



DIGITAL CODE OF THE REPUBLIC OF KAZAKHSTAN

Unofficial translation

Code of the Republic of Kazakhstan dated January 9, 2026 № 255-VIII ZRK

Unofficial translation

SECTION 1. BASIC PROVISIONS

Chapter 1. GENERAL PROVISIONS

Article 1. Relations regulated by this Code

1. This Code shall regulate public relations, arising in the digital environment during the creation, circulation, storage, transmission and use of digital data and digital objects.

The digital environment shall be understood to mean the totality of infrastructure, technologies, processes and conditions for the creation, circulation, storage, transfer and use of digital data and digital objects, the exercise and transfer of rights thereto, regardless of the territory of their placement or registration of rights, insofar as they affect the public relations regulated by this Code.

2. Property and other civil law relations, arising in the digital environment shall be regulated by the civil legislation of the Republic of Kazakhstan, subject to the specific provisions, established by this Code.

3. Foreign nationals, stateless persons and foreign legal entities, involved in the creation, circulation, storage, transfer and use of digital data and digital objects in the territory of the Republic of Kazakhstan, shall enjoy the rights and freedoms in the Republic of Kazakhstan and shall bear the obligations, established for citizens and legal entities of the Republic of Kazakhstan, unless otherwise provided by The Constitution of the Republic of Kazakhstan, this Code, the laws of the Republic of Kazakhstan and international treaties, ratified by the Republic of Kazakhstan.

Article 2. Digital legislation of the Republic of Kazakhstan

1. The digital legislation of the Republic of Kazakhstan shall be based on the Constitution of the Republic of Kazakhstan and consist of this Code and other regulatory legal acts of the Republic of Kazakhstan.

2. International treaties, ratified by the Republic of Kazakhstan, shall take precedence over this Code. The procedure and conditions in the territory of the Republic of Kazakhstan for the operation of international treaties, to which the Republic of Kazakhstan is a party, shall be determined by the legislation of the Republic of Kazakhstan.

3. In cases of conflict between this Code and other laws of the Republic of Kazakhstan, regarding the regulation of relations in the digital environment the provisions of this Code shall apply.

Article 3. The purpose and objectives of the digital legislation of the Republic of Kazakhstan

1. The purpose of the digital legislation of the Republic of Kazakhstan shall be to ensure sustainable development and functioning of the digital environment in the interests of individuals and legal entities, society and the state.

2. The objectives of the digital legislation of the Republic of Kazakhstan shall be:

- 1) legal regulation of social relations arising in the digital environment;
- 2) defining mechanisms for implementing a unified state policy in the digital environment ;
- 3) strengthening law and order in the digital environment;
- 4) creating conditions, conducive to attracting investment in the development of the digital environment in the Republic of Kazakhstan;
- 5) legal support for the digital transformation of all social relations areas.

Article 4. Principles of digital legislation of the Republic of Kazakhstan

Legal regulation of social relations in the digital environment shall be governed by the following fundamental principles:

- 1) respect for the rights, freedoms, and legitimate interests of individuals in the digital environment;
- 2) security of individuals, society and the state in the use of digital technologies;
- 3) freedom of digital data circulation;
- 4) freedom to create, develop and use digital technologies;
- 5) balance of private and public interests;
- 6) accessibility and inclusiveness of the digital environment;
- 7) proportionate and justified state participation in the digital environment;
- 8) technological neutrality of legal regulation;
- 9) digital ethics and social responsibility.

Article 5. Respect for human rights, freedoms and legitimate interests in the digital environment

1. Human rights, freedoms and legitimate interests in the digital environment shall be recognized as the highest value and may be limited only by the laws of the Republic of Kazakhstan and only to the extent necessary to protect the constitutional order, public order, human rights and freedoms, public health and morality.

2. Relations in the digital environment shall be based on the free, conscious and expressed will of the individual.

3. Algorithmic and automated decisions affecting human rights, freedoms and legitimate interests in the digital environment shall be applied in compliance with transparency, non-discrimination and ability of the digital environment user to exercise control.

Article 6. Security of individuals, society and the state in the use of digital technologies

1. Security of an individual, society and the state in the use of digital technologies is an integral element of sustainable operation of the digital environment.

2. The state shall take measures to prevent and mitigate the risks of negative impact and use of digital technologies on the rights, freedoms and legitimate interests of an individual, society and the state, ensuring their necessity and proportionality to the goals pursued.

Article 7. Freedom of digital data circulation

1. The Republic of Kazakhstan ensures freedom of search, formation, transmission, storage and use of digital data within the limits established by this Code and the laws of the Republic of Kazakhstan.

2. Restriction of access to digital data shall be allowed in accordance with the laws of the Republic of Kazakhstan.

3. The State shall promote the development of a mechanism for the openness, reliability, accessibility, relevance, completeness of digital data, their digital compatibility and free exchange of digital data.

Article 8. Freedom to create, develop and apply digital technologies

1. Creation, development and application of digital technologies shall be free, unless otherwise provided by this Code and the laws of the Republic of Kazakhstan.

2. The state shall create enabling conditions for scientific research, innovation and development of digital technologies.

3. The state shall ensure implementation of measures to improve digital literacy among the population, develop accessible infrastructure and eliminate digital divide, and also equal conditions for the development of private initiatives and competition in the digital environment.

Article 9. Balance of private and public interests

1. Public relations in the digital environment shall be regulated with observance of a balance between private and public interests.

2. Pursuit of public interests must not lead to unjustified restriction of the rights of private individuals.

3. In the exercise of state regulation proportionality shall be ensured between its goals and consequences for a person and a citizen, interests of the society and the state.

4. State bodies and organizations shall ensure transparency, openness and motivation of decisions, adopted with the use of digital technologies.

Article 10. Accessibility and inclusivity of the digital environment

1. The State shall ensure equal access for citizens to digital technologies, products, services and opportunities in the digital environment.

2. Digital resources, for which accessibility requirements are established by the legislation of the Republic of Kazakhstan, shall be developed and used with due regard to accessibility

for persons with disabilities, as well as persons with visual, hearing or speech impairments and other functional limitations and persons with limited mobility.

Article 11. Proportionate and justified state involvement in the digital environment

1. The state shall participate in the digital environment within the frames established by this Code and the laws of the Republic of Kazakhstan.

2. State involvement in the creation and operation of digital resources and systems shall be permitted for the purposes of performing state functions, providing public services and ensuring security, sustainability and accessibility of digital infrastructure subject to the requirements for preventing unjustified interference in the competitive environment.

Article 12. Technological neutrality of legal regulation

1. The principle of technological neutrality of legal regulation presupposes equal treatment of various digital technologies.

2. Legal regulation of relations in the digital environment is based on the functional characteristics of digital technologies.

3. The state shall ensure predictability and stability of legal regulation as new digital technologies emerge, without creating obstacles to their development.

Article 13. Digital ethics and social accountability

1. Digital technologies shall be created, developed and applied in accordance with the principles of respect for human rights and dignity, non-discrimination, fairness, integrity, transparency and accountability.

2. The state, organizations and citizens shall participate in the development and observance of ethical standards of conduct in the digital environment, aimed at preventing discrimination, manipulation, abuse of digital technologies and other violations of the rights, freedoms and legitimate interests of individuals, society and the state.

Chapter 2. STATE REGULATION IN THE DIGITAL ENVIRONMENT

Article 14. Jurisdiction of the digitalization authority

1. The digitization authority (hereinafter referred to as the authorized body) is the central executive body, exercising leadership and cross-sectoral coordination in digitalization.

2. Within its jurisdiction the authorized body shall:

1) formulate the state policy in digitalization in accordance with the legislation of the Republic of Kazakhstan based on and pursuant to the main directions of the internal and foreign policy of the state, determined by the President of the Republic of Kazakhstan, and the main directions of the socio-economic policy of the state, its defense capability, security and public order, developed by the Government of the Republic of Kazakhstan;

2) perform strategic, regulatory, realizing and supervising functions;

3) develop and approve regulatory legal acts in digitalization field;

4) exercise other powers, stipulated by this Code, other laws of the Republic of Kazakhstan, acts of the President of the Republic of Kazakhstan and the Government of the Republic of Kazakhstan.

Article 15. Jurisdiction of state bodies in digitalization

Within their jurisdiction the State bodies shall:

- 1) participate in the implementation of state policy in digitalization;
- 2) develop and approve regulatory legal acts in digitalization;
- 3) exercise state supervision within their jurisdiction;

4) exercise other powers, stipulated by this Code, other laws of the Republic of Kazakhstan, and acts of the President of the Republic of Kazakhstan and the Government of the Republic of Kazakhstan.

SECTION 2. DIGITAL ENVIRONMENT OBJECTS

Chapter 3. DIGITAL DATA

Article 16. Digital data

1. Digital data refers to information provided in digital form that is suitable for automated and (or) analytical collection, storage, processing, use, transmission, distribution or deletion, regardless of the method by which it was obtained or the form in which it is provided digitally

2. Digital data may be freely created, collected, stored, processed, used and transmitted, unless otherwise provided by the laws of the Republic of Kazakhstan.

3. State bodies, state legal entities and quasi-public sector entities, with the exception of special state bodies, shall provide access to digital data and digital records to the digital government operator (hereinafter referred to as the operator) for the purpose of data analytics in accordance with the requirements for digital data management, developed by the authorized body in coordination with the state statistics authority and approved by the Government of the Republic of Kazakhstan.

4. Management of the digital data, containing state secrets, official or confidential information, personal data, and other information, protected by law shall be effected in accordance with the requirements and specific provisions, established by the laws of the Republic of Kazakhstan.

Article 17. Open Data

1. Open data is digital data presented in machine-readable form and intended for free use, processing, re-publication and distribution, placed in the public domain.

2. The open data internet portal is the state digital resource for the centralized placement, description, storage, search, access and reuse of open digital data, as well as the provision of software interfaces for machine access to such data.

3. The open data internet portal shall provide free, open, and non-discriminatory access to the open data posted on it, subject to technical limitations related to ensuring stability, security or performance of the portal.

4. The operator shall ensure its technical support, cybersecurity, uninterrupted availability, relevance of the posted open data, and also logging of the portal user actions in the manner determined by the authorized body.

5. Information holders, as defined by the Law of the Republic of Kazakhstan On Access to Information shall publish open data on the open data portal on an ongoing basis and update them timely in accordance with the legislation of the Republic of Kazakhstan on access to information.

6. Other digital environment entities, not specified in this article shall have the right to voluntarily submit digital data that do not contain restricted information, for publication on the open data portal.

7. Digital data that became accessible to an unlimited number of persons due to a leak, errors, security breaches, unauthorized use, granting of access to such data, or other unlawful actions, shall not be considered open data and shall be subject to immediate removal from digital resources in accordance with the procedure, established by the legislation of the Republic of Kazakhstan, with notification to the cybersecurity authority and the National Security Committee of the Republic of Kazakhstan.

Article 18. Administrative digital data

1. Administrative digital data are digital data, generated by state bodies, state legal entities, quasi-public sector entities and the entities performing their assigned state functions and providing state services.

2. The administrative digital data shall be collected, formed, stored, processed, used, updated and transmitted in accordance with data management requirements and the legislation of the Republic of Kazakhstan on state statistics.

3. The authorized body for determining the administrative digital data quality shall be the state statistics authority in accordance with the legislation of the Republic of Kazakhstan on state statistics.

