DIGITAL CODE OF THE KYRGYZ REPUBLIC

General Part

SECTION I
BASICS OF LEGAL REGULATION IN THE DIGITAL ENVIRONMENT

Chapter 1. General Provisions

Article 1. Definition of the basic concepts contained in this Code

The following basic concepts and their definitions related to the digital environment are applicable to this Code:

1) **automatic decision** – a decision made based on the digital data in which the results of processing digital data are generated and used to establish, modify, or terminate legal relations without human intervention;

2) **author of a digital document** – a subject of legal relations in the digital environment whose digital signature or identifier refers to the digital document;

3) **accreditation of the certification center** – recognition by the industry regulator of the National digital ecosystem (hereinafter referred to as the "national ecosystem") of the certification center as complying with the requirements established by this Code and the regulations adopted on its basis;

4) **broadcasting services** – telecommunication services intended exclusively for the distribution of TV and radio channels, including the bundling of TV and radio channels into the broadcasting multiplexes;

5) **virtual operator** – a telecommunications service provider that uses a digital numbering resource or a digital radio frequency resource of the Kyrgyz Republic for the purpose of its provision but does not own telecommunications networks in the Kyrgyz Republic;

6) **personal data records owner** – a subject of legal relations in the digital environment who, independently or jointly with others, determines the purposes and methods of personal data processing;

7) **owner of a digital signature verification key certificate** – a subject of legal relations in the digital environment to whom the certification center has issued a digital signature verification key certificate in the manner established by this Code;

8) **digital resource owner** – a subject of legal relations in the digital environment who independently or jointly with others has created such a digital resource or obtained the right to permit or restrict access to a digital resource based on law or an agreement;

9) **digital technological system owner** – a subject of legal relations in the digital environment who independently or jointly with others has created such a system or obtained the right to operate it based on law or an agreement;

10) **digital ecosystem owner** – a subject of legal relations in the digital environment who independently or jointly with others determines the digital ecosystem rules;

11) **digital records owner** – a subject of legal relations in the digital environment who independently or jointly with others has created such records or obtained the right to authorize or restrict access to digital records based on law or agreement;

12) **high-frequency devices** – the devices intended to make physical impact on objects by radio emission;

13) **state digital service** (hereinafter referred to as "the state service") – a digital service used to fulfill the functions, duties, and powers of state and local government bodies;

14) **state (municipal) digital resource** – a digital resource created for the purpose of providing state services by state or local government bodies;

15) **deepfake** – the creation or alteration of images or audio or video materials that closely resemble existing persons, objects, phenomena, or events, and may create false impressions in individuals about the authenticity of such images or materials;

16) **trusted third party** – a person providing joint recognition of the authenticity of digital signatures created in accordance with norms of the foreign state law and digital signatures created in accordance with this Code;

17) **trusted digital service** – a digital service aimed at certifying the occurrence, change, or termination of relations in the digital environment;

18) **identifier** – any information, including code, cipher, number, or address, which allows linking the digital records containing such information with each other and with the subject of legal relations in the digital environment;

19) **identity** – sameness of the subject with itself throughout the legal relations;

20) **information** – content of digital data, digital records, directly available for human perception;

21) **personal information** – information (regardless of its reliability) about an individual who can be identified based on this information alone or in combination with other information available to or obtainable by the record owner;

22) **infrastructure** – lands (land plots), buildings, structures, facilities, and other similar objects;

23) **incident in digital environment** – an event or action resulting in incomplete, inaccurate, irrelevant digital records, inaccessibility or disruption of the operation of digital services or digital technological systems;

24) **qualified digital signature verification key certificate (qualified certificate)** – a digital signature verification key certificate issued by an accredited certification center or a trustee of an accredited certification center or a industry regulator performing the functions of a root certification center;

25) **key** – any information (code, cipher) that is available to the person whom the identifier refers to and that unambiguously links that person to the identifier used by him/her;

26) **digital signature verification key** – a unique sequence of characters, unambiguously associated with the digital signature key and intended to verify the digital signature authenticity;

27) **digital signature key** – a unique sequence of symbols intended to create a digital signature;

28) **radio frequency conversion** – the process of transferring radio frequency bands defined in the National Radio Frequency Allocation Table or parts thereof:

a) from the category of government use to the category of civil use or joint government and civil use;

b) from the category of joint governmental and civil use to the category of civil use;

29) **constructive data protection** – data protection based on the design of technological systems that are aimed at protecting their users' interests and taking into account the life cycle of digital records processed by the system and digital services provided through it;

30) **contact information** – an identifier intended for communication in the digital environment with the person whom it refers to;

31) **coordinating body** – an authorized state body that carries out inter-sectoral and interagency coordination of activities of the state bodies, local government bodies, legal entities in the process of digital transformation of the Kyrgyz Republic;

32) **metadata** – structured digital data characterizing any digital objects of legal relations in the digital environment for their identification, search, and management;

33) **mobile device** – a digital device that has an international identification code (IMEI);

34) **national ecosystem** – a national (state-wide) digital ecosystem owned by the Kyrgyz Republic;

35) **processing** – any action (operation) or set of actions (operations) performed on digital data (digital records), including collection, recording, organization, structuring, accumulation, storage, adaptation or modification, downloading, viewing, use, disclosure by transmission, dissemination, exchange or other type of access, collation or combination, reduction, deletion, or destruction;

36) **processor** – a subject of legal relations in the digital environment that has been entrusted by other subjects through a contract or legal act to process digital records, operate digital technological systems or provide digital services, as well as to provide access to objects of legal relations in the digital environment;

37) **publicly accessible digital technological system** – a digital technological system to which access is not restricted by law, contract, or the owner's decision;

38) **publicly accessible digital records** – digital records, including those containing open data, to which access is not restricted by law, contract, or the owner's decision;

39) **open data** – digital data that are available in a machine-readable format and can be reused without restrictions;

40) **industry regulator** – an authorized state body performs inspections and makes decisions mandatory for subjects of legal relations in the relevant sphere of activity, and in cases provided for by this Code, it also issues permits (licenses);

41) **protected goods** – human life and health, human and civil rights and freedoms, the environment, the state's defense capability, national security, public order, and morality;

42) **personal data** – digital data containing personal information;

43) **personal data records** – digital records containing personal information;

44) **personal resources** – digital resources consisting of personal data records;

45) **user** – a subject of legal relations in the digital environment that requests or provides access to digital records, digital resources, digital services, or technological systems;

46) **digital service provider** – a subject of legal relations in the digital environment that provides digital services to users, either independently or jointly with others;

47) **consumer** - an individual who uses a digital technological system or digital service for personal, non-profit-making purposes;

48) **the government communications network of the Kyrgyz Republic (government network)** – special integrated classified telecommunications network designed to conducting secret negotiations and exchanging classified information between the state agencies, local government bodies, institutions and organizations (enterprises) of the Kyrgyz Republic, including those located outside its borders, having the appropriate clearance to carry out activities using information constituting state secrets, in the interests of state administration, national security, defense, law enforcement and emergency situations, and conducting secret negotiations and exchanging secret information with foreign competent state bodies;

49) **applicable legislation** – the legislation to be applied to legal relations in the digital environment involving foreign individuals or legal entities or complicated by another foreign element, which is determined in accordance with the Civil Code of the Kyrgyz Republic, other laws of the Kyrgyz Republic, international treaties entered into force in accordance with the Kyrgyz Republic legislation, recognized international customs, and based on the agreement of the parties;

50) **data (records) principal** – a subject of legal relations in the digital environment whom digital data or records refer to (i.e., contain information about him/her);

51) **spatial data** – data on spatial objects, including data on their shape, location, and properties;

52) **spatial metadata** – data that allow describing the content and other characteristics of spatial data necessary for their identification and retrieval;

