Kazakhstan – September 2026

Digital Code of the Republic of Kazakhstan

On 12 July 2026, the Digital Code of the Republic of Kazakhstan dated 9 January 2026 No. 255-VIII (the "**Digital Code**") entered into force. The Digital Code establishes a unified legal framework for relations in the digital environment arising from the creation, circulation, storage, transfer and use of digital data and digital objects. If the Digital Code conflicts with another law of Kazakhstan on matters governing relations in the digital environment, the Digital Code prevails. International treaties ratified by Kazakhstan prevail over the Digital Code. Subject to the Constitution, applicable laws and ratified international treaties, the Digital Code also applies to foreign individuals and foreign legal entities carrying out the relevant activities in Kazakhstan[1].

Upon the Digital Code's entry into force, the Law of the Republic of Kazakhstan dated 7 January 2003 "On Electronic Documents and Electronic Digital Signatures" was repealed. The Digital Code now directly regulates the relevant matters.

The key principles of the new framework include protection of human rights and legitimate interests, security of the digital environment, free circulation of digital data and use of digital technologies, a balance between private and public interests, technological neutrality, digital accessibility, digital ethics and social responsibility[2]. The main provisions that, in our view, may be relevant to businesses are summarised below.

1. Digital Data and Digital Objects

The Digital Code establishes a general principle that digital data may be freely created, collected, stored, processed, used and transferred. Digital data containing personal data, state secrets, confidential information or other information protected by law remain subject to the specific requirements of the applicable legislation[3].

The Digital Code also establishes rights of individuals and legal entities to whom digital data processed in the digital environment relate. Digital data subjects may access their data, control their use, request their deletion or restriction of processing, and obtain information about the purposes, legal grounds and methods of processing. A personal data subject may request deletion, anonymisation or restriction of processing, subject to statutory exceptions, including mandatory retention; performance of obligations under law or contract; protection of life, health and third-party rights; proceedings concerning offences; administration of justice; a public interest expressly established by law; archival, statistical or research purposes; and performance of state functions or provision of public services[4].

The Digital Code systematises the legal regime of digital objects. Digital objects include digital records, digital assets, digital resources, software, digital systems, digital platforms, digital infrastructure facilities and digital data products[5]. Owners and/or holders of digital objects must respect third-party rights,

[1] Articles 1(1), 1(3) and 2 of the Digital Code:;
[2] Article 4 of the Digital Code;
[3] Article 16 of the Digital Code;
[4] Articles 37 and 41 of the Digital Code;
[5] Article 20 of the Digital Code;

+7 705 209 91 59 | +998 97 727 0345
zv@vakhidovlaw.com
vakhidovlaw.com

including personal data and confidentiality requirements, and take measures to prevent unlawful access to, copying, alteration or deletion of digital data and digital objects.

The Digital Code separately regulates digital infrastructure facilities, including data centres, telecommunications networks and communications equipment, as well as distributed digital objects. Distributed digital objects may be centrally distributed or decentralised. For the joint ownership, use and disposal of distributed digital objects, the Digital Code introduces the concept of a "digital condominium", in which the participants' rights and obligations are determined by agreement or smart contract[6].

Digital assets remain subject to special regulation. Their issuance, circulation, storage and accounting are governed by the Law of the Republic of Kazakhstan "On Digital Assets in the Republic of Kazakhstan", while the Digital Code applies to matters not regulated by that special legislation[7].

2. Digital Platforms and Circulation of Digital Data Products

The Digital Code distinguishes between ordinary users and business users of digital platforms. A business user is an individual or legal entity that uses a platform to sell goods, perform work, provide services or carry out other income-generating activities. Activities conducted through platforms and requirements applicable to platform users are also governed by sector-specific legislation.

Owners of digital platforms must ensure transparency of the terms of use set out in their user agreements.

Requirements applicable to digital platforms must be proportionate to the functions performed, their impact on the rights of an indefinite group of persons, and the nature of their control over digital data, services, goods and the results of user interaction[8].