4. Administrative digital data must be maintained and updated on an ongoing basis for the following purposes:

- 1) ensuring the quality of national registers;
- 2) improving the efficiency of public administration and provision of public services;
- 3) generating official statistical information;
- 4) data analysis;
- 5) executive decision-making.

Article 19. National registers

1. The National Register is a digital resource containing reference digital data, defined within the framework of the digital government architecture, and used as a single source of

reliable information for the performance of state functions, provision of public services, interdepartmental interaction and state statistics.

2. The list of national registers, their structure, composition of the reference digital data, as well as the requirements for their maintenance and updating shall be determined by the authorized body in consultation with the state statistics authority.

3. Owners and (or) holders of digital objects, who are holders or sources of digital data for national registers, shall ensure the appropriate quality of the digital data, contained in the relevant national registers.

The quality of digital data, included in national registers shall be determined by the state statistics authority in accordance with the legislation of the Republic of Kazakhstan in the state statistics.

4. If digital data are available in the national register, the state digital entities, using such data must obtain them directly from the relevant national register.

5. State bodies, state legal entities and quasi-public sector entities through database integration shall provide access to administrative digital data, contained in national registers to the state statistics authority for the pursuance of statistical activities, and also to the authorized body for data analysis.

Chapter 4. DIGITAL OBJECTS

Article 20. Digital objects and their types

1. A digital object is a separate element of the digital environment, created, used, or transmitted through digital technologies, possessing unique digital characteristics and enabling digital entities to exercise the rights of ownership, use, or disposal to the extent established by the legislation of the Republic of Kazakhstan.

2. Digital objects include:

- 1) digital records;
- 2) digital assets;
- 3) digital resources;
- 4) software;
- 5) digital systems;
- 6) digital platforms;
- 7) digital infrastructure objects;
- 8) digital data products;
- 9) other digital objects, stipulated by the laws of the Republic of Kazakhstan.

3. Digital objects are subject to systematization through their identification, categorization, description and recording in a digital object classifier, which is compiled and maintained by the authorized body.

4. Suspension of operation or restriction of user access to digital objects shall be permitted in cases and in the manner, stipulated by the laws of the Republic of Kazakhstan and only to

the extent, necessary for the purpose of protecting the constitutional order, public order, human rights and freedoms and the public health and morality.

Article 21. Digital records

1. A digital record is defined as a separate digital object, consisting of information recorded in digital form or data regarding such information, that possesses unique identification characteristics, enabling determination of the record's content, source, structure, or purpose.

2. Digital records are classified into:

1) identification digital records - recording factual, personal or official information and intended to individualize digital data;

2) title certification digital records - certifying creation, ownership, transfer, encumbrance, or termination of rights to digital and (or) tangible objects, including items, goods, raw materials, and other assets, as well as claims related to such objects.

3. Identification digital records, including those containing personal data, are not involved in civil circulation, and the rights to their content (information) are protected as intangible assets (personal non-property rights) or as restricted-access information in accordance with the legislation of the Republic of Kazakhstan.

4. Digital records containing personal data and provided to state bodies shall be used by state bodies only on the basis and within the limits established by the laws of the Republic of Kazakhstan, without the emergence of ownership rights of the state to such data, except in cases expressly provided for by the laws of the Republic of Kazakhstan.

5. Title certification digital records may be transferred, alienated, encumbered, or allow for other disposal of the corresponding property rights. The specific procedures for the creation, use, accounting and circulation of title certification digital records shall be established by the legislation of the Republic of Kazakhstan on digital assets.

Article 22. Digital assets

1. Digital assets are defined as digital objects, classified as digital assets in accordance with the Law of the Republic of Kazakhstan On Digital Assets in the Republic of Kazakhstan.

2. The creation (emission), release, circulation, storage, accounting, termination of circulation, and other relations, pertaining to digital assets and financial instruments derived therefrom shall be regulated by the Law of the Republic of Kazakhstan On Digital Assets in the Republic of Kazakhstan and other laws of the Republic of Kazakhstan, establishing the legal regime for digital assets and related financial instruments.

3. The provisions of this Code on digital objects shall apply to digital assets to the extent not regulated by the Law of the Republic of Kazakhstan On Digital Assets in the Republic of Kazakhstan.

Article 23. Software

1. Software is a digital object consisting of a set of codes, prepared for use, implementing algorithms that ensure the performance of certain functions, processing, storing, reproducing and (or) transmitting digital data.

2. The rights to the software belong to the right holder and shall be protected in accordance with the legislation of the Republic of Kazakhstan on copyright and related rights.

3. Open-source software may be created and maintained by multiple entities that jointly participate in its development or modification.

Open-source code is defined as a code that is available for viewing, studying, using, copying, and (or) modifying under the terms specified by the copyright holder and the rules for participation in the development of such code.

Source code is the text of a program written in a programming language, intended for the creation and modification of the software.

4. Open-source software shall be distributed and used under the terms of an open license.

5. An open license is defined as a license of the copyright holder that grants an unlimited number of persons the right to use, study, copy, modify, and distribute open-source software, subject to the terms and restrictions established by such license.

Article 24. Digital resources

1. A digital resource is a collection of organized digital data, digital records and software for their creation, storage, processing, display and distribution.

2. A digital resource, hosted on a digital infrastructure and identified by a domain name, Internet address, or other digital identifier is recognized as an Internet resource.

3. Subject to restrictions, established by the laws of the Republic of Kazakhstan, the owner and (or) holder of a digital resource shall have the right to:

1) establish the procedure and conditions for access to the digital resource, as well as the rules for using such digital resource;

2) use designations, identifiers, and other means of individualizing the digital resource that are not prohibited by the laws of the Republic of Kazakhstan;

3) protect their rights, freedoms, and legitimate interests from unlawful interference, impact, blocking, copying, modification, security breach, or other unlawful use of the digital resource.

4. The owner and (or) holder of a digital resource is obligated to:

1) ensure the safety, integrity, protection, and confidentiality of digital data and digital records posted or processed in the digital resource;

2) comply with the requirements of the legislation of the Republic of Kazakhstan on personal data and their protection;

3) provide users of the digital resource with information on the terms of access, processing of digital data and digital records and use of its functionality.

5. The owner and (or) holder shall have other rights and shall fulfill other obligations, established by the laws of the Republic of Kazakhstan.

6. The terms of posting, processing and use of digital data and digital records in digital resources, as well as access to such digital data and digital records shall be determined by the legislation of the Republic of Kazakhstan, the terms of the public offer, the user agreement, or other agreements concluded with the digital resource users.

Article 25. Digital infrastructure objects

1. A digital infrastructure object is defined as a set of material, technical and technological resources that support the placement and operational environment of digital objects.

2. Digital infrastructure objects include data processing centers, telecommunications networks, communications and other infrastructure facilities.

3. Requirements for the creation, placement, operation, modernization, sustainability, integrity, and cybersecurity of digital infrastructure objects shall be established by the legislation of the Republic of Kazakhstan.

4. Digital infrastructure objects may be state-owned or privately owned.

5. State digital infrastructure objects shall be created to implement state functions, provide public services, protect national interests and ensure the continuity of public administration.

6. Non-state digital infrastructure objects may be used to support the operation of state digital objects in accordance with the laws of the Republic of Kazakhstan.

Article 26. Distributed digital objects

1. A distributed digital object is defined as a digital object created, stored, processed, or used through a distributed architecture, characterized by the use of multiple interconnected technical means that ensure consistency, authenticity and integrity of digital records without their single processing center.

2. Distributed digital objects operate on the basis of internal interaction regulations that define the procedure for recording, coordinating, verifying, storing and using digital data, as well as algorithms for ensuring consistency, authenticity and immutability of digital records.

3. Distributed digital objects are classified as:

1) centralized-distributed, in which a single entity coordinates, controls, maintains, or confirms transactions of the participants;

2) decentralized, in which participants directly coordinate, verify, and record digital data among themselves without a designated coordinator using consensus algorithms or other mechanisms.

4. The specifics of ownership, use and disposal of distributed digital objects shall be determined by this Code and the laws of the Republic of Kazakhstan.

5. Distributed digital objects are objects of joint ownership, excluded from circulation.

Article 27. Data processing centers

1. A data processing center is a digital infrastructure object, designed to host and to provide an operational environment for other digital objects using technological, engineering, technical means and software.

2. Data processing centers may undergo a national or international technical audit in accordance with the procedure, established by the authorized body in consultation with the National Security Committee of the Republic of Kazakhstan.

3. A data processing center must have an engineering, power, telecommunications and technological infrastructure, ensuring its uninterrupted, fault-tolerant, and secure operation.

4. Data processing centers used to host digital objects containing state digital data, restricted-access data, or critical digital objects must comply with the requirements, established by the authorized body in consultation with the National Security Committee of the Republic of Kazakhstan.

Article 28. Digital systems

1. A digital system is a functionally integrated set of digital resources that utilizes digital infrastructure objects to facilitate creation, collection, processing, storage and distribution of digital data, also to automate the interaction of digital environment entities and (or) to enable the provision of services in the digital environment.

2. The owner and (or) proprietor of a digital system shall have the right, unless otherwise established by the laws of the Republic of Kazakhstan or by the owner and (or) proprietor of digital resources, to determine the rules for the operation of the digital system, including the conditions for the movement and use of the digital resources contained therein.

The owner and (or) proprietor of a digital system shall ensure reliability, integrity, protection and cybersecurity of the digital system, and also comply with the requirements of the legislation of the Republic of Kazakhstan on personal data and their protection.

3. If the owner and (or) proprietor of a digital system are not the owners and (or) proprietors of the digital resources contained therein, the procedure for operating the digital system and accessing the digital resources shall be determined by an agreement between such owners and (or) proprietors.

4. The creation, commercial operation, maintenance, development, integration, termination of commercial operation and protection of secure digital systems, classified as state secrets, shall be carried out in accordance with this Code, unless otherwise provided by the legislation of the Republic of Kazakhstan on state secrets.

Article 29. Digital platforms

1. A digital platform is a digital object, providing access to services in the digital environment, data, services and goods (works, services), offered by digital environment subjects and enabling interaction between them.

2. Depending on their activities on the platform, users of digital platforms are classified into digital platform users and business users:

1) digital platform users – are individuals or legal entities using the digital platform to search for, order, or purchase goods, perform work, provide services, and for other consumer or ancillary purposes unrelated to income generation, including entrepreneurial activity;

2) business users of the digital platform are individuals or legal entities, using the digital platform to sell goods, perform work, provide services, or engage in other income-generating activities, including entrepreneurial activity.

3. Activities carried out on the digital platform, as well as the requirements for digital platform users, are determined by the industry-specific legislation of the Republic of Kazakhstan.

4. Requirements for digital platforms shall be established to an extent commensurate with the functions performed, the extent of influence on the rights of an indefinite number of persons, and the nature of control over digital data, services, goods, or the results of interaction.

5. Digital platform owners shall ensure transparency of the terms of use, set out in the user agreement.

6. In cases where a business user, owner, and (or) proprietor of a digital platform, in accordance with the Tax Code of the Republic of Kazakhstan, performs the duties of a tax agent or taxpayer, such duties shall be carried out in the manner and to the extent, established by the Tax Code of the Republic of Kazakhstan.

Chapter 5. DIGITAL DATA PRODUCTS AND THEIR CIRCULATION

Article 30. Digital data product

1. A digital data product is an aggregated, formalized result of digital data processing, comprising structured or otherwise transformed digital data, suitable for use, exchange, and (or) circulation in the digital environment.