53) **spatial objects** – natural, artificial, and other objects (including buildings, structures), the location of which can be determined;

54) **public obligations** – obligations to perform certain actions or carry out certain activities related to the radio frequency spectrum use, as imposed by decision of the industry regulator or other authorized state body;

55) **radio service** – use of the radio frequency spectrum for specific purposes;

56) **radio frequency spectrum** of the Kyrgyz Republic – a limited state resource that represents an ordered set of radio frequencies located within the limits established by the International Telecommunication Union and can be used to operate radio electronic means or high-frequency devices within the Kyrgyz Republic territory;

57) **radio-electronic means** – devices designed for data transmission and/or reception, telemetry, radiolocation, induction-type communications, and measurement of various parameters using radio waves;

58) **distributed digital resource** – a digital resource in which digital records are created and processed according to common rules, namely, in accordance with data processing protocols common for the digital technological systems using two or more technical devices distributed in space and belonging to different owners of such resource;

59) **risk (in the digital environment)** – a combination of the likelihood and severity of incidents in the digital environment;

60) **website** – a digital resource identified using a domain name or Internet address;

61) **digital wellness service** – a service aimed at improving an individual's quality of life based on the processing of digital data on his/her physiological characteristics;

62) **digital signature verification key certificate** – a digital document or a paper document issued by the certification center and confirming that the digital signature verification key belongs to the digital signature verification key certificate owner;

63) **artificial intelligence system** – a digital technological system that, based on digital data and goals set by a person, can form forecasts, recommendations, or make decisions with a certain degree of autonomy that affect the state of external subjects or objects;

64) **high risk artificial intelligence system** – an artificial intelligence system, the use of which increases the probability of causing harm to protected goods;

65) **smart contract** – a set of digital records including software for digital devices, setting out all or part of the terms and conditions of a transaction between parties in a digital environment, which is executed independently of the parties' involvement upon receipt of digital data specified by the parties to the transaction;

66) **owner of material carriers with personal information** – a person who owns material carriers with personal information that is not in the form of personal data;

67) **certification center facilities** – software and (or) hardware used for the functions of creating, storing, and issuing digital signature verification key certificates, and maintaining the register of digital signature verification key certificates;

68) **digital signature** – the encryption (cryptographic) means used to perform at least one of the following functions: creation of digital signature, verification of digital signature, creation of digital signature keys, and digital signature verification keys;

69) **personal data subject** – an individual who is the personal data principal;

70) **subject of legal relations in the digital environment** – a participant of relations regulated by this Code, which includes the Kyrgyz Republic, other states, state bodies, local government bodies and their officials, and individuals and legal entities. The rules established by this Code shall apply to relations with the participation of foreign citizens, stateless persons, foreign legal entities, foreign states, unless otherwise provided for by this Code or the law;

71) **telecommunications** – the exchange of digital data with other users through a telecommunications service, including by accessing digital data downloaded or created by other users, as well as voice connections with other users through a telecommunications service;

72) **telecommunication network** - a digital technological system designed to provide telecommunication service;

73) **telecommunications facility** - the telecommunications operator's infrastructure created or adapted to accommodate telecommunications networks and/or their elements (including, but not limited to, base stations, antenna-mast structures, antenna-feeder devices, and line-cable structures), which is not a capital construction object;

74) **telecommunications service** - the opportunities available to users to use digital technological systems to exchange digital data with other users, including by accessing digital data downloaded or created by other users, and the opportunities of voice connections over the telecommunication network;

75) **cross-border transfer of personal data** - the personal data transfer to record owners located under the jurisdiction of other states;

76) **certification center** - a legal entity or an individual entrepreneur engaged in the creation and issuance of digital signature verification key certificates;

77) **digital wellness devices** - digital technological systems and their elements used as part of digital wellness services;

78) **personal data leakage** - a type of unlawful processing of personal data in which personal data become available to individuals who have no legal grounds to access them;

79) **digital authentication** - confirmation connection between an identifier and the person whom the identifier refers to, using a key;

80) **digital record** - digital data that can be identified using metadata;

81) **digital identification** - searching a digital record to establish a link between the data principal and such digital record;

82) **digital signature** - information in digital form that is attached to other digital information in digital form and (or) logically linked to it, and is used to ensure the immutability of a digital document and to identify the digital document author;

83) **digital environment** - a system of social relations involving the digital data processing with digital devices that has no territorial boundaries;

84) **digital technological system** - a system of digital devices, software for them and databases designed to process digital data;

85) **digital resilience** - the state of the digital environment characterized by the continuity of provision and use of digital services, ensured through implementation of cybersecurity measures, and effective risk and resource management;

86) **digital ecosystem** - a set of publicly available digital technological systems, digital resources and digital services used to ensure the interaction of subjects of relations in the digital environment under common rules;

87) **digital application (app**) - a digital resource that is software for electronic computers and other digital devices used to access digital data;

88) **digital community** - an association of subjects of relations in the digital environment, regardless of whether it has the status of a legal entity, formed by them on their own initiative and based on voluntariness to carry out tasks of its participants based on common rules for developing and/or using objects of legal relations in the digital environment;

89) **digital device** - a technical device designed to process digital data, including an electronic computer (EC);

90) **digital** - a term that characterizes any phenomenon that requires the use of digital data (in most cases, data expressed in binary code);

91) **digital archive** - a digital technological system that ensures the integrity and immutability of digital records processed with its help and limited access to them;

92) **digital document** - a digital record the immutability of which is ensured by a digital signature or identifier used in accordance with the identification system's rules;

93) **digital duplicate of a document** - a digital record that fully reproduces the information originally contained in the original document on paper or other tangible medium signed with a handwritten signature, including its requisites;

94) **digital register** - a digital resource consisting of records that confirm ownership of rights to use the accounting objects listed in this Code;

95) **digital resource** - an ordered set of digital records, including a database, designed for storage and use of and access to digital records and (or) digital data;

96) **digital service** - ability to use a digital technology system to create, transmit, store or access digital data;

97) **digital service for identification of mobile devices** - a digital service for identifying and verifying the authenticity of the identification code of mobile devices operating and imported into the Kyrgyz Republic territory;

98) **digital data** - data that can be processed using digital devices, regardless of the form and method of their storage and transmission;

99) **digital rights** - rights to the object of legal relations in the digital environment, including the right to access the object of legal relations in the digital environment and the right to establish the access conditions;

100) **gateway** - a digital device that provides data transfer between telecommunications services for data transfer and voice connection provision;

101) **National telecommunications operator** - a legal entity in which the state holds at least 80 percent interest, as determined by a resolution of the Cabinet of Ministers of the Kyrgyz Republic (hereinafter referred to as the "Cabinet of Ministers").

Article 2. Fundamentals of relations in the digital environment

1. This Code lays down the rules that subjects of legal relations are obliged to follow in the digital environment.

2. The subject of this Code is the digital environment at the following levels:

1) relations involving the processing of digital data, creation and use of digital records, including in the form of digital documents, and digital resources;

2) relations involving the creation and use of digital services, building digital ecosystems, and participating in them;

3) relations involving the creation of digital technological systems, including data processing centers and telecommunications networks;

4) relations involving the access of digital technological systems owners to infrastructure (lands, buildings, structures, facilities, and other similar objects).

3. Relations on dissemination of certain types of information or access to it, depending on its content, shall be regulated by information legislation and shall not fall within the scope of regulation of this Code.

4. Relations arising from the counterintelligence and intelligence activities, as well as the operational and investigative activities, are regulated by the relevant legislation and are not the subject of regulation by this Code.

5. As part of regulating the digital environment, this Code establishes an exclusive list of cases in which the following are allowed:

1) restriction of access to objects of legal relations in the digital environment;

2) compulsory establishment of non-discriminatory access to the objects of legal relations in the digital environment.

