks may have more material consequences than the fine itself, being primarily associated with reputational exposure.

The use of artificial intelligence is directly linked to risks relating to data processing. In many cases, the use of AI involves active engagement with users' personal data. Such data was previously already subject to protection under personal data protection and informatisation legislation. With the entry into force of the Law, an additional protection regime for such data has been established, the requirements for the protection of users' data have been strengthened, and the ability to transfer such data to third parties, including foreign platforms, without the user's proper consent has been restricted. For businesses, this means the need to review practices regarding the use of cloud-based solutions, as well as to conduct more thorough legal assessments of the terms of engagement with AI service providers. It should also be noted that, unlike judicial practice concerning artificial intelligence, judicial practice on liability for personal data breaches is sufficiently well developed and indicates that companies are frequently held liable for violations in this area.

A further significant risk for business is the entrenchment in the Law of the principle of direct liability for the activities of artificial intelligence systems. The Law establishes that all entities involved in the creation, deployment and operation of AI systems shall bear responsibility for the functioning of the respective artificial intelligence systems and for the results of their activities, having regard to their role at each stage of the life cycle.

In effect, the legislator proceeds from a broad approach to defining the range of potentially liable persons. At risk are not only developers and owners of artificial intelligence systems, but also other persons interacting with AI, even where no specific regulation exists in respect of such persons (for example, integrators, distributors, suppliers, and the like), and in certain cases even end users, where their actions have resulted in a breach of legislative requirements. For businesses, this means that the use of artificial intelligence ceases to be an exclusively technological tool and becomes an independent source of legal risk requiring separate management.

It is expressly established that liability for the creation and operation of an artificial intelligence system is borne by all entities carrying out such activities. The Law enshrines a delineation of roles between the owner, the possessor of the artificial intelligence system, and the user of the artificial intelligence system. These persons are obliged to ensure continuous control over the artificial intelligence system to the extent and in the manner depending on their role, at all stages of the life cycle of the artificial intelligence system.

In practice, however, a reallocation of liability among the participants in the entire chain cannot

be excluded. For instance, where harm has arisen as a result of the characteristics of the AI model itself, deficiencies in its training, or the absence of built-in safeguards, claims may be brought not only against the user, but also against the developer or the owner of the artificial intelligence system. All of this entails not only the need to allocate technical responsibilities among all participants in the use of AI, but also the need for more careful structuring of the relationships between all participants, including the allocation of liability.

On the basis of the current provisions of the Law, it is reasonable to assume that the owner or possessor of an artificial intelligence system may be held liable on the basis of fault or negligence. The fault of the owner of the artificial intelligence system may consist in the incorrect selection of technology for a specific context (for example, the use of a consumer chatbot for creditworthiness scoring), the failure to conduct a bias audit with respect to its client base, the unlawful collection of data for training the model, the refusal to implement mandatory human oversight processes, and the like.

The liability of the user will, in all likelihood, traditionally be confined to the scope of their intentional unlawful acts. A user may be held liable for the nature of the text requests submitted and for conscious unlawful decisions taken by them on the basis of AI recommendations. It is submitted, however, that given that ordinary users do not always appreciate the boundary between what is prohibited and what is permitted, it would be reasonable to limit the liability of the user in cases where the developer of the artificial intelligence system has failed to implement basic control mechanisms and safeguards within their own artificial intelligence system (for example, those directed at preventing the generation of responses to impermissible or potentially unlawful user requests).

It is important to note that the concept and role of "artificial intelligence system developer" is not provided for in the Law, which complicates the determination of their level of liability in this area. The Law operates only with such entities as the owner, the possessor of the artificial intelligence system, and the user. At the same time, artificial intelligence system developers are not always the owners, possessors, or users of the artificial intelligence system. Given that the liability of an entity depends on their role at the relevant stage of the life cycle of the artificial intelligence system, the absence of specific regulation of the activities of an artificial intelligence system developer does not mean that they bear no obligations or liability. In such a case, the artificial intelligence system developer will be held liable on general grounds based on their role.

It may be assumed that an artificial intelligence system developer bears responsibility for the technical correctness, security, and compliance with established restrictions at the stage of creation of the artificial intelligence system. It is submitted that the artificial intelligence system developer should bear strict liability for architectural defects of the artificial intelligence system, encompassing liability for the safety of outputs, the absence of built-in safety mechanisms and ethical constraints, as well as for bias that is originally and algorithmically embedded in the model. There is a foreseeable risk that if an artificial intelligence system enables a user to unlawfully practise a regulated activity (law, economics, medicine, and the like) and such practice causes damage to third parties, potential liability may indirectly be attributed not only to the user but also to the artificial intelligence system developer.

The institution of civil liability in the field of artificial intelligence is complicated by the fact that the Civil Code of the Republic of Kazakhstan currently lacks specialised provisions governing the procedure for compensation of damage caused by the autonomous actions of artificial intelligence systems. In this regard, when resolving questions of liability, it will likely be necessary to apply by analogy the general rules on torts (obligations arising from the infliction of harm). However, a classical tort traditionally requires mandatory proof of an unlawful act, the fault of the tortfeasor, and a direct causal link. Proving the fault of a specific programmer or owner of an artificial intelligence system where harm has been caused as a result of multi-layered machine learning is, under the current legislation, virtually impossible.

Of separate significance is the risk associated with algorithmic decision-making. Whereas previously the adoption of discriminatory decisions was prohibited on the basis of the general approach and principles of legislation, which complicated the process of proving violations and holding offenders liable, the Law now expressly prohibits any discriminatory practices in the use of artificial intelligence that infringe upon the rights and legitimate interests of individuals. In practice, this means that companies must ensure the correctness and justifiability of decisions made using AI, particularly in sensitive areas.