2. The structure, quality, and metadata of digital data products of state bodies, state legal entities and quasi-public sector entities shall be regulated in accordance with data management requirements.

3. A digital data product on the digital data product exchange and circulation platform may be the subject of transactions, alienation and transfer under the terms determined by the owner, with the exception of publicly available information, stipulated by the legislation of the Republic of Kazakhstan.

4. A digital data product on a digital data exchange and circulation platform must have the following properties:

1) not containing personal data that could allow identification of personal data subjects directly and (or) indirectly;

2) created, processed and structured in accordance with digital data security and quality requirements;

3) comprising the necessary metadata on the composition, structure, purpose and terms of use.

Article 31. Digital data exchange and circulation platforms

1. A digital data exchange and circulation platform is a digital platform that provides access to digital data products hosted thereon with established conditions for their exchange and circulation in accordance with this Code and the legislation of the Republic of Kazakhstan.

2. State bodies, state legal entities, quasi-public sector entities and private businesses operating in the Republic of Kazakhstan may create digital data exchange and circulation platforms in compliance with uniform requirements in digitalization and cybersecurity, as well as the operating rules for digital data exchange and circulation platforms, approved by the authorized body for data economy development in consultation with the authorized body.

3. The authorized body for data economy development is the government body exercising leadership in strategic planning, reform implementation and state statistics areas.

4. Digital data exchange and circulation platforms shall be included in the register of digital data exchange and circulation platforms subject to the criteria and procedure determined by the authorized body for data economy development.

5. Owners and (or) holders of digital data exchange and circulation platforms are required to:

- 1) ensure creation and maintenance of the list of digital data products;
- 2) ensure conditions for access, exchange and use of digital data products;
- 3) prevent unauthorized access, leakage and cross-border transfer of digital data products, if such transfer is restricted by the laws of the Republic of Kazakhstan.

6. The authorized body for data economy development shall monitor digital data exchange and circulation platforms.

7. From the moment they commence operations, the owner and (or) operator of platforms for the exchange and circulation of digital data products are required to file a notification regarding the commencement or termination of operations or activities to the authorized body for data economy development, in accordance with the legislation of the Republic of Kazakhstan on permits and notifications.

8. The authorized body for the data economy development shall develop and approve a standard methodology for assessing the value of digital data products for state bodies, state legal entities and quasi-public sector entities in consultation with the authorized body.

9. Owners and (or) holders of platforms for the exchange and circulation of digital data products shall be prohibited from:

1) circulating raw (unprocessed) data, including personal data, unless otherwise provided by the laws of the Republic of Kazakhstan;

2) placing or storing digital data products outside the territory of the Republic of Kazakhstan, if such placement or storage is restricted;

3) transferring digital data products to third parties without the consent of the owner and (or) holder of the digital data product, except in cases, stipulated by the legislation of the Republic of Kazakhstan.

Chapter 6. SPECIAL REGIMES FOR DIGITAL OBJECTS

Article 32. Trusted digital objects

1. Trusted digital objects are defined as digital objects, excepting digital records and digital assets that meet the criteria for security, reliability, localization and technical support established by the authorized body, as well as other requirements of the legislation of the Republic of Kazakhstan.

2. Trusted digital objects shall be included in the register of trusted digital objects by the authorized body if the digital object complies with the established requirements for trusted digital objects. The authorized body shall create and maintain the register of trusted digital objects, and also determine the types of digital objects to be included in the register, in accordance with the rules for the creation and maintenance of the register.

3. State bodies, state legal entities and quasi-public sector entities shall procure digital objects, included in the register of trusted digital objects in accordance with the legislation of the Republic of Kazakhstan on public procurement and on procurement by certain entities of the quasi-public sector.

4. Inclusion of a digital object in the registry of trusted digital objects shall not grant the state exclusive rights to such digital object, nor shall it restrict the rights of its owner.

5. If a digital object ceases to meet the established requirements for trusted digital objects, the authorized body shall decide to remove the digital object from the registry of trusted digital objects and notify the interested state bodies, owners and (or) holders and users of the digital object accordingly in compliance with the rules for the formation and maintenance of the registry.

Article 33. Critical digital objects

1. Critical digital objects are digital objects, whose disruption or cessation of operation leads to unlawful collection and processing of restricted personal data and other information, containing legally protected secrets, a social and (or) man-made emergency, or significant negative consequences for defense, security, international relations, economy, individual economic sectors, or the livelihoods of the population residing in the relevant territory, including infrastructure, such as heat supply, electricity supply, gas supply, water supply, industry, healthcare, communications, banking, transportation, hydraulic structures, law enforcement or digital government.

2. The list of critical digital objects, as well as the rules and criteria for classifying digital objects as critical shall be approved by the cybersecurity authority.

3. Non-state digital objects classified as critical digital objects, as well as those intended for the formation of state digital resources, are required to comply with cybersecurity requirements.

4. In cases, stipulated by the laws of the Republic of Kazakhstan, the owner and (or) holder of critical digital objects are required to conduct a cybersecurity audit.

Article 34. National digital objects

1. National digital objects are state digital objects, whose status is established by the laws of the Republic of Kazakhstan due to their critical importance for the performance of state functions, provision of public services, or sustainable operation of the state's digital architecture.

2. A digital object is designated as national in accordance with the laws of the Republic of Kazakhstan, which establish the status of such digital objects and define the specific procedures for their creation, development, operation, modification, and protection.

3. National digital objects are objects of public interest and may not be alienated, pledged as collateral, encumbered, or subject to property claims, nor may they be subject to enforcement proceedings based on the obligations of their owners or other persons, except in cases expressly provided for by the laws of the Republic of Kazakhstan.

4. Creation, development, operation, modification, and protection of national digital objects shall be funded from state budget or other sources, not prohibited by the legislation of the Republic of Kazakhstan.

Article 35. Digital condominium

1. A digital condominium is a form of ownership, in which participants exercise joint rights of ownership, use and disposal of distributed digital objects, created and used by them in accordance with common interaction rules.

2. A digital condominium consists of:

- 1) individual digital objects, belonging to the participants;
- 2) shared digital objects, used jointly by the participants for the operation of the relevant infrastructure.

3. Participants own, use and dispose of the digital objects belonging to them, while shared digital objects are used in accordance with the terms set forth in an agreement or a smart contract.

4. Shared digital objects are managed by entities in the digital environment either directly or through an authorized representative, acting under a contract with the participants.

5. The rights and obligations of participants shall be determined by an agreement between them or by the terms of a smart contract and are evidenced by digital records confirming participation and scope of the relevant rights.

6. The procedure for the creation, operation, accounting and termination of digital condominiums shall be determined by the authorized body.

SECTION 3. DIGITAL ENVIRONMENT ENTITIES Chapter 7. DIGITAL ENVIRONMENT ENTITIES, THEIR TYPES, RIGHTS AND OBLIGATIONS

Article 36. Types of digital environment entities

1. Digital environment entities are individuals and legal entities, including state bodies and organizations, possessing a digital identity in accordance with the legislation of the Republic of Kazakhstan, including:

- 1) digital data entities;
- 2) owners and (or) holders of digital objects;
- 3) users of digital objects;
- 4) other digital environment entities, defined by this Code and other laws of the Republic of Kazakhstan.

2. The rights and obligations of digital environment entities shall be determined in accordance with this Code and the laws of the Republic of Kazakhstan.

Article 37. Digital data subjects

1. A digital data subject is an individual or legal entity, to whom digital data processed in a digital environment relate and who can be identified using such digital data.

2. Individuals to whom personal data relate are considered personal data subjects.

3. Personal data may be processed or transferred only with the consent of the digital data subject or in cases, expressly provided for by the laws of the Republic of Kazakhstan.

4. A digital data subject shall have the right to protect his personal non-property rights, arising in connection with the creation and use of their digital data, as well as their rights with respect to such digital data, including the right to access, control and delete such data, to restrict its processing and to receive information about the purposes, legal grounds and methods of processing the digital data.

5. These rights shall be exercised upon confirmation of the digital data subject or the authority of his representative, also upon verification of the relevant digital data, belonging to such a subject.

6. The specifics for exercising the rights of digital data subjects shall be determined by the laws of the Republic of Kazakhstan.

Article 38. Owners and (or) holders of digital objects

1. Owners and (or) holders of digital objects shall hold ownership or other rights stipulated by the laws of the Republic of Kazakhstan and the terms of the agreement with respect to such digital objects.

2. The owner and (or) holders of a digital object are obligated to:

1) respect the rights, freedoms and legitimate interests of third parties, including requirements for the protection of personal data and confidential information;

2) take measures to prevent unauthorized access, copying, modification, or deletion of digital data and digital objects;

3) fulfill other obligations, established by this Code and the laws of the Republic of Kazakhstan.

3. The transfer of rights to digital objects shall be carried out on the grounds and in accordance with the procedures provided for by the Civil Code of the Republic of Kazakhstan, this Code and the terms of the contract.

4. The owner and (or) holder of a digital object shall be liable for harm caused by their unlawful actions (or inaction) in the creation, use or disposal of the digital object, in the cases and to the extent, established by the laws of the Republic of Kazakhstan.

Article 39. Users of digital objects

1. Users of digital objects are individuals or legal entities that lawfully use digital objects in accordance with paragraph 2 of this article.

2. A user of a digital object shall have the right to:

- 1) use digital objects under the terms and conditions determined by the legislation of the Republic of Kazakhstan and by the owner and (or) holder of the digital object;
- 2) receive accurate information on the characteristics and risks of the digital object;
- 3) protect their rights against unlawful restriction of access or abuse by the owner and (or) holder or other users of the digital object;
- 4) enjoy other rights, established by this Code and the laws of the Republic of Kazakhstan

3. A user of digital objects shall be obligated:

- 1) to comply with the requirements of the legislation of the Republic of Kazakhstan on the protection of personal data and confidential information;
- 2) not to interfere with the operation of the digital object or modify it without the permission of the owner and (or) holder of the digital object;
- 3) to act in good faith and not cause harm to other users of the digital object;
- 4) to perform other duties in accordance with this Code and other laws of the Republic of Kazakhstan.

Chapter 8. FUNDAMENTAL RIGHTS OF DIGITAL ENVIRONMENT SUBJECTS

Article 40. The right to digital identity and its protection

1. Digital identity is a set of digital records, enabling establishment or confirmation of the attribution of digital actions, rights or objects to a specific digital environment entity. Digital identity shall be subject to protection as a personal non-property asset.

2. No one may be compelled to undergo digital identification, except in cases, where such an obligation is expressly provided for by the laws of the Republic of Kazakhstan.

3. Participation in digital environment interactions without identification shall be permitted only with respect to services and actions that do not give rise to rights and obligations, whose exercise requires identification.

4. In the absence of digital identification possibility a digital environment subject has the right to receive state and other services stipulated by the laws of the Republic of Kazakhstan,

provided that they undergo identification by another method, established by the legislation of the Republic of Kazakhstan.

5. The State shall ensure protection of digital identity against unauthorized access to digital records that would allow identification of digital environment subjects without their consent.

Article 41. Right to deletion, anonymization and restriction of personal data processing

1. A personal data subject shall have the right to request deletion, anonymization, or restriction of processing of their personal data stored or processed in the digital environment, regardless of the ground for its receipt, except in cases stipulated by the laws of the Republic of Kazakhstan.