Article 3. Principles of regulating the digital environment

1. Regulation of the digital environment shall be based on general legal, target and industry principles.

2. General legal principles applicable to the digital environment regulation shall include:

1) fairness and proportionality of regulation, that prioritizes the interests of the individual as the sole end-user of digital technologies (the fairness principle);

2) accessibility, comprehensibility and predictability of legal regulation (the certainty principle);

3) participation in the development of the digital environment rules of all persons subject to the rules, directly or through representatives (the participation principle).

3. The digital environment regulation aims to implement the following organizational principles:

1) possibility for subjects of legal relations in the digital environment to use any digital technologies of their choice, if the requirements established by this Code are met when using them (the technological neutrality principle);

2) application of the norms of this Code shall be non-discriminatory and shall apply to all subjects of relations in the digital environment, regardless of the quality, demand and other content characteristics of the digital data they process (the content neutrality principle);

3) long-term sustainability of the rules and legal relations defined by this Code, continuity of services and processes, and the protection of objects and subjects of legal relations in the digital environment (the sustainability principle);

4) promotion of competition in digital markets, openness and compatibility of data formats and records with transferability between providers of different digital services and owners of different digital technological systems, accessibility of digital data and decision-making based on them, including their reuse (the openness principle);

5) storage of the necessary digital data throughout the life cycle of the relevant technology confirming the fulfillment of obligations by the legal relations subjects, including their elimination of infringements and/or observance of the digital environment rights (the accountability principle).

4. The industry principles that form the basis for regulating relations in separate areas are enshrined in the relevant chapters of this Code.

Article 4. Digital Code and other normative legal acts

1. This Code shall take precedence in regulating relations in the digital environment. The norms of other laws and normative legal acts adopted in accordance with them, which determine the rules for regulating relations in the digital environment, may not contradict the provisions of this Code. In case of conflict between this Code and another normative legal act, the norms of this Code shall prevail and be applied, in accordance with the conflict resolution rules established by the normative legal acts.

2. Normative legal acts on legal regulation in the digital environment may be adopted only in cases expressly established by this Code.

3. A draft law on amendments to this Code shall be subject to mandatory approval by the coordinating body to ensure the unity of the digital environment at all levels established by this Code and compliance with the principles of regulating relations in the digital environment. This Code may be amended no more than once a year.

Article 5. Digital code and digital community rules

1. Digital communities shall be created by subjects of legal relations in the digital environment based on their initiative and willingness. Digital communities may have any organizational form and governance arrangements not prohibited by legislation. Subjects of legal relations that are participants of digital communities shall independently determine the

rules of such communities. In the Kyrgyz Republic, state bodies, local government bodies, their officials, individuals and legal entities, when determining the rules of digital communities in which they participate, shall be obliged to adhere to the Constitution of the Kyrgyz Republic, this Code, and laws of the Kyrgyz Republic.

2. When applying the digital communities' rules, the state bodies, local government bodies and officials of the Kyrgyz Republic shall be obliged to ensure compliance with requirements of the Kyrgyz Republic legislation and bear responsibility for non-compliance.

Article 6. Internationally recognized practice

1. The provisions of standards and recommendations published by international organizations, expert communities of foreign countries and actively used by subjects of legal relations in the digital environment shall form the generally recognized international practice.

2. In cases stipulated by this Code, when choosing technologies or ways of exercising their rights and fulfilling their obligations in the digital environment, subjects of legal relations in the digital environment shall take into account the generally recognized international practices approved by the industry regulator in the relevant sphere stipulated by this Code. In absence of a generally recognized international practice approved by the industry regulator, subjects of legal relations in the digital environment shall have the right to consider generally recognized international practices that do not contradict the approved standards and normative legal acts of the Kyrgyz Republic.

3. Subjects of legal relations in the digital environment shall demonstrate that the selected technologies comply with internationally recognized practices or requirements that are equivalent to or higher than those of internationally recognized practices, by publishing declarations of conformity.

Chapter 2. State Regulation in the Digital Environment

Article 7. Forms of state regulation

In the Kyrgyz Republic, the state regulates relations in the digital environment in the following forms:

1) inter-sectoral and interdepartmental coordination of activities of state bodies, local government bodies, and legal entities in the digital environment;

2) sector regulation and supervision.

Article 8. Coordination of activities in the digital environment

1. Cross-sectoral and interdepartmental coordination of activities of state bodies, local government bodies and legal entities in the digital environment shall be carried out by:

1) defining the nationwide goals and objectives, programs and plans for activities in the digital environment;

2) planning and monitoring the activities budgets in the digital environment of state bodies, local government bodies, while taking into account the secrecy regime, and the protection of state or other secrets protected by law;

3) providing strategic guidance of digital reforms and programs, and coordinating regional and international assistance allocated for implementation of activities in the digital environment;

4) supporting cooperation of all stakeholders, including unions and associations of subjects of relations in the digital environment, in the development and implementation of goals and objectives, nationwide initiatives, plans, and programs;

5) coordinating activities to create architecture of the state digital ecosystem, common digital platforms and services, and piloting innovative solutions;

6) ensuring smoothness, integration and coherence in the activities of all subjects of legal relations to achieve the goals of public administration in the digital environment.

2. The coordinating body in the digital environment shall be determined by the Cabinet of Ministers.

Article 9. Industry regulation and supervision

1. In the digital environment, regulation and supervision shall be carried out through inspections, and decisions (administrative acts) that are mandatory for subjects of legal relations in the digital environment, and, in cases provided for by this Code, issuance of permits (licenses).

2. This Code shall establish the state bodies powers to carry out regulation and supervision (industry regulators) in the following spheres:

1) personal data;

2) national digital ecosystem;

3) telecommunications.

3. The Cabinet of Ministers shall approve regulations on industry regulators.

4. The procedure for formation and operation of the industry regulator should ensure the independence of its regulation.

5. One and the same industry regulator may not exercise powers in several spheres set forth by this Code.

6. Each industry regulator shall be obliged to submit an annual report on the state of relations in the sphere within its competence, its decisions, human and financial resources, their volumes and utilization, planned actions, and measures. The report shall be published on the industry regulator’s website.

7. Industry regulators shall establish training centers in their respective spheres and ensure their operation. The industry regulators training centers shall conduct educational and outreach activities, research and practical development on a reimbursable or grant basis.

Article 10. Expert councils

1. The industry regulator may establish an expert council.

The expert council shall be an advisory and consultative body established on a voluntary basis. It is composed of representatives of expert, scientific circles, and professional environment in the relevant regulation sector, to prepare proposals and recommendations for the development and compliance with the principles of the digital environment regulation.

The industry regulator’s decision to convene the expert council with indication of the term of commencement of the expert council's activities and the term of its powers shall be published on the industry regulator’s website.

2. The expert council and experts may not interfere with the industry regulator’s activity, participate in inspections or make decisions that are binding on subjects of legal relations in the digital environment.

3. The regulation of the expert council, including the procedures for its formation, shall be approved by the industry regulator.

Article 11. Accreditation of subjects to carry out inspections in the relevant sphere

1. The industry regulator of the respective sphere shall accredit individuals and/or legal entities for the right to carry out inspections of the subjects of regulation in cases provided for

by this Code. Accredited persons shall have the right to carry out inspections with consent of the regulation subject.

2. In accordance with this Code, requirements to accredited persons, procedure of accreditation and type of document issued based on the results of inspections by accredited persons shall be established by acts of the Cabinet of Ministers.

3. Accredited persons shall pay an annual fee for accreditation, calculated based on the methodology approved by the Cabinet of Ministers and considering the following:

1) income from the services provided by accredited persons;

2) number of inspections;

3) weighting coefficient that includes the social factor;

4) calculation indicator;

5) coefficient of efficiency of the accredited person's activity.