A separate regime applies to platforms for the exchange and circulation of digital data products. A digital data product means an aggregated and formalised result of digital data processing, comprising structured or otherwise transformed digital data suitable for use, exchange and/or circulation in the digital environment. These platforms may be established, including by private businesses, subject to compliance with digitalisation and cybersecurity requirements[9].

Owners and/or holders of these platforms must:

• create and maintain a list of digital data products and provide the conditions for access, exchange and use;

• prevent unauthorised access to and leakage of digital data products, and prevent their cross-border transfer where such transfer is restricted by the laws of Kazakhstan; and

• notify the Agency for Strategic Planning and Reforms of the Republic of Kazakhstan of the commencement or termination of the relevant activity or actions in accordance with the legislation on permits and notifications.

---

[6] Articles 25, 26 and 35 of the Digital Code;
[7] Article 22 of the Digital Code;
[8] Article 29 of the Digital Code;
[9] Article 30 of the Digital Code;

Owners and/or holders of these platforms are also prohibited from circulating source or unprocessed data, including personal data, unless otherwise permitted by law; placing or storing digital data products outside Kazakhstan where such placement or storage is restricted; and transferring digital data products to third parties without the consent of the owner and/or holder of the product, except where permitted by law[10].

3. Algorithmic Systems and Artificial Intelligence

The Digital Code does not replace the Law of the Republic of Kazakhstan "On Artificial Intelligence", but establishes general rules for algorithmic systems and fully automated decisions. An algorithmic system is defined as a digital system that makes or influences decisions based on automated data processing, including an artificial intelligence system[11].

Decisions made using algorithmic systems must not result in discrimination. In the cases and according to the procedure established by the laws of Kazakhstan, a person in relation to whom a fully automated decision is made may obtain information about the use of an algorithmic system and an explanation of the key factors and criteria that influenced the decision, without disclosure of the algorithm, source code or legally protected secrets. If the decision has legal consequences or may affect the person's rights and legitimate interests, the person is entitled to request the decision to be reviewed by an authorised employee of the organisation or state authority that uses the algorithmic system and makes the relevant decision[12].

The Digital Code also provides for quality audits of digital objects. An audit of the quality of an artificial intelligence system must consider the quality and lawfulness of the use of data libraries for model training, as well as the presence of prohibited functionalities under artificial intelligence legislation[13].

4. Digital Identification, Electronic Digital Signatures and Electronic Documents

Legal relations in the digital environment are carried out using technologies that identify participants, confirm their expression of intent and record legally significant facts. The unique identifiers are the individual identification number for an individual and the business identification number for a legal entity, branch or representative office, as well as for an individual entrepreneur operating as a joint enterprise[14].

Digital authentication confirms the identity of an individual or the legal capacity of a legal entity when accessing digital services and digital objects. Multi-factor digital authentication constitutes a basis for the creation, amendment or termination of legal relations in the digital environment and may serve as evidence of legally significant actions[15].

Codes, passwords, one-time digital identifiers, push notifications, biometric confirmations and other tools specified by the Digital Code may be used as digital confirmation where provided by law or agreed by the parties. Digital confirmation is not an electronic digital signature and does not, by itself, ensure the

[10] Article 31(9) of the Digital Code;
[11] Article 43(1) of the Digital Code;
[12] Article 43(2)-(5) of the Digital Code;
[13] Article 100 of the Digital Code;
[14] Articles 44 and 45 of the Digital Code;
[15] Article 46 and 47 of the Digital Code;

authenticity or integrity of a digital record. Biometric data used for digital authentication constitute personal data and must be protected under personal data legislation; mandatory processing of biometric data and biometric authentication are permitted only in cases established by law.

An electronic digital signature ("**EDS**") is equivalent to a handwritten signature where the conditions established by the Digital Code are met. The public-key certificate must be issued by a certification authority accredited in Kazakhstan or by a foreign certification authority registered with Kazakhstan's trusted third party. A foreign EDS is therefore recognised in Kazakhstan only through the prescribed cross-border authenticity-verification mechanism[16].