Anonymization of personal data refers to actions that make it impossible to determine the ownership of the personal data by the personal data subject.

2. The digital objects owner or another person processing personal data shall be obligated to comply with the personal data subject's request to erase, anonymize, or restrict the processing of personal data in accordance with the procedure, established by the legislation of the Republic of Kazakhstan on personal data and their protection.

3. If the legislation of the Republic of Kazakhstan establishes mandatory retention periods for digital data, the owner of the relevant digital object or another person processing the personal data shall be obligated to restrict access to such data and suspend its processing at the request of the personal data subject, with the exception of processing:

- 1) on the basis of a final and binding court order;
- 2) to fulfill obligations stipulated by the laws of the Republic of Kazakhstan or an agreement;
- 3) to ensure archival storage in accordance with the laws of the Republic of Kazakhstan.

4. A request to delete, anonymize, or limit the processing of personal data shall not be enforced, if the retention of the personal data is necessary for:

- 1) protection of life, health, rights, freedoms, and legitimate interests of third parties;
- 2) investigation of offenses;
- 3) administering of justice or enforcing of final and binding court rulings;
- 4) safeguarding the public interest, expressly established by the laws of the Republic of Kazakhstan;
- 5) the purposes of state statistics or scientific research, provided that the personal data are anonymized;
- 6) performance of state functions and provision of public services.

Article 42. Digital accessibility and the rights of persons with disabilities in the digital environment

1. State bodies, state legal entities, quasi-public sector entities and other entities, involved in the provision of public services shall ensure accessibility of digital systems, digital

resources and services in the digital environment for all categories of users, including persons with disabilities.

2. When creating, developing, modifying and operating digital assets, through which public services are provided, the requirements for ensuring accessibility of services in the digital environment, as stipulated by the uniform requirements in digitalization and cybersecurity, shall be taken into account.

The uniform requirements in digitalization and cybersecurity shall be developed and updated with regard to international approaches and recommendations in the digital environment accessibility.

Article 43. Rights of digital environment subjects in the use of algorithmic systems and fully automated decision making

1. An algorithmic system is a digital system that makes or influences decisions based on automated data processing, including artificial intelligence systems.

2. A decision made with the use of algorithmic decision-making systems must not result in discrimination, including discrimination on the grounds, established by the laws of the Republic of Kazakhstan.

3. A fully automated decision is the one, made without human involvement in assessing the circumstances or approving the result in cases, stipulated by the laws of the Republic of Kazakhstan or by agreement.

4. A data subject in respect of which a fully automated algorithmic system was applied shall have the right, in the cases and in the manner, prescribed by the legislation of the Republic of Kazakhstan:

- 1) to receive information regarding the use of the algorithmic system;
- 2) to receive an explanation of the key factors and criteria that influenced the decision, without disclosing the algorithms, source code or information, constituting a legally protected secret;
- 3) to request a review of the decision with the participation of an authorized specialist (specialists), if the decision entails legal consequences or is capable of affecting the rights and legitimate interests of an individual within the time frames, established by the legislation of the Republic of Kazakhstan.

5. The specifics of applying algorithmic systems and fully automated solutions shall be established by the legislation of the Republic of Kazakhstan.

SECTION 4. LEGAL RELATIONS IN DIGITAL ENVIRONMENT

Chapter 9. DIGITAL IDENTIFICATION

Article 44. Emergence, exercise and termination of rights in the digital environment

1. The grounds for the emergence, modification and termination of legal relations in the digital environment are legally significant facts expressed in digital records.

2. Legal relations in the digital environment arise due to the creation, receipt or use of digital objects and performance of actions, and also in other cases provided for by this Code.

3. Legal relations, arising in the digital environment are implemented using digital technologies that ensure the identification of participants, confirmation of their expression of will and recording of legally significant facts.

4. Termination of legal relations in the digital environment occurs as a result of the fulfillment of obligations, loss of a digital object, expiration of a right or other legally significant facts, established by this Code, other laws of the Republic of Kazakhstan or an agreement.

Article 45. Digital data identifiers

1. Identifiers and digital records containing them shall be processed in accordance with the legislation of the Republic of Kazakhstan on personal data and their protection with regard to the specifics, established by this Code.

2. Unique identifiers in the Republic of Kazakhstan shall be:

- 1) for individuals – an individual identification number;
- 2) for legal entities (branches and representative offices, and sole proprietors operating as joint ventures) – a business identification number.

3. Identifiers used in state digital objects, as well as identifiers used to exchange digital records between digital objects of different owners, are recognized as public identifiers.

4. Identifiers used exclusively in private digital resources or restricted digital systems are recognized as private identifiers.

5. The selection of an identifier for inclusion in a digital record is made:

- 1) by the personal data subject when collecting data about them by the owner of the digital records;
- 2) by the owner of the digital records when creating digital data by the owners themselves, including when creating or assigning an identifier;
- 3) by a third party when transferring digital data to the owner of the digital records, not received from the personal data subject.

6. The owner of the digital records shall be obligated to ensure uniqueness and consistency of the identifiers used within their digital object, as well as their correct matching when exchanging digital records between digital objects.

Article 46. Digital authentication

1. Digital authentication is defined as a procedure for verifying the identity of an individual or the legal capacity of a legal entity when accessing services and objects in the digital environment in cases, stipulated by the legislation of the Republic of Kazakhstan or by agreement of the parties.

2. Digital authentication shall be carried out using digital objects and identification tools that comply with the requirements of the legislation of the Republic of Kazakhstan on cybersecurity, personal data and their protection.

3. When applying for state services, digital authentication is recognized as an appropriate expression of the individual's will to receive the service, provided that it is performed in accordance with uniform requirements in digitalization and cybersecurity.

4. Digital authentication, performed with the use of multi-factor means, shall be the ground for creation, modification or termination of legal relations in the digital environment, and also for the purposes of proving legally significant actions, performed in digital format.

5. Digital records of digital authentication facts may not be deemed legally invalid solely on the grounds that they are presented in digital data form.

Article 47. Digital verification

1. Digital verification is an action by a digital environment subject, expressing consent or other expression of will, performed after digital authentication with the use of digital technologies.

2. Digital verification includes codes, passwords, one-time digital identifiers, push notifications, biometric verification, digital records in distributed ledgers and other means, generated and sent by digital systems to:

1) cellular subscriber devices, including those registered on the digital government's web portal;

2) instant messaging services;

3) email;

4) distributed digital objects and other systems.

3. Digital verification may be used by a digital environment subject in cases established by the laws of the Republic of Kazakhstan or by agreement of the parties.

4. Digital verification is not an electronic digital signature and does not ensure the authenticity and immutability of the content of a digital record.

Article 48. Biometric authentication

1. Biometric data used for digital authentication are recognized as personal data and shall be subject to protection under the Law of the Republic of Kazakhstan On Personal Data and Their Protection.

2. Every citizen of the Republic of Kazakhstan shall have the right to biometric registration for digital authentication purposes.

3. Mandatory processing of biometric data and biometric authentication shall be permitted only in cases, established by the laws of the Republic of Kazakhstan.

4. Biometric authentication is the process of matching and verifying the conformity of biometric data for the purpose of establishing identity.

5. Biometric authentication, as provided for by the laws of the Republic of Kazakhstan, shall be carried out with the use of the national biometric authentication system in the context of digitalization of the state body activities, including performance of state functions and

provision of state services in accordance with the rules for operating and connecting to the national biometric authentication system, approved by the authorized body, unless otherwise provided for in paragraph 6 of this article.

6. The procedure for conducting biometric authentication by financial and payment organizations, including cases of mandatory use and (or) filling the national biometric authentication system with biometric data, obtained by the identification data exchange center of the National Bank of the Republic of Kazakhstan, shall be determined by the authorized body for regulation, control and supervision of the financial market and financial organizations and the National Bank of the Republic of Kazakhstan.

7. The national biometric authentication system is a digital object of the digital government, intended for facial biometric authentication, the creation, development, support and system maintenance of which are carried out by the operator.

8. The provisions of this article shall not apply to relations, arising from the collection, processing and protection of biometric data in the course of intelligence, counterintelligence, operational investigative activities, as well as the implementation of security measures to ensure the safety of protected persons and objects.

Chapter 10. ELECTRONIC DIGITAL SIGNATURE

Article 49. Electronic digital signature

1. An electronic digital signature is a digital record (a set of digital data), created with the use of the private key of an electronic digital signature and electronic digital signature tools, confirming the authenticity of an electronic document, its ownership and immutability of its content.

2. An electronic digital signature shall be equivalent to the signatory's handwritten signature and shall have equal legal force provided the following conditions are met:

1) the authenticity of the electronic digital signature is confirmed using a public key that has a public key certificate for the electronic digital signature;

2) the person, who signed the electronic document is in lawful possession of the private key for the electronic digital signature;

3) the electronic digital signature is used in accordance with the information, specified in the public key certificate for the electronic digital signature;

4) the public key certificate for the electronic digital signature is issued by a certification authority, accredited in the Republic of Kazakhstan or by a foreign certification authority, registered with a trusted third party in the Republic of Kazakhstan.

3. An electronic digital signature, created with the use of a public key certificate for an electronic digital signature of a digital object shall be equivalent to the electronic digital signature of the owner of such digital object. The use of such an electronic digital signature

shall be permitted for the automatic signing of similar electronic documents that do not contain an expression of intent, aimed at establishing, amending or terminating civil rights and obligations.

Article 50. Electronic digital signature tools

1. Electronic digital signature tools refer to the combination of software and digital infrastructure objects, used to create and verify the authenticity of an electronic digital signature.

2. Electronic digital signature tools shall be subject to conformity assessment in the cases and the procedure established by the legislation of the Republic of Kazakhstan in technical regulation.

3. When generating an electronic digital signature, the software, using the electronic digital signature tools must ensure the following requirements are met:

1) the person, signing the electronic document is given the opportunity to review its contents before signing it;

2) the electronic digital signature is created only after explicit confirmation of the action to create it by the person, signing the document;

3) after signing the electronic document, a notification is generated regarding creation of the electronic digital signature and its application;

4) the information necessary to confirm the existence of the electronic digital signature at a specific point in time is ensured;

5) the person, signing the electronic document is given the opportunity to save the signed electronic document, except in cases, expressly provided for by the laws of the Republic of Kazakhstan.

4. When verifying an electronic digital signature, the software, using the electronic digital signature tools must:

1) ensure the retrieval of the contents of the electronic document;

2) provide information on the results of the electronic digital signature verification;

3) display the data of the public key certificate of the electronic digital signature, enabling identification of the owner of the private key, used to sign the electronic document.

5. The requirements of paragraphs 3 and 4 of this article shall not apply to electronic digital signature tools, used to create or verify electronic digital signatures of digital systems.

Article 51. Electronic digital signature keys

1. A public digital signature key is digital data, intended to verify the authenticity of an electronic digital signature.

2. A private digital signature key is digital data, intended to create an electronic digital signature with the use of electronic digital signature tools.

3. Private digital signature keys are the property of the persons who legally own them.

An individual may hold multiple public digital signature key certificates and corresponding private keys.

Transferring private keys to other persons, or using private keys by other persons is prohibited.

Private keys may be stored in a certification authority in accordance with the procedure, determined by the authorized body.