Article 12. Rules and standards for professional activities in the digital environment

1. Professional associations of subjects of legal relations in the digital environment shall have the right to approve regulations binding on their members. Regulations may include rules and standards of professional practice of the association members that do not conflict with this Code.

2. Professional associations shall be required to monitor compliance with such regulations by their members.

3. Information on membership in such professional associations, results of the compliance control with mandatory regulations and violations committed and their resolutions shall be publicly available information. This information should be published by professional associations on their websites.

Article 13. Provision of telecommunication networks and facilities for state administration purposes

1. The Kyrgyz Republic’s telecommunications industry regulator, state bodies and local government bodies operating the internal, closed and classified telecommunications networks, and telecommunications network operators regardless of their form of ownership shall be obliged to provide telecommunications networks and facilities in the interest of state administration, national security, defense, law enforcement, and in emergency situations.

2. In case of emergencies, the telecommunications industry regulator shall take measures to ensure the provision of necessary telecommunications services. The telecommunications industry regulator may establish special temporary bodies to operate telecommunications networks and provide telecommunications services wholly or partially in the territory where an emergency or crisis situation has occurred.

3. The Cabinet of Ministers may use telecommunication services and facilities in the interests of state administration, national security, defense, law enforcement and in emergency situations (natural disasters, quarantines, etc.). Only in specified exceptional circumstances, the authorized state bodies may exercise the priority right to operate or suspend the operation of telecommunications networks and facilities.

4. The government network shall be organized and provided by the authorized state body responsible for ensuring the national security. The government network should ensure the security of information transmitted over that network.

Article 14. Suspension and resumption of the telecommunication networks operation

1. In the case provided for in part 3 of Article 13 of this Code, the telecommunications networks operation and provision of telecommunication services shall be suspended by

telecommunication operators based on a written, reasoned decision by an authorized official from the state body responsible for ensuring the national security, in cases established by the Kyrgyz Republic legislation.

2. In accordance with the procedure established by the Cabinet of Ministers, telecommunications operators shall not be entitled to provide access to their telecommunications network, and shall be obliged to prevent use of the relevant telecommunications service by mobile devices, if the international identification code (IMEI) is included in the "Black List" of the State Mobile Devices Identification System.

3. Telecommunications operators shall be obliged to resume the telecommunications networks operation and provision of telecommunications services based on the court order or written reasoned decision by an authorized official from the state body responsible for ensuring the national security, who has made decision to suspend the network operation or provision of telecommunications services.

4. The Cabinet of Ministers shall compensate losses incurred by the telecommunications operator as a consequence of suspension of its activity, in accordance with the established procedure.

Chapter 3. Special regulation in the digital environment

Article 15. Objectives and principles of special regulation

1. Subjects of certain types of activities in the digital environment may be temporarily exempted from certain obligations established by this Code and normative legal acts adopted in accordance with it (special regulation). Such exemption may be introduced in accordance with the procedure established by this Chapter of the Code.

2. The purposes of special regulation include:

1) development of advanced forms, methods and ways of economic and social activity;

2) safe testing of digital innovations in a real-world environment;

3) improving the quality and accessibility of the objects of legal relations in the digital environment;

4) encouraging fair competition;

5) attracting investments in the digital economy;

6) improving the efficiency of public administration and local self-government;

7) reducing regulatory uncertainty regarding innovative products and services.

3. Special regulation shall be based on the principles of:

1) temporary nature of the special rules to be introduced;

2) clear compliance of special rules to their objectives;

3) prohibition of depriving citizens of their rights and freedoms by special rules;

4) maintaining digital resilience;

5) equality of subjects of special regulation;

6) voluntary participation in special regulation;

7) transparency of the content of special rules and their objectives;

8) effective control of the industry regulator over implementation of special rules.

4. The National Bank of the Kyrgyz Republic shall establish procedure for establishment and participation, requirements to participants of special regulatory regimes in the market of banking and payment systems.

5. Special regulation shall be introduced only for relations in the digital environment and may not limit competition or equality among subjects. It may not exempt anyone from the obligation to pay taxes or other non-tax payments, nor may it exempt anyone from compensating for the harm caused.

Article 16. Introduction of special regulation

1. Special regulation shall be introduced by the decision of the Kyrgyz Republic President (hereinafter - the President) at the initiative of subjects of legal relations in the digital environment, including state bodies and local government bodies, and shall be approved by the industry regulator stipulated by this Code, in the sphere of activity of which special regulation is introduced.

2. The subject of legal relations in the digital environment, taking the initiative to introduce special regulation (the initiator), shall submit an application to the industry regulator for introduction of special regulation, containing the following data:

1) reference to provisions of the Code and normative legal acts adopted in accordance with it, which establish obligations of subjects of legal relations in the digital environment in the form of performing, observing certain procedures, prohibiting or restricting certain actions;

2) indication of the range of subjects that will be affected by the special regulation;

3) description of the goals and objectives of the proposed special regulation, significance of the relations to which special regulation is introduced, rationale for advantages of introducing special regulation;

4) rationale that exemption of the initiator and other entities engaged in similar activities from the listed obligations will contribute to achievement of one or more objectives of special regulation established by this Code;

5) description of possible negative consequences from the introduction of special regulation, measures necessary to mitigate them, methodology for assessing success of the results.

3. The industry regulator that has received an application for introduction of special regulation shall publish it on its website. The application should be published on the website within five business days from the date of receipt of the application.

4. Simultaneously with the publication of the application for introduction of special regulation, the industry regulator shall publish on its website the contact information for comments.

5. Based on results of the review of the application for special regulation and the comments received on it, the industry regulator shall make decision containing one of the following recommendations:

1) approve introduction of special regulation;

2) return the application for introduction of special regulation for revision, to take into account the comments to be listed in the industry regulator’s decision;

3) reject the application for special regulation.

6. Decision to approve introduction of special regulation by the industry regulator shall include conclusion of whether the application complies with the special regulation objectives and requirements established by this Article.

7. Within ten days, the industry regulator shall send a proposal to introduce special regulation to the President for a decision on special regulation introduction, together with a draft of the corresponding President’s decision and other necessary documents from the initiator attached.

8. The President's decision to introduce special regulation shall include the following:

1) indication of the purpose(s) of introducing special regulation from among those specified in this Code;

2) indication of specific provisions of laws and other normative legal acts of the Kyrgyz Republic, in relation to which special regulation is introduced;

3) description of special rules being imposed, consisting of exemptions from the obligation to perform certain acts, comply with certain procedures, prohibitions or restrictions;

4) indication of the range of subjects of legal relations in the digital environment, in respect of which special regulation is introduced;

5) description of types of activities in respect of which special regulation is introduced;

6) a list of measures that subjects of legal relations in the digital environment are obliged to take to reduce possible negative consequences from the introduction of special regulation;

7) frequency and list of data that subjects of legal relations in the digital environment applying special regulation should transfer to the industry regulator for the special regulation monitoring;

8) other conditions that define the procedure for the special regulation regime for this subject.

9. The decision on introduction of special regulation shall come into force thirty days after its official publication, unless longer period is established by the decision. Special regulation shall be introduced for three years, unless shorter period is requested by the initiator who applied for special regulation.

10. Other procedures and conditions for introducing special regulation, including procedures for submission, evaluation of applications of participants, procedures for the special regulation monitoring and reporting of participants shall be established by the Cabinet of Ministers.

Article 17. Application of special regulation

1. The subject of legal relations in the digital environment that applies special regulation, shall be obliged to notify other subjects with whom he/she enters into legal relations in the digital environment, by indicating it on its website, in applications, texts of agreements and in other similar ways.