An additional risk is also associated with the possibility of claims for compensation of damage. The Law expressly provides that compensation for damage caused by artificial intelligence systems shall be carried out in accordance with the general procedure established by the Civil Code of the Republic of Kazakhstan, which may indicate that owners of artificial intelligence systems bear liability for damage caused, including proprietary, reputational, and in certain cases moral harm.

Questions of liability arising from engagement with artificial intelligence may, in general, be identified as a subject worthy of a separate and dedicated publication. Given the broad range of potential violations in the use of AI, this matter warrants separate consideration. Set out below are the principal propositions relating to questions of liability.

From the perspective of the technical and legal nature of AI, three key categories of liability may be identified that can arise in connection with the use of artificial intelligence:

1) Administrative liability, which is expressly provided for by the legislation of Kazakhstan (under the Code of Administrative Offences of the Republic of Kazakhstan).

2) Civil liability, which arises in the event of harm and damage caused as a result of the use of artificial intelligence systems. The Law expressly refers to the application of the general provisions of civil legislation, in particular the rules on compensation for harm and damage.

3) Contractual liability, which assumes key significance in the relationships between participants in the chain of creation and use of AI. Under agreements between developers, suppliers, integrators and end users, the parties are entitled to allocate risks in detail, including the establishment of limitations of liability, warranties, data use conditions, and incident response procedures.

As noted above, a distinguishing feature of the current regulatory framework is that the Law enshrines the principle of distributed liability, under which multiple entities may potentially be held liable simultaneously depending on their respective roles.

For instance, where harm has arisen as a result of incorrect training of an artificial intelligence model or the absence of necessary safeguards, claims may be brought against the artificial intelligence system developer. Where an artificial intelligence system was used in breach of instructions or without regard to legislative requirements, liability will, in all likelihood, be attributed to the owner or the possessor of the artificial intelligence system.

By way of illustration, consider a typical situation in the financial sector, where credit organisations frequently use artificial intelligence systems to assess the creditworthiness of a client. In the event that an artificial intelligence system issues a refusal decision on the basis of incorrect or discriminatory data, the client is entitled to challenge such a decision. In the course of the dispute, questions may arise as to whether the artificial intelligence model was trained appropriately, whether the credit organisation had the ability to verify the correctness of its operation, and whether it ensured the requisite level of oversight. Depending on these circumstances, liability may be allocated between the credit organisation as the owner of the artificial intelligence system and the supplier as the developer of the artificial intelligence system.

Separate attention should be drawn to the risks associated with the opacity of the internal processes of AI operation. Many artificial intelligence models are characterised by limited

explainability of the decisions they produce, which in itself creates difficulties from the standpoint of demonstrating the lawfulness of their functioning. Under the conditions established by the Law, the absence of proper documentation, operation logs, and internal control procedures may significantly complicate a company's ability to defend its position in the course of regulatory inspections or in the resolution of potential disputes.

Without an established risk management and internal control system, a company is effectively deprived of the ability to demonstrate that it took reasonable measures to prevent violations. This is particularly critical for artificial intelligence systems classified as high-risk, where the requirements for transparency and oversight are heightened. Accordingly, it becomes of fundamental importance for businesses not only to implement AI solutions, but also to ensure their documentability, traceability, and manageability, not only from a technical standpoint, but also from legal and managerial perspectives.

It should be noted that a significant proportion of the risks enumerated above are not fundamentally new for business. Companies that have been actively implementing digital solutions have previously already encountered questions of liability for automated processes, personal data protection, algorithmic transparency, and the non-discriminatory nature of decisions made. The adoption of the Law in this regard does not so much create new categories of risk as formalise and reinforce already existing requirements, transposing them into the sphere of direct legal regulation and oversight.

It is equally important to note that the formalisation of the rules governing the use of AI enhances the predictability of the legal environment. For investors and technology partners, the existence of clear regulation is frequently a key factor in decisions regarding market entry or project scaling. In this sense, the Law performs not only a restrictive, but also a stimulating function, creating the foundation for the development of the AI ecosystem in Kazakhstan.

Practical Recommendations for Business

In conclusion, a number of recommendations may be identified that appear justified from the standpoint of minimising business risks and ensuring compliance with the requirements of the Law:

1) Companies are advised to adopt an internal AI compliance policy for the allocation of zones of responsibility, as well as to establish a unified register of artificial intelligence algorithms and software in use. These measures will enable the establishment of transparent rules for oversight of AI infrastructure and ensure the protection of informatisation objects.

2) It is recommended to conduct an audit of the lawfulness of the origin of information used for current machine learning, verifying that the information used for training the model has been obtained lawfully and does not infringe copyright, commercial, or personal data rights, and to document the information security processes applicable to such activities. The collection and further processing of users' personal data must be carried out subject to the user's prior consent to such collection and processing.

3) For the purpose of establishing an evidentiary basis, companies should develop internal technical passports describing the architecture of each artificial intelligence system. It is additionally recommended to implement labelling of AI-generated content in order to eliminate the risk of misleading users.

4) It is important to review existing contracts, confidentiality agreements, and user agreements, in which the conditions of AI use should be expressly stipulated and the limits of liability for potential system errors or failures of the artificial intelligence system clearly delineated.

5) To protect against financial losses, it is recommended to utilise voluntary liability and property interest insurance mechanisms. In parallel, it is recommended to organise regular audits of artificial intelligence algorithms and the collection of user feedback for the purposes of identifying technical vulnerabilities.

***

47 Abai Ave., office 2, Almaty 050000
Republic of Kazakhstan
+7 727 3 968 968
aequitas@aequitas.kz