Chapter 11. CERTIFICATION AUTHORITIES AND ELECTRONIC DIGITAL SIGNATURE INFRASTRUCTURE

Article 52. Certification authority

1. A certification authority is a legal entity, established in accordance with the legislation of the Republic of Kazakhstan that verifies the authenticity of public key certificates for electronic digital signatures, as well as the ownership and validity of public keys for electronic digital signatures.

2. The root certification authority of the Republic of Kazakhstan is a certification authority that confirms the ownership and validity of public keys for electronic digital signatures of certification authorities.

3. A certification authority of state bodies of the Republic of Kazakhstan is a certification authority that provides electronic digital signature tools and public key certificates for electronic digital signatures to government officials for the generation and verification of electronic digital signatures in electronic documents in state and non-state digital systems.

4. The National certification authority of the Republic of Kazakhstan is the certification authority that provides electronic digital signature tools and electronic digital signature certificates to individuals or legal entities for the generation and verification of electronic digital signatures in electronic documents in government and non-government digital systems.

5. The operator shall perform the functions of the certification authority of state bodies of the Republic of Kazakhstan, the national certification authority of the Republic of Kazakhstan and the root certification authority of the Republic of Kazakhstan.

6. The authorized body shall coordinate the activities of the root certification authority of the Republic of Kazakhstan, the certification authority of state bodies of the Republic of Kazakhstan, the national certification authority of the Republic of Kazakhstan and the trusted third party of the Republic of Kazakhstan.

Article 53. Special certification authority

1. A Special certification authority is an authorized division of a state body of the Republic of Kazakhstan that certifies correspondence of a public key for an electronic digital signature to a private key for an electronic digital signature and carries out activities, related to the use of information, constituting state secrets.

2. A special root certification authority of the Republic of Kazakhstan is a certification authority that confirms the ownership and validity of public keys for electronic digital signatures of special certification authorities.

3. The National Security Committee of the Republic of Kazakhstan shall approve the rules for the issuance, storage and revocation of public key certificates for electronic digital signatures and for confirmation of the ownership and validity of a public key for an electronic digital signature by a special root certification authority of the Republic of Kazakhstan.

4. The National Security Committee of the Republic of Kazakhstan shall ensure implementation of the functions of the special root certification authority of the Republic of Kazakhstan.

5. Accreditation of a special root certification authority is the official recognition by the National Security Committee of the Republic of Kazakhstan of the special root certification authority's competence to carry out its activities.

6. Accreditation of special certification authorities shall be a mandatory requirement for special certification authorities (with the exception of the special root certification authority of the Republic of Kazakhstan) to carry out their activities within the territory of the Republic of Kazakhstan.

Article 54. Accreditation of the certification authority

1. Accreditation of a certification authority is an official recognition by the cybersecurity authority of the certification authority's competence to provide services.

2. Accreditation of certification authorities shall be a mandatory requirement for certification authorities (with the exception of the root certification authority of the Republic of Kazakhstan) to pursue their activities within the territory of the Republic of Kazakhstan. Accreditation shall be performed by the cybersecurity authority.

3. Accreditation of a certification authority is free of charge for a period of three years, unless a shorter period is specified in the certification authority's application in accordance with the rules for issuing and revoking certificates of accreditation for certification authorities , as approved by the authorized body.

Article 55. The functions of the certification authority

1. The certification authority shall perform the following functions:

- 1) issue electronic digital signature tools;
- 2) issue, store and revoke public key certificates for electronic digital signatures;
- 3) approve the policy for the application of public key certificates for electronic digital signatures;
- 4) provide gratuitously a timestamping service, confirming the point in time at which an electronic digital signature existed in an electronic document, in accordance with the rules for the generation and verification of the authenticity of electronic digital signatures, approved by the authorized body;
- 5) provide gratuitously the list of revoked public key certificates for electronic digital signatures and an online service for checking the revocation status of public key certificates for electronic digital signatures;

6) maintain records of current and revoked public key certificates for electronic digital signatures;

7) provide users' electronic digital signature certificates, and also information on their revocation to the root certification authority of the Republic of Kazakhstan;

8) revoke electronic digital signature certificates upon request from the owner, signed with the private key of the electronic digital signature, the electronic digital signature certificate of which was issued by the national certification authority of the Republic of Kazakhstan.

2. The certification authority shall take all necessary measures to prevent the loss, modification and forgery of public keys and private keys of electronic digital signatures in its custody.

3. The certification authority shall ensure the protection of information about the owners of electronic digital signature certificates and disclose it in cases, stipulated by the laws of the Republic of Kazakhstan.

4. For failure to fulfill the obligation, stipulated by paragraph 2 of this article, the certification authority shall bear liability established by the laws of the Republic of Kazakhstan.

5. The rules for issuing, storing and revoking public key certificates for electronic digital signatures, as well as for confirming the ownership and validity of a public key for electronic digital signatures by a certification authority shall be approved by the authorized body.

6. Copies of public key certificates for electronic digital signatures shall be stored in the relevant certification authorities in the manner determined by the authorized body.

7. The storage term of revoked public key certificates for electronic digital signatures in certification authorities shall be no less than five years from the revocation date.

8. Upon expiry of the period specified in paragraph 7 of this article, the revoked public key certificates for electronic digital signatures shall be transferred to archival storage in accordance with the procedure, established by the legislation of the Republic of Kazakhstan.

Article 56. Termination of the certification authority's operations

1. The certification authority's operations shall be terminated in accordance with the procedure, established by the legislation of the Republic of Kazakhstan.

2. In the event of a decision to terminate its operations, the certification authority shall notify all participants in the digital systems it services and the authorized cybersecurity body thereof ninety calendar days prior to the termination.

3. Upon termination of a certification authority's operations the public key certificates for electronic digital signatures, issued by it and the corresponding electronic digital signature keys, as well as information about the owners of the public key certificates for electronic digital signatures shall be transferred to other certification authorities in agreement with the owner of the public key certificate for electronic digital signatures.

4. Upon expiry of the term, specified in paragraph 2 of this article, the public key certificates for electronic digital signatures and the corresponding electronic digital signature keys that have not been transferred to other certification authorities, shall cease to be valid and shall be stored in accordance with the legislation of the Republic of Kazakhstan.

Article 57. Recognition of foreign electronic digital signature

1. A trusted third party of the Republic of Kazakhstan is a digital system that verifies the authenticity of foreign electronic digital signatures and electronic digital signatures, issued in the Republic of Kazakhstan within the framework of cross-border interaction.

2. The rules for the registration and termination of interaction between the certification authorities and trusted third parties of foreign countries and a trusted third party of the Republic of Kazakhstan shall be approved by the authorized body.

3. The rules for verifying the authenticity of an electronic digital signature by a trusted third party of the Republic of Kazakhstan shall be approved by the authorized body.

Article 58. Rights and obligations of the holder of a public key certificate of an electronic digital signature

1. A public key certificate of an electronic digital signature is a digital record, certified by the electronic digital signature of a certification authority, which serves to confirm the electronic digital signature's compliance with the requirements, established by this Code.

2. The holder of a public key certificate of an electronic digital signature is an individual or a legal entity, in whose name the public key certificate for an electronic digital signature was issued, who is a legal owner of the private key corresponding to the public key, specified in the public key certificate of an electronic digital signature.

3. The holder of a public key certificate of an electronic digital signature shall be entitled to request the certification authority to revoke the public key certificate of digital signature in accordance with this Code and the rules for issuing, storing and revocation of digital signature certificates by the certification authority, as approved by the authorized body.

4. The holder of a public key certificate of an electronic digital signature shall take measures to protect their private key digital signature against unauthorized access and use.

5. The private key and the corresponding public key certificate of an electronic digital signature, issued by the certification authority for the digital system are installed in the digital system, and its owner shall ensure its security, safe use and protection against unauthorized access.

Article 59. Revocation of a public key certificate of an electronic digital signature

1. The certification authority that issued the public key certificate of an electronic digital signature may revoke it based on a corresponding notification in the following cases:

1) at the request of the holder of the public key certificate of an electronic digital signature in the manner, determined by the certification authority;

2) upon establishing that false information or an incomplete set of documents was submitted, when obtaining the public key certificate of an electronic digital signature;

3) upon the death of the holder of the public key certificate of an electronic digital signature;

4) upon a change in the last name, first name, or patronymic (if indicated in the identity document) of the holder of the public key certificate of an electronic digital signature;

5) upon a change of management, name change, reorganization or liquidation of the legal entity that holds the public key certificate of an electronic digital signature;

6) by the final and binding court ruling.

2. The certification authority shall revoke the public key certificate of the electronic digital signature in the manner and within the timeframes, determined by the rules for issuing, storing and revoking the certificate of the electronic digital signature by the certification authority.

Article 60. Rejecting the issue of a public key certificate of an electronic digital signature

The certification authority shall reject the issue of a public key certificate of an electronic digital signature in the following cases:

1) incomplete documentation;

2) submission of false information;

3) entry of a court order into force;

4) the person has not reached the age of sixteen.

Article 61. Generation and verification of an electronic digital signature

1. The generation and verification of an electronic digital signature shall be carried out in accordance with the rules for the generation and verification of an electronic digital signature.

2. The authority to sign on behalf of a legal entity (branches and representative offices) is verified by the digital system in which the signing is performed, using the authority verification service of the root certification authority of the Republic of Kazakhstan.

3. To ensure trust and uniformity of electronic document verification the authorized body shall provide an electronic document verification service.

4. A digital system, in which electronic documents are signed using an electronic digital signature, enables verification of such signatures through an open service, provided by the system owner.

5. If in accordance with the regulatory legal acts of the Republic of Kazakhstan a document, signed by a legal entity (branch and representative office) is subject to certification by a seal, an electronic document, certified by an electronic digital signature of an employee of a legal entity, authorized to sign such a document in accordance with the legislation of the Republic of Kazakhstan, shall be recognized as equivalent to a paper document, signed by hand and certified with a seal.

Chapter 12. DOCUMENTS IN THE DIGITAL ENVIRONMENT

Article 62. An electronic document

1. A digital record, whose authenticity, ownership, and immutability are confirmed by an electronic digital signature, shall be recognized as an electronic document.

An electronic document must be capable of being circulated and stored outside the digital system, in which it was created, without altering its properties.

2. An electronic document that complies with the requirements of this Code and is certified by an electronic digital signature of the person, authorized to sign it, shall be equivalent to a signed paper document.

3. Electronic documents shall be generated, stored and presented through state and (or) non-state digital systems, as well as outside of them, in accordance with the procedure established by the legislation of the Republic of Kazakhstan.

4. The procedure for collecting, processing, storing, transmitting, searching, distributing, using, protecting, registering, confirming and destroying electronic documents and other data, containing information, constituting state secrets, using secure digital systems classified as state secrets, as well as the procedure for establishing, accrediting and terminating the activities of a special certification center, shall be determined by the National Security Committee of the Republic of Kazakhstan.

5. Electronic documents of state bodies shall be transferred for state storage to digital archives in accordance with the procedure, established by the legislation of the Republic of Kazakhstan.

6. The head of a legal entity or a person replacing him shall have the right to delegate authority to an employee of the said legal entity or a person designated by them to sign electronic documents. In this case each employee uses a public key certificate for an electronic digital signature, issued in his name, and the corresponding private key for an electronic digital signature.

Article 63. Digital documents

1. A digital document is an intangible digital presentation of authentic information, generated in a digital environment on the basis of the data, contained in the national registries at the time of a request or presentation.