2. The subject of legal relations in the digital environment that applies special regulation, shall be obliged to provide the industry regulator with the data necessary for the special regulation monitoring in anonymized form, within the terms established in the decision to introduce special regulation.

3. Within its competence, the industry regulator shall monitor special regulation, within which it shall collect and summarize data received from subjects that apply special regulation. It shall also identify and summarize facts of violations of the rights and legitimate interests of subjects of legal relations in the digital environment resulting from application of special regulation, including based on incoming subjects' complaints.

4. If, based on the results of the special regulation monitoring, the industry regulator reveals incompliance of the applied special regulation with the principles established by this Code, or insufficiency of measures that subjects of legal relations in the digital environment are obliged to take to reduce possible negative consequences of the special regulation introduction, the industry regulator shall make a proposal to terminate or change special regulation.

5. Summarized data of the special regulation monitoring shall be included in the industry regulator's annual report.

Article 18. Modification and completion of special regulation

1. Special regulation shall be modified within the term of its validity by making amendments to the relevant President's decision.

2. Special regulation shall be completed:

1) upon expiration of its term;

2) in case of exclusion from this Code or a normative legal act adopted in accordance with it of duties, the temporary exemption from which was the special regulation subject;

3) in case of cancellation of the President's decision, by which special regulation was introduced.

3. The President shall cancel the decision to introduce special regulation if after its adoption it is revealed that the application of special regulation is not compliant with the

principles and objectives of its introduction as established by this Code, or there is no result of measures to reduce the negative consequences of its introduction.

4. If special regulation is terminated due to expiration of its term, no later than six months before the expiration date, the industry regulator shall be obliged to publish on its website and send to the President the report on the special regulation results with proposals for amending the legislation to exclude obligations, the exemption from which was the subject of special regulation, or a proposal to maintain the existing legislative regulation.

Chapter 4. Interaction in the digital environment

Article 19. Legal basis for interaction in the digital environment

1. Subjects of legal relations in the digital environment shall have the right to interact using objects of legal relations in the digital environment, of which they are the owners (providers). In cases established by law, subjects of legal relations in the digital environment shall be obliged to interact in accordance with the procedure established by this Code, normative legal acts adopted in accordance with this Code, or the relevant digital community rules.

2. Interaction in the digital environment can be public, private-public or private.

3. Interaction shall be public if one of the participants can make decisions or impose data processing requirements binding on the other participants in the interaction. The procedure for public interaction, including the procedure for data processing in course of public interaction, shall be determined by the law providing for such public interaction.

4. The interaction shall be private-public in the following cases:

1) implementation of public-private partnership in accordance with the Kyrgyz Republic legislation on public-private partnership;

2) when participating in the national ecosystem;

3) when telecommunications operators interact using their telecommunications networks (hereinafter referred to as the “interconnection”) with a telecommunications operator recognized as an economic entity occupying dominant position, in accordance with antimonopoly legislation, in cases established by part 6 of Article 189 of this Code;

4) when providing telecommunication services under special conditions in accordance with this Code.

5. Interaction shall be private in cases not specified in parts 3 and 4 of this Article, including interconnection without participation of a telecommunications operator recognized as an economic entity occupying dominant position in accordance with antimonopoly legislation. Private interaction is carried out based on the agreements between subjects of legal relations in the digital environment.

6. Private-public interaction shall be carried out based on an agreement concluded in accordance with the procedure established by this chapter of the Code, following provisions of the public-private partnership legislation (for interaction in implementation of public-private partnership) and provisions of this Code on interaction in the relevant areas of relations in the digital environment.

7. Transactions between participants of interaction involving goods, works, services, intellectual property or objects of legal relations in the digital environment shall be made in accordance with the civil legislation. Procurement by state bodies, local government bodies, state and municipal institutions, funds and other legal entities established at the expense of public funds, funds of state bodies or local government bodies (public participants of interaction) shall be regulated by the public procurement legislation of the Kyrgyz Republic.

Article 20. Principles of interaction regulation

1. Interaction in the digital environment should be based on predetermined, clear and unambiguous rules (principle of relationship certainty).

2. The term of interaction in the digital environment should allow each of the participants to achieve their goals and objectives based on such interaction (the long-term interaction principle).

3. Interaction in the digital environment should be beneficial for all its participants, including those for whom it is mandatory (the mutual benefit principle).

4. Interaction in the digital environment may not aim at or actually lead to the restriction of the citizens' rights and freedoms (the principle of inadmissibility of restriction of rights and freedoms).

5. Interaction in the digital environment may not aim at or have effect of restricting competition in the digital environment (the principle of impermissibility of restricting competition).

6. Interaction with other participants should not lead to decrease in the digital resilience of any of them (principle of preserving digital resilience).

7. The nature, rules and goals of interaction in the digital environment should be open and available to the other subjects of legal relations in the digital environment (the transparency of interaction principle).

Article 21. Cooperation agreement

1. The interaction agreement subject shall be cooperation between the parties in the following areas:

1) processing of digital data, records and documents;

2) creating, using and providing access to digital resources, websites and applications;

3) creating and providing digital services, including trusted services;

4) interconnection and interaction using other digital technology systems.

2. Unless otherwise established by this Code or interaction agreement, the parties shall equally participate in achieving the results of interaction.

3. If the interaction agreement provides for obligations of the parties to grant the right to use intellectual property, the interaction agreement term and form of its conclusion should comply with requirements of the civil law to license agreements.

4. The interaction agreement conditions obliging the parties to refrain from certain actions may not contradict requirements of the antimonopoly legislation.

Article 22. Conclusion of a public-private interaction agreement

1. Conclusion of the agreement shall be mandatory:

1) for owners of state and municipal digital technological systems - when interacting within the national ecosystem;

2) for the telecommunications operator recognized as an economic entity occupying a dominant position in accordance with antimonopoly legislation - in interconnection in cases set forth in part 6 of Article 189 of this Code;

3) for telecommunications operators - when providing telecommunications services under special conditions, in accordance with this Code.

2. An interaction agreement in the digital environment under the public-private partnership shall be concluded in the procedure set forth by the public-private partnership legislation.

3. The subject of legal relations in the digital environment that has the right to conclude such an agreement (the authorized party) may send a proposal to conclude an interaction agreement to the subject with which the conclusion of such an agreement is mandatory (the obliged party).

4. The obligated party shall enter into private-public interaction agreements on equal terms with any authorized subjects, including its affiliates.

5. If an interaction agreement is not concluded within three months of the date on which the obliged party receives a proposal from the authorized party, either party shall have the right to apply to the industry regulator to resolve the interaction dispute.

6. An interaction agreement shall be concluded without time limit, if the proposal of the authorized party does not specify the term, for which it is proposed to conclude the agreement.

Article 23. Modification and termination of the cooperation agreement

1. The interaction agreement shall be amended or terminated by agreement of its parties, and if the parties fail to reach agreement - by decision of the industry regulator or court.

2. The parties' agreement or decision to terminate the interaction should contain:

1) indication of the ownership of rights (including digital rights) to the objects of legal relations in the digital environment created or modified as a result of interaction;

2) the parties' obligation to transfer to each other the technical documentation and other supporting materials for the objects of legal relations in the digital environment created or modified as a result of interaction;

3) order of succession in relations with users affected by the interaction termination.

3. An interaction agreement concluded for a certain period shall contain the conditions stipulated in part 2 of this Article.

4. Upon termination of interaction, the parties shall be obliged to stop data processing to the extent that the interaction agreement was the basis for their processing.

SECTION II
LEGAL RELATIONS IN THE DIGITAL ENVIRONMENT

Chapter 5. Objects of Legal Relations in the Digital Environment

Article 24. Types of objects of legal relations in the digital environment

1. Objects of legal relations in the digital environment include:

1) digital data, digital records (including as digital documents) and digital resources;

2) digital services and digital ecosystems;

3) digital technological systems, including data centers and telecommunication networks;

4) land, buildings, structures, facilities and other similar objects in terms of access to them by the digital technological systems owners.