Transfer of an EDS private key to another person, and use of that key by another person, are prohibited. The certificate holder must protect the private key against unlawful access and use. An EDS certificate is subject to revocation, including upon a change of the head or name of a legal entity, or its reorganisation or liquidation[17].

An electronic document signed with the EDS of an authorised person is equivalent to a paper document. The head of a legal entity may authorise an employee or another designated person to sign electronic documents, but that person must use the EDS certificate and corresponding private key issued in their own name.

The Digital Code also regulates smart contracts, which provide for automatic performance of terms agreed by the parties. Smart-contract terms may be expressed in computer code if the parties' rights and obligations can be determined unambiguously and reproduced in a human-readable form. A smart contract must provide for a dispute-resolution procedure under which the final decision is made by a human[18].

5. Digital Public Administration

A substantial part of the Digital Code concerns the digitalisation of public administration. The Digital Code establishes the foundations of the state's digital architecture and digital government and regulates unified state digital platforms, the digital government web portal, digital events, proactive delivery of public services and the life cycle of state digital objects[19].

State bodies and other entities that have access to national registers must obtain the required information directly from the relevant reference-data sources and must not require individuals or legal entities to provide documents if the information is already contained in national registers. In addition, government notices sent through the single notification point are deemed delivered where the system records their proper delivery[20].

[16] Articles 49 and 57 of the Digital Code;
[17] Articles 51, 58 and 59 of the Digital Code;
[18] Article 67 of the Digital Code;
[19] Articles 68- of the Digital Code;
[20] Articles 64 and 66 of the Digital Code;

For businesses, these provisions are relevant when obtaining electronic public services and interacting with state digital systems. Companies should keep their contact details current and regularly monitor state digital services because properly delivered digital notices may have legal consequences.

6. Cybersecurity, State Control and Liability

The Digital Code establishes two distinct regulatory regimes for trusted and critical digital objects. A digital object is classified as trusted if it meets the prescribed requirements relating to security, reliability, localisation and technical support and is included in the register of trusted digital objects. Digital objects in healthcare, banking, communications, transport, industry and other significant sectors may be designated as critical. The owners and/or holders of critical digital objects must comply with special cybersecurity requirements and, where required by law, conduct cybersecurity audits[21].

The Digital Code provides for state control in the fields of digitalisation, electronic documents and EDS. Control may take the form of inspections and preventive control in accordance with the Entrepreneurial Code of the Republic of Kazakhstan and cybersecurity legislation[22].

Owners and/or holders are responsible for protecting their digital objects. Digital data protection must include technical, organisational, legal and other measures intended to prevent, identify and eliminate cyberthreats[23]. Cybersecurity compliance testing is mandatory for the digital objects specified by law. In other cases, testing and audits may be conducted at the initiative of the owner and/or holder. Owners and/or holders of critical digital objects must conduct cybersecurity audits in cases provided by the laws of Kazakhstan[24].

A breach of digital legislation entails liability under the laws of Kazakhstan. Administrative or criminal liability does not release the responsible person from the obligation to remedy the breach[25].

Overall, the Digital Code creates a baseline legal framework for digital data, digital objects and platforms, algorithmic systems, digital identification, electronic documents and cybersecurity. Companies should determine their status under the Digital Code; assess whether any platforms or digital objects they use must be included in the relevant registers; update user agreements and internal data-processing rules; and ensure compliance with digital authentication, EDS and cybersecurity requirements. Because a number of operational requirements depend on implementing regulations, companies should also monitor the adoption and amendment of the relevant registration criteria, platform rules, cybersecurity requirements and audit procedures.

[21] Articles 32 and 33 of the Digital Code;
[22] Article 96 of the Digital Code;
[23] Articles 97 and 98 of the Digital Code;
[24] Articles 33(4) and 99 of the Digital Code;
[25] Article 105 of the Digital Code;

Contacts:

Zafar Vakhidov

Partner, Vakhidov & Partners
Kazakhstan/Uzbekistan
ZV@vakhidovlaw.com

Zhanibek Nurgali

Associate, Vakhidov & Partners
Kazakhstan
ZhanibekN@vakhidovlaw.com