2. A digital document confirms the legally significant facts and information contained therein that are necessary for receiving government and other services, making transactions or engaging in other legal relations.

3. A digital document shall be certified by an electronic digital signature of the relevant state body in cases, where it is subject to presentation or verification by third parties.

4. The digital document service operator is responsible for correct formation and technical integrity of the digital document, when it is presented.

5. When receiving payment and financial services the digital identity documents are used by financial and payment institutions and are presented to them through the digital document service upon personal request (presence) of individuals.

Article 64. Digital data

1. Digital data refer to the data contained in national registries and other state digital resources, used to verify facts, rights and obligations without the need to issue a separate document.

2. The use of digital data in legal relations shall be equivalent to the presentation of a digital document, if its authenticity can be verified at the time of presentation through a digital document service.

3. State bodies and other entities with access to national registries are required to obtain the necessary information directly from reference data sources without requesting documents from an individual, if the national registries contain such data.

4. Third-party access to digital data through the digital document service is granted with the user's consent in accordance with the procedure, established by the authorized body, with mandatory protection of personal data.

Article 65. Digital archive

1. A digital archive is a collection of electronic archival records and electronic copies of archival records, organized and stored in electronic form in accordance with the procedures, established by the authorized body in archival affairs and administrative documentation management.

2. The digital archive operates to preserve the cultural heritage of the people of Kazakhstan.

3. The digital archive ensures accessibility, preservation, integrity and confidentiality of the stored information in accordance with the requirements of the legislation of the Republic of Kazakhstan.

4. The procedure for the operation of the digital archive shall be determined by the authorized body in archival affairs and administrative documentation management in consultation with the cybersecurity authority.

5. The storage, use and destruction of electronic documents and digital objects shall be carried out in accordance with the procedure, determined by the authorized body in archival affairs and administrative documentation management.

Article 66. Notification of digital entities

1. Digital environment entities shall be notified digitally through the single notification point.

2. The single notification point is a state digital facility that enables targeted delivery of notifications from state bodies to digital entities, mobile subscriber devices, and (or) email, including when providing state services and which ensures guaranteed delivery and storage of information regarding delivery status.

3. Notifications from the single notification point are deemed delivered if there is information confirming their proper delivery.

Article 67. Smart contracts

1. A smart contract is an agreement providing for an automatic execution of the terms previously agreed by the parties upon the occurrence of certain circumstances through the use of digital technologies.

2. By agreement of the parties all or part of the terms of a smart contract may be expressed in software code, provided that such code allows for the unambiguous determination of the parties' rights and obligations and ensures the ability to reproduce the terms in a form accessible to human perception.

3. A smart contract must provide for a dispute resolution procedure between the parties, under which the final decision on the dispute is made by a human in accordance with the procedure, established by the legislation of the Republic of Kazakhstan or by agreement of the parties.

4. Parties to legal relations have the right to use insurance and other mechanisms to protect against risks, associated with a technical error, software malfunction or digital platform failure, resulting in non-fulfillment or improper fulfillment of obligations under the smart contract.

5. Requirements regarding the use of smart contracts in specific activity areas shall be established by this Code and (or) the laws of the Republic of Kazakhstan.

SECTION 5. DIGITAL PUBLIC ADMINISTRATION Chapter 13. DIGITAL ARCHITECTURE OF THE STATE

Article 68. Digital architecture of the state

1. Digital architecture of the state is a comprehensive description of digital objects and digital data, created and used to achieve state objectives, as well as the tasks, functions and public administration processes by industry (sphere), formalized and presented in digital format to ensure the coordinated development, integration and standardization of digital solutions.

2. Digital architecture of the state (including the architecture of the digital government) includes:

1) architectural principles for the construction and development of digital objects (digital systems and digital platforms);

2) requirements for the integration and compatibility of digital systems, including standardized interaction interfaces;

3) requirements for an architecture ready for deployment in a cloud infrastructure (cloud readiness);

4) requirements for a service architecture that ensures modularity, component reuse and interoperability;

5) requirements for a digital data architecture that ensures the quality, compatibility, security and rational use of the digital data;

6) requirements for architectural security and resilience, including digital data protection, cybersecurity and resilience to cyber threats.

3. State bodies, state legal entities, quasi-public sector entities, legal entities, whose fifty or more percent of the voting shares (equity interests) are directly or indirectly held by quasi-public sector entities, as well as other organizations, involved in the performance of state functions and the provision of state services, are required to comply with the rules for the formation, development and monitoring of the digital architecture of the state, approved by the authorized body.

Article 69. Digital government architecture

1. Digital government is a system of digital interaction between state bodies, and also with individuals and legal entities, based on the integrated use of digital technologies.

2. Digital government operates on the basis of the digital government architecture.

3. The formation, implementation monitoring and development of the digital government architecture shall be carried out in accordance with the uniform requirements in digitalization and cybersecurity and the rules for the formation, development and monitoring of the state's digital architecture.

Article 70. Smart cities and smart regions

1. Smart cities and smart regions are cities and regions, whose governance, infrastructure and service delivery are organized on the basis of digital data and artificial intelligence through digital infrastructure.

2. Development of smart cities and smart regions shall be carried out in accordance with the state's digital architecture and the methodology for building "smart cities" and "smart regions," as approved by the authorized body.

Article 71. Architectural portal of state digital objects

1. The architectural portal of state digital objects is a digital object, intended for recording, storing and systematizing information about digital state objects, the state's digital architecture and platform software products for subsequent use by state bodies for monitoring, analysis and planning in digitalization area.

2. State bodies, state legal entities, quasi-public sector entities, legal entities, whose fifty percent or more of the voting shares (equity interests) are directly or indirectly held by quasi-public sector entities, as well as other organizations, involved in the performance of state functions and provision of state services, shall post information about digital objects and their technical documentation on the architectural portal of state digital objects, maintain records of them and update them as required by the rules for the formation, development and monitoring of the state's digital architecture.

3. The list of technical documentation for a digital object shall be determined by the rules for the formation and monitoring of the performance of the state's digital architecture.

Technical documentation is a set of documents for a digital object, based on which the creation and development of the digital object, as well as its pilot and industrial operation, are carried out.

4. The state's architectural portal for digital objects operates on the digital infrastructure located within the Republic of Kazakhstan.

Article 72. Architectural coordination center

1. The architectural coordination center is a legal entity, designated by the Government of the Republic of Kazakhstan.

The architectural coordination center ensures integrity, compatibility and efficacy of the digital architecture of state bodies, state legal entities, entities of the quasi-public sector and legal entities, whose fifty or more percent of the voting shares (equity interests) are directly or indirectly held by quasi-public sector entities, as well as other organizations involved in public administration processes.

2. The architectural coordination center shall:

1) participate in the implementation of state policy in digitalization and artificial intelligence;

2) form, develop and monitor the performance of the digital architecture of the state in accordance with the rules for the formation, development and monitoring of the digital architecture of the state;

3) provide organizational and methodological support for the development of the digital architecture of the state and the digital transformation of public administration;

4) carry out expert assessments of process reengineering;

5) develop methodology for the construction of smart cities and smart regions;

6) conduct an expert review of investment proposals, feasibility study for budget investments, and technical assignment for the creation and development of digital government's digital objects;

7) issue expert opinions to the authorized body on the calculation of expenses for public procurement of goods, works and services in digitalization;

8) support assessment of the efficacy of state bodies in the application of digitalization and assessment of the public service delivery automation;

9) manage projects for the creation and development of digital objects of the digital government, and also projects for the implementation of strategic and program documents;

10) provide consulting, methodological, and practical assistance to state bodies in the creation and development of digital objects of the digital government, management of digital data, artificial intelligence and project management within the framework of implementing the documents of the State Planning System of the Republic of Kazakhstan;

11) record information on digital objects of the digital government and technical documentation on the architectural portal of digital objects of the state;

12) analyze the integration of digital objects of the digital government to identify incomplete and outdated information contained therein and develop recommendations for their elimination;

13) ensure compliance with uniform requirements in digitalization and cybersecurity.

14) participate in the development of standardization documents in the artificial intelligence;

15) analyze data, including open data, generated by state bodies, state legal entities, quasi-public sector entities, legal entities, whose fifty percent or more of the voting shares (equity interests) are directly or indirectly held by quasi-public sector entities, and also other organizations;

16) organize the creation and development of digital objects according to the service model of digitalization.

Chapter 14. DIGITAL GOVERNMENT

Article 73. Digitalization of state bodies' activity

1. Digital objects of the digital government include digital objects of state bodies and other entities, intended for the implementation of state activities, performance of state functions and provision of state services.

2. Digitalization shall be understood to mean a set of measures, aimed at digitizing processes and applying digital technologies to automate the activities of state bodies, organizations and citizens.

3. Digitalization of a state body's activity, including state functions and provision of state services is implemented through:

1) creation, development, and acquisition of digital objects of the digital government;

2) development and deployment of platform software products in accordance with the state's digital architecture and with regard to the conducted process reengineering;

3) acquisition of digital services using a service-based digitalization model.

A service-based digitalization model is understood as a method of providing digital services on the terms of access to digital solutions or in a service format without the need for the state body to independently develop them, including with the possibility of subsequently transferring such solutions to the state body's balance sheet in accordance with the legislation of the Republic of Kazakhstan.

4. Digital assets of the digital government are subject to systematization through their identification, categorization and description in a classifier of digital assets of the digital government, compiled by the authorized agency.

Article 74. Digital government operator

1. The operation of digital objects of the digital government shall be provided by the operator, a legal entity assigned by the Government of the Republic of Kazakhstan.

2. The operator shall:

1) provide system and technical maintenance and support for digital infrastructure assets of the digital government in accordance with the list and rules for its formation approved by the authorized body;

2) provide digital services to state bodies and quasi-public sector entities in accordance with the list approved by the authorized body;

3) develop platform software products for state bodies and quasi-public sector entities;

4) ensure a secure storage of state digital resources, hosted on the digital government platform and in the digital infrastructure of the digital government, during their storage and processing in accordance with the legislation of the Republic of Kazakhstan on cybersecurity;

5) render services in the provision of the digital government platform for development, advancement and deployment of digital objects and (or) platform software products;

6) integrate and connect the digital government's digital objects to the digital government gateway and the national gateway of the Republic of Kazakhstan, and also connect the state bodies' digital objects to the digital infrastructure of the digital government;

7) provide connection services and communication services of the uniform transport environment to digital environment entities, determined by the authorized body for the operation of their digital resources and digital systems.

To provide communication services it has the right to engage other persons as subcontractors (co-contractors) for such services;

8) create and develop the digital government platform and the unified transport environment of state bodies;

9) provide support and system and technical maintenance, manage projects for the development of the national gateway of the Republic of Kazakhstan;

10) collect, process, store and transmit digital data and digital records on the digital government platform in accordance with data management requirements.

11) engage other entities' digital infrastructure facilities to develop the digital infrastructure of the digital government, as well as other entities to provide support and system and technical maintenance for the state bodies' digital facilities;

12) collect, process, store and transmit digital data and digital records for data analytics in accordance with data management requirements, and also transmit digital data and digital records to the digital government platform;

13) provides digital infrastructure services for the provision of information, reference and consulting services to legal entities;

14) provide data analytics services in accordance with data management requirements;

15) on the basis of information, received from the personal data protection authority, notify personal data subjects about a breach of personal data security or about processing of personal data by sending information to their personal account on the digital government web portal, the digital government mobile application and (or) to their mobile subscriber number in the form of a short text message.