2. In cases stipulated by this Code, digital rights shall be established for objects of legal relations in the digital environment, which include the right of access to the object of legal relations in the digital environment and the right to establish access conditions. Digital rights shall be alienable and can be transferred from one subject of legal relations in the digital environment to another based on agreement. Digital rights shall be protected by this Code.

3. Several subjects of legal relations in the digital environment may jointly own the digital rights to the same object. In this case, the manner in which digital rights are exercised and disposed of shall be determined by an interaction agreement between all the entities involved.

4. Digital rights shall be exercised subject to observance of the data principals' rights and restrictions imposed on the respective digital records.

5. This Code shall establish restrictions on digital rights, including the right to free access to objects of digital rights, with respect to certain types of objects, to implement the principles of regulating relations in the digital environment.

6. Forced alienation or restriction of digital rights with respect to a particular object shall be allowed only based on a court decision and in cases expressly provided for by the Kyrgyz Republic legislation.

Article 25. Digital data and digital records

1. Digital data shall be freely transmitted between any subjects and processed for these purposes without restriction and shall not themselves be subject of digital rights. Digital personal data shall be processed according to the rules established by this Code. Digital records shall be the object of digital rights of their owner, unless otherwise is established by this Code or by an agreement between the subjects of relations in the digital environment.

2. Regarding digital records, their owner shall have the following digital rights to:

1) authorize or restrict access to digital records, determine the procedure and conditions of such access;

2) use digital records and distribute them;

3) provide digital records to other persons under agreement or other legally established basis;

4) protect their rights by means established by law in case of illegal access to digital records or their illegal use by other persons.

3. The rights to digital records, which are virtual assets, shall be determined by the Kyrgyz Republic legislation on virtual assets. The rights to digital records that constitute intellectual property shall be determined by the Kyrgyz Republic intellectual property legislation.

4. Requirements related to the composition or presentation of digital data, metadata, or digital records constitute the data format or record format, respectively. The data format or record format may be provided for by normative legal acts or an agreement between subjects of relations in the digital environment.

5. Requirements for the data format and record format of digital documents shall be determined by the digital document author. Requirements for the data format and record format of digital documents of state bodies, local government bodies, and digital documents that are appeals to state bodies and local government bodies, shall be established in accordance with this Code.

Article 26. Digital resources

1. The digital resource owner shall have the following digital rights to:

1) permit or restrict access to the digital resource, determine the procedure and conditions for such access;

2) distribute digital data from the digital resource;

3) use any designations not prohibited by law to identify a digital resource;

4) protect their rights in the manner established by law in case of illegal access to a digital resource or its illegal use.

2. The rules established by this Code for digital resources shall apply to digital (including mobile) applications.

Article 27. Digital services

1. Digital services include the ability for users to use digital technological systems for the following purposes:

1) to create, process, store the digital data or access to them;

2) exchange digital data with other users, including by accessing digital data uploaded or created by other users.

2. Digital services shall be provided and used following the rules approved by the digital service provider.

3. This Code shall establish requirements for state services.

Article 28. Digital ecosystems

1. Participants in the digital ecosystem and the corresponding digital community shall include the digital ecosystem owner, digital resources owner, digital services providers and users (consumers).

2. Participants in the digital ecosystem shall have the right to participate in determining the digital ecosystem rules in the manner determined by this Code and the digital ecosystem rules.

3. The Kyrgyz Republic industry regulators and state bodies authorized to implement antimonopoly regulation in the relevant area shall take measures aimed at protecting and developing competition in digital ecosystems, including by:

1) developing a methodology for assessing the state of competition in digital ecosystems;

2) determining the specifics of applying general competition rules to economic sectors where the digital ecosystems owners violate the antimonopoly legislation requirements by creating obstacles to the competition development.

4. Parts 1 and 2 of part 3 of this Article shall be implemented by normative legal acts of the Cabinet of Ministers.

Article 29. Digital technological systems

1. Digital technological systems include digital data processing systems (including data centers and artificial intelligence systems) and telecommunications networks. This Code shall regulate the relations concerning the creation, construction, placement, and operation of digital technological systems. This Code shall also apply to relations regarding the placement and use of technical means included in digital technological systems (elements of digital technological systems) and to the regulation of services provided using digital technological systems.

2. Digital technological systems can be state, municipal or private. State and municipal digital technological systems shall be created for the state authorities and local government bodies to provide state services. Digital technological systems created for other purposes shall be private systems.

3. Digital technological systems shall be created and operated by their owner(s) or users jointly based on the agreed rules.

4. Unless otherwise specified in this Code, the establishment of mandatory requirements for digital technological systems and confirmation of compliance with the established requirements shall be regulated by the Kyrgyz Republic legislation on technical regulation.

5. The location and operation of the digital technological systems, and provision of services using them shall be regulated by civil legislation taking into account the characteristics established by this Code.

Chapter 6. Subjects of Legal Relations in the Digital Environment

Article 30. Legal status of subjects of legal relations in the digital environment

1. The Kyrgyz Republic and other states, state authorities, local government bodies and officials, and individuals and legal entities shall have an inalienable right to be subjects of legal relations in the digital environment, and have other rights set forth by this Code and the digital communities' rules, and have the related obligations.

2. Subjects of legal relations in the digital environment shall have the following digital rights to:

1) access digital data, of which they are principals;

2) create, distribute and use digital data, process them in any way not prohibited by law, have digital rights to created or otherwise obtained objects of relations in the digital environment;

3) create digital communities and participate in determining the rules for them;

4) determine their identity (including by indicating the name, title, other identifiers) within the digital community;

5) choose whether to continue participating in the digital community or to withdraw from, and the right to delete any data relating to their identity within the digital community, unless the law establishes the community obligation to keep certain data.

3. Subjects of legal relations in the digital environment may act as owners of digital records, digital resources, digital technological systems or ecosystems, digital service providers, data principals, users, processors or other in status provided for by this Code, the digital communities rules or agreements of subjects of relations in the digital environment.

4. All subjects of legal relations in the digital environment shall have the right to protect their rights stipulated for by this Code.

5. Subjects of legal relations in the digital environment may not discriminate unlawfully against other subjects of legal relations in the digital environment or unlawfully restrict competition in the digital environment.

Article 31. Digital records owner

1. Digital records owner shall be obliged to ensure that digital records are complete, accurate and up-to-date to the extent necessary for their intended use.

2. Digital records owner shall have digital rights to his/her digital records provided for in this Code.

3. The digital records owner shall be obliged to:

1) assist other persons in exercising their right to access digital data;

2) restrict access to digital records if such obligation is established by law, other normative legal acts or by agreement of the parties;

3) place digital records on physical media located in the Kyrgyz Republic territory in cases provided for by this Code.

4. Unless otherwise provided by law, the digital records owner shall have the right to condition granting access to digital records to another person, with this person being obliged not to disclose content of such digital records to third parties or distribute them (the confidentiality requirement). A user who violates the confidentiality requirement shall be obliged to pay compensation to the digital records owner for losses caused by such a violation, unless:

1) information contained in the digital records is publicly available or has become publicly available not through the user's breach of his or her duties;

2) information contained in digital records has previously been independently developed by the user or received from third parties without requirement to maintain its confidentiality.

5. Unless the place of processing digital records or the location of the digital resource is expressly provided by law, the digital records owner shall determine the location where the digital records are processed at his or her discretion.

Article 32. Digital resource owner

1. The digital resource owner shall have the digital rights to it provided for in this Code.

2. The digital resource owner shall define rules for the digital resource use, including its access rules.

3. The digital resource owner shall observe the restrictions on access to digital data or resources established by this Code.

4. The rules for use of state and municipal digital resources shall be established by normative legal acts of the Cabinet of Ministers. Unless otherwise specified by law, establishing the rules of use of a particular state or municipal digital resource, access to it shall not be restricted.

Article 33. Digital service provider

1. Unless otherwise specified in this Code, the digital service provider shall independently determine the terms of use of the digital service.

2. The digital service provider shall be obliged to make the following metadata about the digital service publicly available on its website or application:

1) name of the provider;

2) legal address of the provider;

3) contact information of the provider for direct and effective contact with the provider;

4) information about the provider registration in the state or similar public registry, its registration number, or an equivalent means of identification in that registry;

5) reference to the applicable legislation that establishes requirements for the digital service;

6) measures necessary to connect the digital service;

7) existing restrictions on the digital service use.

Article 34. Digital ecosystem owner

The digital ecosystem owner shall be obliged to:

1) ensure respect of rights and legitimate interests of participants in the digital ecosystem, including the digital rights and the data principal's right established by this Code;

2) provide opportunity to participate in defining the digital ecosystem rules for all participants in the digital ecosystem;

3) provide opportunity to freely connect to the digital ecosystem and freely quit the digital ecosystem with possibility to delete all data related to the participant leaving the digital ecosystem, unless the obligation to store such data is provided for by law;

4) provide the participant leaving the digital ecosystem with opportunity to obtain a copy of the data relating to him or her or, if the digital ecosystem processor has such technical capability, to transfer them to another digital resource specified by such participant;

5) provide equal and non-discriminatory access for all ecosystem participants to digital records, digital services and digital technological systems within the digital ecosystem;

6) protect competition within the digital ecosystem and not conduct monopolistic activities in relation to other subjects of relations in the digital environment;

7) provide opportunity to consider disputes between participants in the digital ecosystem based on equal rules for all participants and ensure execution of the decisions taken on such disputes.

Article 35. Digital technological systems owner

1. This Code shall establish rights and obligations of the digital technological systems owner.

2. No permit (license) shall be required to own and operate a digital technological system, except in cases established by this Code.

Article 36. User

1. User rights shall arise based on the normative legal acts or agreements with owners of digital records, digital resources, digital technological systems, and digital service providers.

2. A user shall be obliged to comply with the rules of use, including access restrictions established by law, by owner of digital records, digital resource, digital technological system, and digital service provider.

Article 37. Data principal

1. The data principal shall have the right to access digital records relating to him/her, and the right to participate in determining the rules for access to such records and their use as part of other objects of relations in the digital environment. The data principal's rights shall be exercised and protected, regardless of the rights to these digital records. The data principal's rights shall be inalienable and cannot be transferred to other persons. The data principal's rights may only be restricted by law and principles of regulation of relations in the digital environment.

2. To exercise the rights provided for by this Code, the data principal shall be obliged to provide information confirming that the relevant digital records relate specifically to him/her.

Article 38. Processor

1. The processor shall act in interests of the person who ordered the digital records processing, the digital technological systems operation or digital services provision, and access to objects of legal relations in the digital environment (the processing order).

2. The subject of legal relations in the digital environment, who instructed a processor to perform actions in his/her interests, shall be responsible for the processor's actions as if they were his/her own actions.

3. The processing order should define the list of actions (operations) with digital records, the purposes of processing, and establish the processor's obligation to comply with the established restrictions on access to digital records, digital technological systems or digital services, and it should also specify the requirements for ensuring the protection of objects of legal relations in the digital environment in accordance with this Code.

Chapter 7. Digital identification

Article 39. Right to identity

1. Subjects of legal relations in the digital environment shall have an inalienable right to determine their identity (to identify or not to identify themselves), including by choosing an identifier.

2. In cases established by law, subjects of legal relations in the digital environment shall be obliged to identify themselves in the manner established by this Code, normative legal acts adopted in accordance with it, or rules of the relevant digital community.

Article 40. Protection of the right to identity

1. No one may be forced to identify (including by indicating a specific identifier), except in cases established by this Code or by law.

2. Subjects of legal relations in the digital environment shall not be required to maintain their identity for longer than is necessary for the exercise of rights and performance of obligations by other participants in the same legal relations in the digital environment.

3. Aggregating digital records that contain identifiers shall be prohibited if it violates the right to identity or prevents subjects from protecting such right.

4. The Kyrgyz Republic shall provide each of its citizens with a unique public identifier for life, and, in accordance with its international commitments, ensure the identification opportunity for citizens of other states, stateless persons and organizations.

Article 41. Industry principles of digital identification

1. The Kyrgyz Republic's state policy in the field of digital identification aims at identifying and eliminating administrative barriers to the use of digital identification and creating conditions that allow individuals and legal entities to access digital identification. The presence or absence of the digital identification opportunity for a citizen should not affect the ability to exercise rights or fulfill obligations in the digital environment (the non-discrimination principle).

2. Digital identification should be available to everyone on reasonable terms, and all costs associated with digital identification should be proportional to the benefits acquired as a result (the availability principle).

3. Digital identification systems should be based on open standards and comply with the principles of compatibility, data portability and digital resilience, processing only those digital data that are necessary for digital identification (the sufficiency principle).

4. Digital identification shall be carried out based on trust and accountability between the subjects of legal relations in the digital environment. Subjects of legal relations in the digital environment should be able to exercise control over the use of their data, and have guarantees of independent control and fair consideration of disputes (principle of trust).

Article 42. Identifiers and digital data sources

1. Identifiers and digital records that contain them shall be processed according to the personal data rules established by this Code for personal data, with the features provided for in this chapter of the Code.

2. The unique public identifier in the Kyrgyz Republic shall be:

1) personal identification number for individuals;

2) taxpayer identification number for legal entities.

3. Unique public identifiers shall be publicly available data processed in accordance with this Code.

4. An identifier for inclusion in a digital record shall be chosen by:

1) the data principal – when the data about him/her is collected by the records owner;

2) the records owner- when the data are created by the records owner, including when an identifier is created or assigned;

3) by a third party - when the record owner receives data not from the data principal.

5. It is the record owner's responsibility to ensure the uniqueness of identifiers used in digital records.

Article 43. Use of identifiers in digital records

1. In accordance with the digital identification system rules, a digital record in which an identifier is used shall be considered as digital document similar to a paper document signed with a handwritten signature, if one of the following conditions is met:

1) the identifier is contained in the digital record itself and, in accordance with the digital identification system rules, clearly indicates consent of the person to whom the identifier relates to the digital record content or clearly indicates that such person is familiar with the digital record content;

2) in accordance with the digital identification system rules, indication of the identifier was a necessary condition to create a digital record using the digital identification system, and the digital record metadata contain an unambiguous indication of the person on whose behalf the digital record was created.

2. To contact government agencies and local government bodies of the Kyrgyz Republic, and to receive state services, identifiers should be used in accordance with the Unified Identification System rules approved by the Cabinet of Ministers.

3. An appeal and materials attached to it, which form a digital document, shall be recognized as equivalent to an appeal and other materials signed with a handwritten signature and presented on paper, except in cases where the law prohibits appeals to state bodies and local government bodies in form of a digital record.

Article 44. Contact information:

1. The identifier, which is contact information, may be used to send notices regarding the creation, change, or termination of legal relations only with the prior consent of the person to whom such identifier relates.

2. Digital authentication may be carried out by contact with the person to whom the contact information relates, exclusively in the cases and in the manner provided for by the identification system rules in accordance with this Code.

Article 45. Digital identification in digital communities

1. Digital identification in digital communities shall be carried out in accordance with the community rules.

2. No transfer of identifiers and digital records containing them to persons who are not the community members shall be permitted, except in cases established by law.