Article 75. Digital government web portal

1. The digital government web portal is a digital object that represents a single window for access to consolidated information, posted by state bodies and other entities, providing state services, including the regulatory framework, and also to government and other services provided in electronic form.

2. On the digital government web portal interaction between individuals and legal entities with service providers regarding the government services, applications to entities reviewing requests from said individuals, and also the use of personal data are carried out through a personal account.

3. State bodies and other entities, involved in the state services shall provide the operator with the digital data and digital records necessary for the information content of the digital government web portal.

4. Requirements for the content, maintenance and information content of the digital data and digital records of the digital government web portal shall be established by the authorized body.

5. State and other services shall be rendered through the digital government web portal, the digital government mobile application and (or) a subscriber's cellular device.

6. State services shall be rendered in the manner prescribed by the legislation of the Republic of Kazakhstan on government and socially responsible services with mandatory access to them via the digital government web portal and (or) the digital government mobile application.

7. If other services provided electronically meet the criteria, established in accordance with the procedure, determined by the authorized body, mandatory access to such services shall be ensured through the digital government web portal and (or) the digital government mobile application.

8. Registration and linking of a mobile network subscriber number, provided by a mobile network operator to an account on the digital government web portal for the purpose of receiving state and other services in electronic form via a mobile device shall be carried out in accordance with the procedure, determined by the authorized body.

9. To receive state and other services via the digital government web portal and a mobile device, the mobile phone number registered in the database of mobile citizens of the Republic of Kazakhstan is used.

The database of mobile citizens is a digital resource containing the mobile phone numbers of digital government users.

Article 76. Digital event

1. A digital event is a circumstance, recorded in digital form resulting from the actions of a digital environment subject or the operation of a digital object and reflects their interaction parameters in the digital environment.

2. Data on digital events is stored during the operation of digital objects and shall be used to ensure their functioning for the provision of services and operation logging, taking into account technical features and limitations.

3. Processing of data on digital events shall be permitted in cases, established by the laws of the Republic of Kazakhstan:

to confirm legal facts;

to ensure the security of the digital environment.

Article 77. Digital space of a citizen of the Republic of Kazakhstan

1. The digital space of a citizen of the Republic of Kazakhstan is a section of the personal account on the digital government web portal that provides access to information about recorded digital events, their viewing, management and use.

2. The operator shall ensure confidentiality, integrity and control by the citizen of the Republic of Kazakhstan of the use of digital events, contained in the digital space.

3. Requirements for the digital space of a citizen of the Republic of Kazakhstan are determined by the authorized body.

4. When requesting digital data of a citizen of the Republic of Kazakhstan from the digital government's digital objects, the digital objects through which the request is made, must generate a digital event regarding the use of such data and transmit it to the digital space of the citizen of the Republic of Kazakhstan.

Article 78. Open government

1. Open government is a digital entity providing access to information about government activities and citizen participation in discussions and decision-making through interconnected open data internet portals, open budgets and open regulatory legal acts.

2. Information shall be posted on the open data internet portals in accordance with this Code and the legislation of the Republic of Kazakhstan on access to information.

Article 79. Uniform platform for government digital resources

1. The uniform platform for government digital resources is a digital platform designed to host government digital resources.

2. State bodies are required to publish digital resources on the uniform platform of the state bodies' digital resources and to ensure accuracy and timeliness of their content in accordance with the laws of the Republic of Kazakhstan on access to information.

Article 80. Payment gateway of the digital government

1. The digital government's payment gateway is a digital object that automates the transfer of payment information on the provision of paid services.

2. The digital government's payment gateway ensures:

1) the transfer of payment requests;

2) notification of payment for the service.

3. Second-tier banks, payment organizations, and organizations that perform certain types of banking operations, when participating in the processes of accepting and processing

payments for the provision of services, shall ensure integration of their own digital objects, involved in these processes with the digital government's payment gateway, either directly or through the facility of the national center for managing the national digital financial infrastructure.

Article 81. Unified transport environment of state bodies

1. The unified state bodies' transport environment is a telecommunications network that is part of the digital government infrastructure and is designed to ensure the interaction of local (excluding local networks with internet access), departmental, and corporate telecommunications networks of state bodies, their subordinate organizations and local governments, and also other digital environment entities, determined by the authorized body, while maintaining the required cybersecurity level.

2. State bodies, their subordinate organizations and local governments, as well as other digital environment entities, determined by the authorized body, are required to use exclusively the uniform transport environment of state bodies for the interaction of local (excluding local networks with internet access), departmental and corporate networks.

3. To ensure cybersecurity the connection of local, departmental and corporate networks, connected to the uniform transport environment of state bodies, to public telecommunications networks and other telecommunications networks shall be carried out in accordance with uniform digitalization and cybersecurity requirements.

Article 82. Digital government platform

1. The digital government platform is an operator's digital platform designed for the development, advancement, deployment, and integration of platform software products and (or) deployment of digital assets.

2. Software developed and deployed on the digital government platform constitutes a platform software product.

3. The operator has the right to provide the platform software product through the provision of digital services.

A digital service includes services for the rental (lease, temporary use) and (or) deployment of computing resources and provision of software, software products, technical equipment for use, including communication services, which enable the operation of these services through a digitalization service model, in accordance with the rules for the creation, development and deployment of digital assets.

4. Digital objects implementing state functions and the resulting state services shall be developed and hosted on the digital government platform in accordance with the rules for implementing the stages of the digital government object's life cycle, approved by the authorized body in coordination with the authorized state planning body, and also transfer digital data to the digital government platform in accordance with data management requirements.

5. Ownership of the digital government platform does not create ownership rights to digital data and records created with its use and (or) hosted on it, which belong to other owners and (or) holders, unless otherwise provided by the legislation of the Republic of Kazakhstan or an agreement between them.

6. The use of digital records, hosted on the digital government platform, in the digitalization of state bodies' activities, including their government functions and provision of state services, as well as the operator's data analytics, shall be carried out without the consent of their owners and (or) holders of the digital data, in compliance with the requirements of the legislation of the Republic of Kazakhstan on personal data and their protection and other legislation of the Republic of Kazakhstan.

7. The digital government platform shall operate on a digital infrastructure, located within the territory of the Republic of Kazakhstan.

Article 83. Integration of digital objects

1. Integration of digital objects shall mean measures to organize and ensure interaction between digital objects through integration services by means of standard data transfer protocols.

2. Integration services shall mean functional digital objects that enable interaction, data exchange and execution of coordinated operations between digital objects through standard interfaces, protocols and access mechanisms, defined by the authorized body.

3. Integration of digital objects of the digital government is effected through the digital government's gateway in accordance with the rules for the integration of digital objects of the digital government, approved by the authorized body in consultation with the cybersecurity authority and the National Security Committee of the Republic of Kazakhstan, subject to compliance with the cybersecurity and personal data protection requirements, established by the legislation of the Republic of Kazakhstan.

4. Integration of non-governmental digital objects with digital objects of the digital government, including on a fee basis, is effected through the digital government's external gateway in accordance with the rules for the integration of digital objects of the digital government, subject to the cybersecurity and personal data protection requirements, established by the legislation of the Republic of Kazakhstan.

5. The digital government gateway is a digital object designed to integrate digital objects of the digital government with other digital objects.

6. The digital government external gateway is a subsystem of the digital government gateway to facilitate the interaction of digital objects, located in the uniform transport environment of state bodies, with digital objects, located outside the uniform transport environment of state bodies.

The operating rules and technical requirements for the digital government external gateway shall be approved by the authorized body in consultation with the cybersecurity authority.

7. The National gateway of the Republic of Kazakhstan is a digital object designed to facilitate international (interstate) information interaction of digital objects.

8. International (interstate) information interaction using digital technologies shall be carried out through the National gateway of the Republic of Kazakhstan.

9. The list of digital objects through which international (interstate) information interaction is carried out via the National gateway of the Republic of Kazakhstan shall be approved by the authorized body.

Chapter 15. LIFE CYCLE OF A DIGITAL OBJECT

Article 84. Life cycle of digital government's digital object and its stages

1. The life cycle of a digital government's digital object is a set of stages of planning, creation, pilot operation, cybersecurity compliance testing, commissioning, development, decommissioning, modification, archiving and decommissioning of a digital government's digital object, aimed at ensuring its effective operation.

2. The life cycle of a digital government's digital object may include all or some of these stages, depending on the type of digital object and its operational characteristics in accordance with the rules for implementing the stages of the digital government object's life cycle.

Article 85. Planning, creation and development of a digital government digital object

1. Planning is an initial stage of the digital object's life cycle, which includes a range of activities to justify the need for its creation and define the objectives, requirements, resources and implementation conditions.

Planning of a digital government object involves process reengineering, which comprises analysis of current processes, a digital review of regulatory legal acts and design of new processes and is carried out in accordance with digital transformation rules, approved by the authorized body.

2. When planning, creating and developing digital objects of the digital government it is necessary to obtain an opinion from the authorized body and the cybersecurity authority on the developed regulatory and technical documentation, also on the calculation of costs for public procurement of goods, works and services in digitalization in accordance with the rules for implementing the stages of the life cycle of the digital object of the digital government.

3. Creation and development of digital objects shall be carried out in accordance with regulatory and technical documentation (state investment project, technical specifications, software product requirements specification, also public-private partnership project documentation) in accordance with the digital and budgetary legislation of the Republic of Kazakhstan.

4. Development of a digital object of the digital government shall be carried out after its commissioning.

5. This article does not apply to digital objects of the national security bodies of the Republic of Kazakhstan.

Article 86. Conducting trial operation and testing of the digital government object

1. The trial operation of the digital government's digital object shall be conducted in accordance with uniform requirements in digitalization and cybersecurity, including:

- 1) documenting of the trial operation procedures;
- 2) optimizing and eliminating any identified defects and deficiencies, followed by their correction;
- 3) issuing a certificate of completion of the trial operation.

The trial operation period shall not exceed one year.

2. Testing of the digital government digital object for compliance with cybersecurity requirements shall be conducted in accordance with this Code and the legislation of the Republic of Kazakhstan on cybersecurity.

Article 87. Commissioning of digital government digital object

1. The digital government digital object shall be commissioned in accordance with the requirements of regulatory and technical documentation, subject to successful completion of pilot operation with involvement of the authorized body and the cybersecurity authority.

2. During the commercial operation of the digital government digital object the following shall be ensured:

- 1) compliance with uniform requirements in digitalization and cybersecurity;
- 2) safety, protection and restoration of digital resources in the event of failure or damage;
- 3) backup and monitoring of the timely updating of digital resources;
- 4) automated recording, storage and periodic archiving of information about access to the state body's digital system;
- 5) maintenance of the digital government digital object;
- 6) technical support for the licensed software used by the digital facility of the digital government;
- 7) systems and technical maintenance;
- 8) reduction (or elimination) of the use of paper documents, as well as requirements for their submission, when performing state functions and providing state services;
- 9) warranty service by the supplier of the digital government's digital object, including elimination of errors and defects, identified during the warranty period. Warranty service shall be provided for at least one year from the date of commissioning of the digital government object.

Article 88. Modification of digital government digital object

1. Modification of a digital government digital object refers to work that does not require development of an investment proposal or a feasibility study for budgetary investments in accordance with the budget legislation of the Republic of Kazakhstan, provided that the total cost of the modification does not exceed twenty percent of the initial estimated cost of the

digital government object, established by the state investment project at the time of its creation.

2. Modification of a digital government digital object may be carried out if the following conditions are met:

1) the modification complies with the technical specifications or amendments to the technical specifications;

2) the work performed complies with cybersecurity requirements, established by the legislation of the Republic of Kazakhstan;

3) the authorized body's consent to the modification.

Article 89. Termination of commercial operation of digital government's digital object

1. Cessation of the need for further use of a digital government's digital object entails termination of commercial operation and modification of information about the digital government object on the digital objects' architecture portal in accordance with uniform requirements in digitalization and cybersecurity.

2. The decision on cessation of the need for further operation of a digital government digital object shall be made by the owner and (or) holder in consultation with the authorized body, with notification of the owners and (or) holders of the digital objects, with which the digital government object is integrated.

Article 90. Archiving and decommissioning of digital government's digital object

1. Digital records, technical documentation, source codes and (or) digital government digital objects shall be archived in accordance with the rules for implementing the life cycle stages of the digital government digital objects.

2. In the event that a previously created digital object is replaced by platform software products, developed on the digital government platform and performing all (or more) of its functions, such a digital object may be subject to decommissioning.

3. Decommissioning of digital government digital objects shall be carried out in accordance with the requirements, established by the budget legislation of the Republic of Kazakhstan, pursuant to a decision, adopted by the owner in consultation with the authorized body.

Article 91. Technologically complex digital objects of the digital government

1. Digital objects of the digital government, possessing special architectural and technological characteristics that necessitate the establishment of special requirements for their design, development, modernization, implementation, integration and operation, are classified as technologically complex digital objects of digital government.

2. The criteria for classifying objects as technologically complex digital objects of the digital government shall be determined by the authorized body.

3. The specifics of the creation and development of technologically complex digital objects of the digital government shall be regulated by the digital and budgetary legislation of the Republic of Kazakhstan.

Article 92. The procedure for creation and development of digital objects of the national security bodies of the Republic of Kazakhstan

Digital objects, intended to fulfill the tasks of the national security bodies of the Republic of Kazakhstan, shall be created or developed in the following order:

- 1) adoption of a decision to create or develop a digital object;
- 2) developing technical specifications for the creation or development of a digital object;
- 3) developing technical specifications and cost estimates for the procurement of goods, works and services in digitalization or performance of work without allocation of budgetary funds;
- 4) public procurement of goods, works and services in digitalization or performance of work without allocation of budgetary funds;
- 5) development, pilot operation, implementing and commissioning of the digital object in accordance with the effective standards in the Republic of Kazakhstan.

Expenses for the creation and development of digital objects of the national security bodies of the Republic of Kazakhstan shall be planned based on the conclusion of an ad hoc expert council (independently by the budget program administrator).

Chapter 16. DIGITAL TRANSFORMATION

Article 93. Digital transformation

1. Digital transformation is a process of system changes, based on the implementation of digital technologies, architectural and platform solutions, data analytics and artificial intelligence, with the aim of enhancing the efficacy, transparency and proactivity of management and service delivery.

2. Digital transformation shall pursue:

- 1) improving the interaction channels between digital entities by reducing the number of processes;
- 2) decision making based on data analytics;
- 3) maximizing the transition of public services to proactive services;
- 4) ensuring accessibility, resilience and inclusiveness of digital objects while respecting digital rights and protecting personal data.

3. State bodies, state legal entities and quasi-public sector entities are required to develop, approve, and implement digital transformation programs for their operations, including internal processes.

4. The digital transformation of state bodies, state legal entities and quasi-public sector entities includes upgrade of digital infrastructure facilities and transition to platform solutions, based on the digital government architecture and is carried out in accordance with the rules for the digital transformation of public administration.

5. Cross-sector coordination of the digital transformation of state bodies, state legal entities and quasi-public sector entities shall be performed by the authorized body.

Article 94. National Institute for digital development

1. The National Institute for digital development shall be determined by the Government of the Republic of Kazakhstan with the aim of creating enabling conditions for enhancing competitiveness of the digital environment.

2. The National Institute for digital development shall:

1) implement state support measures in accordance with the Entrepreneur Code of the Republic of Kazakhstan;

2) provide analytical and consulting services in digitalization, and also issue recommendations in digitalization;

3) cooperate with international organizations and foreign legal entities to promote digitalization;

4) analyze development of the digitalization sector;

5) perform other functions provided for by other laws of the Republic of Kazakhstan, decrees of the President of the Republic of Kazakhstan and resolutions of the Government of the Republic of Kazakhstan.

Article 95. Digital development index

1. Digital development index is a complex indicator of the level of institutional, technological and process readiness for the implementation, use and development of digital technologies by state bodies, state-owned legal entities and quasi-public sector entities.

2. The digital development index shall be determined annually as part of the annual performance assessment of central state and local executive bodies of oblasts, cities of national status and the capital.

3. The methodology for determining the digital development index shall be approved by the authorized body in consultation with the Supreme Audit Chamber of the Republic of Kazakhstan.

SECTION 6. SECURITY AND INTERNATIONAL COOPERATION IN DIGITALIZATION

Chapter 17. STATE SUPERVISION AND RISK MANAGEMENT IN THE DIGITAL ENVIRONMENT

Article 96. State supervision in digitalization, and also in the electronic documents and electronic digital signatures

1. State supervision in digitalization shall be carried out in the form of inspections, preventive control with a visit to the subject (object) of control, and preventive control without a visit to the subject (object) of control, unless otherwise provided in paragraph 4 of this article.

2. Inspections and preventive control with a visit to the subject (object) of control shall be carried out pursuant to the Entrepreneur Code of the Republic of Kazakhstan.

3. Preventive control without a visit to the subject (object) of control shall be carried out pursuant to the Law of the Republic of Kazakhstan On Cybersecurity and the Entrepreneur Code of the Republic of Kazakhstan.

4. State supervision of electronic documents and electronic digital signatures shall be carried out in the form of unscheduled inspections and preventive controls with a visit to the subject (object) of supervision pursuant to the Entrepreneur Code of the Republic of Kazakhstan, unless otherwise provided in the second part of this paragraph.

With respect to state bodies the state supervision of electronic documents and electronic digital signatures shall be pursuant to the Law of the Republic of Kazakhstan On Cybersecurity.

The requirement of this paragraph shall not apply to the National Bank of the Republic of Kazakhstan and its subordinate organizations and legal entities, whose fifty or more percent of the voting shares (interests in the authorized capital) are owned by the National Bank of the Republic of Kazakhstan or are held in trust by it, and also special state bodies of the Republic of Kazakhstan.

Article 97. Cybersecurity

1. Cybersecurity is security of the digital objects against violation of their confidentiality, integrity or availability.

2. Protection of digital objects shall be implemented by the owners and (or) holders of digital objects.

3. Measures for protecting digital objects shall be determined by the Law of the Republic of Kazakhstan On Cybersecurity, uniform requirements in digitalization and cybersecurity, and also other laws of the Republic of Kazakhstan.

Article 98. Providing digital data security

1. Digital data security shall be provided through a combination of technical, organizational, legal, and other measures aimed at preventing, detecting and eliminating cyber threats.

2. Technical protection measures include cryptographic and other information protection means.

3. The procedure for applying technical protection measures, their certification and conformity assessment shall be determined by the legislation of the Republic of Kazakhstan on cybersecurity and the legislation of the Republic of Kazakhstan in technical regulation.

Article 99. Testing and auditing of digital objects for compliance with cybersecurity requirements

1. Testing of digital objects for compliance with cybersecurity requirements shall be conducted on a mandatory basis or at the initiative of the owner and (or) holder of the digital object.

2. Digital objects subject to mandatory testing for compliance with cybersecurity requirements and also such testing procedure shall be determined by the Law of the Republic of Kazakhstan On Cybersecurity.

3. Testing of digital objects for compliance with cybersecurity requirements at the initiative of owners and (or) holders shall be conducted in accordance with this Code, the Law of the Republic of Kazakhstan On Cybersecurity and the legislation of the Republic of Kazakhstan in technical regulation.

4. Audits of digital objects for compliance with cybersecurity requirements shall be conducted at the initiative of their owner and (or) holder in accordance with the legislation of the Republic of Kazakhstan on cybersecurity, unless otherwise provided by the laws of the Republic of Kazakhstan.

Article 100. Quality audit of digital objects

1. A quality audit of digital objects shall be conducted to assess their functionality and digital architecture.

2. During the creation, implementation and operation of digital objects a quality audit may be conducted at the initiative of the owner and (or) holder of the digital objects.

3. A quality audit of digital objects shall be conducted by independent individuals and (or) legal entities, possessing specialized knowledge and expertise in accordance with the procedure, established by the authorized body.

4. A quality audit of artificial intelligence systems shall be conducted with regard to the assessment of the quality and legality of the use of data libraries, used to train artificial intelligence models, as well as the presence of prohibited functional capabilities of artificial intelligence systems in accordance with the Law of the Republic of Kazakhstan On Artificial Intelligence.

5. Quality audits of secure versions of digital objects, classified as state secrets shall not be conducted.

Chapter 18. GOALS, PRINCIPLES, MAIN DIRECTIONS OF THE INTERNATIONAL COOPERATION OF THE REPUBLIC KAZAKHSTAN IN DIGITALIZATION

Article 101. Objectives of International Cooperation of the Republic of Kazakhstan in Digitalization

The objectives of international cooperation in digitalization shall be recognized as mutual assistance and coordination of joint actions between the Republic of Kazakhstan and other states and international organizations on digital technology development issues.

Article 102. Principles of International Cooperation of the Republic of Kazakhstan in Digitalization

1. Cooperation with other states and international organizations shall be based on the principles of mutual respect, trust, mutual assistance, compromise, non-discrimination,

non-interference in each other's affairs, timely fulfillment of accepted international obligations and peaceful resolution of disputes.

2. The state is undertaking efforts to create an environment conducive to attracting investment and introducing modern digital technologies based on market-oriented approaches to organizing activities in the digital environment.

Article 103. Key International Cooperation Areas of the Republic of Kazakhstan in Digitalization

The key international cooperation areas of the Republic of Kazakhstan in digitalization shall be:

- 1) creation, implementation and development of digital technologies;
- 2) removal of regulatory barriers to the implementation of digitalization;
- 3) development of the internet;
- 4) combating cyber threats and cybercrime;
- 5) combating digital fraud.

Chapter 19. FINAL AND TRANSITIONAL PROVISIONS

Article 104. Dispute resolution in digitalization

Disputes in digitalization shall be resolved in accordance with the laws of the Republic of Kazakhstan and international treaties, ratified by the Republic of Kazakhstan.

Article 105. Liability for breach of the digital legislation of the Republic of Kazakhstan

1. Breaching of the digital legislation of the Republic of Kazakhstan shall entail liability, established by the laws of the Republic of Kazakhstan.

2. Administrative or criminal liability shall not relieve the guilty parties of their obligation to remedy the breaches.

Article 106. Enacting procedure of this Code

1. This Code shall come into effect six months after the date of its first official publication

2. The Law of the Republic of Kazakhstan of January 7, 2003 On Electronic Documents and Electronic Digital Signature shall be deemed repealed.

*President
of the Republic of Kazakhstan*

K. TOKAYEV