Article 46. Digital identification systems

1. Digital identification shall be carried out according to the digital identification system rules, which should also allow for digital authentication.

2. The digital identification system rules should contain the following provisions:

1) types of participants in the digital identification system;

2) types of relations in which digital identification is carried out in accordance with this digital identification system;

3) a list of identifiers used in the digital identification system and methods for obtaining them;

4) indication of the owner(s) of digital records that contain identifiers and data on the digital identification and digital authentication results, or an indication that such records represent a distributed digital resource;

5) methods of digital authentication (methods of obtaining and presenting the key) and the procedure for digital authentication;

6) procedure for recording the results of digital identification and the procedure for ensuring the integrity of information about the facts of digital identification;

7) methods and procedure for publishing or otherwise providing unlimited access to the digital identification system rules;

8) ban on the transfer of digital records with identifiers to persons who do not participate in the digital identification system, except in cases established by law.

3. In accordance with the digital identification system rules, the digital identification and digital authentication shall be the basis for the occurrence, modification, and termination of legal relations, including for proof purposes.

4. Digital authentication shall be considered as confirmation of an individual's identity when the relevant digital identification system is required by law or agreed upon by the parties. When applying for state services or when making a transaction, digital authentication shall be recognized as proper expression of a person to receive such state service or make a transaction.

5. Digital records of digital identification or digital authentication may not be deemed invalid only on the ground that they are in the form of digital data.

Article 47. Digital authentication service

1. A digital authentication service shall be a digital service in which the provider performs digital authentication of third parties at the request of the service user in accordance with the digital identification system rules.

2. The digital authentication service shall be provided based on an agreement concluded between the service provider and the user. Such an agreement should provide for:

1) a list of used identifiers;

2) procedure for accessing digital records necessary for implementation of digital authentication;

3) procedure for accessing digital records that contain data on the digital authentication results;

4) procedure for updating digital records, based on which digital authentication is carried out;

5) areas of application or types of relations in which the digital authentication service is used, if it can be used in a limited area of application or in certain types of relations;

6) requirements, the implementation of which is necessary for the correct operation of the service and use of its results;

7) procedure for updating and changing the service;

8) procedure for notification of unauthorized access to identifiers, keys or other data necessary for the service operation;

9) requirements for digital resilience of the service;

10) conditions on the amount or procedure for determining the service provider's remuneration or free use of the service;

11) liability for violation of the agreement terms.

3. Digital authentication services should be subject to regular cybersecurity audits. Information about the audit completion with indication of the next audit time should be published on the service provider's website.

Article 48. The Kyrgyz Republic's state system of biometric identification

1. In accordance with this Code, every individual shall have the right to biometric registration for the digital identification and digital authentication purposes.

2. The state biometric identification system shall be formed for digital authentication of the Kyrgyz Republic's citizens during elections and referendums, for receiving and providing state services and can be used for other purposes only in cases expressly provided for by law. In the specified cases, processing of biometric data shall be permitted only for the purpose of digital authentication of an individual by comparing with his or her biometric data stored in databases. Processing of individuals' biometric data for the purpose of digital identification by comparing them with all biometric data available in databases shall be prohibited.

3. The following biometric data of the Kyrgyz Republic citizens shall be processed:

1) digital graphic image of the face;

2) graphic structure of the papillary patterns of fingers of both hands;

3) handwritten signature.

4. In addition to biometric data, the following personal data shall be processed in the State biometric identification system:

1) personal identification number;

2) last name, first name, middle name;

3) nationality (ethnicity);

4) series and number of the passport;

5) birth certificate (for persons who have not previously received a passport of a citizen of the Kyrgyz Republic);

6) gender;

7) date, month, year of birth;

8) place of residence.

5. Personal data of the Kyrgyz Republic citizens in the State Biometric Identification System shall form the state digital resource of biometric data. The Kyrgyz Republic owns the state digital resource of biometric data. The procedure for biometric registration and digital identification using the State biometric data system shall be determined by the Cabinet of Ministers. The processing of biometric data for purposes not specified in part 2 of this Article shall be prohibited.

6. The procedure for ensuring security of biometric data when processing them in the state biometric data digital resource, requirements for material carriers of biometric data and technologies for storing such data outside the biometric data state digital resource shall be determined by the Cabinet of Ministers.

Article 49. Unified Identification System of the Kyrgyz Republic

1. The Unified Identification System of the Kyrgyz Republic shall be used by state bodies, local government bodies, and their officials for digital identification and digital authentication of officials and the state services users. The digital authentication service based on the Unified Identification System of the Kyrgyz Republic can be used by legal entities and individual entrepreneurs for purposes not prohibited by law.

2. The following identifiers shall be used in the Unified Identification System:

1) for individuals – last name, first name, middle name (if any), date of birth, personal identification number, qualified digital signature, contact information (the individual's e-mail address, mobile device number);

2) for legal entities – name, taxpayer identification number, registration number or code of a foreign organization, qualified digital signature.

3. Identifiers shall be entered into the Unified Identification System in the process of their collection from the person whom they relate to, and in their absence, they shall be assigned to such person in the manner established by legislation.

4. The owner the Unified Identification System digital resource shall be the Kyrgyz Republic, on behalf of which the national ecosystem industry regulator operates.

5. The order and procedure of digital identification and digital authentication using the Unified Identification System, the order for recording the digital identification results and the order for ensuring integrity of information on the digital identification facts, the order for using the digital authentication service based on the Unified Identification System shall be determined by the regulation on the Unified Identification System, approved by the Cabinet of Ministers.

6. Digital records that are required for digital identification in the Unified Identification System or contain the digital authentication results using the Unified Identification System shall be exchanged through interdepartmental interaction. Digital records from the State Biometric

Identification System can be used for digital authentication using the Unified Identification System.

Article 50. Anonymization of personal data records

1. Digital records that do not contain identifiers shall be considered anonymous and can be processed for scientific, statistical and other research purposes without the data principal's consent for their processing. Personal data records shall be anonymized in such a way that for the records owner the link between these digital records and this data principal is destroyed.

2. The anonymized personal data records owner who processes them for scientific, statistical and other research purposes shall be considered to be acting in his/her legitimate interests and should comply with the requirements of this Code relating to the personal data records processing.

3. To exercise own rights provided for by this Code, the data principal shall be obliged to provide the records owner with information confirming that the relevant anonymized digital records relate directly to him/her.

Article 51. Liability for violation of the right to identity

1. Subjects of legal relations in the digital environment shall have the right to compensation for damage (including moral damage caused to individuals) in case of violation of their right to identity or deprivation of their ability to protect such a right, including in case of their unlawful digital identification (digital authentication), coercion to digital identification (digital authentication) or denial of digital identification (digital authentication). Compensation for moral damage shall be paid apart from compensation for property damage and losses incurred by the subject of legal relations in the digital environment.

2. Instead of compensation for property damage and losses incurred, a subject of legal relations in the digital environment shall have the right to demand that the violator pay compensation for violation of his/her right to identity. Moral damages shall be compensated in cases and in the manner stipulated by civil legislation.

3. The amount of compensation should be at least one hundred calculation indicators and may be increased by court depending on the nature and duration of violation of the right to identity.

4. The procedure for considering the claims provided for in this Article shall be established by civil procedural legislation.

Chapter 8. Grounds for the Occurrence, Change, and Termination of Legal Relations in the Digital Environment

Article 52. Digital records as grounds for the occurrence, change, and termination of legal relations in the digital environment

1. Legal facts expressed in digital records, including those presented in the form of digital documents or as part of digital resources shall be grounds for the occurrence, change, and termination of legal relations in the digital environment shall be.

2. Certification of the occurrence, change, and termination of legal relations in the digital environment shall be carried out, among other things, with the help of trusted services.

Article 53. Occurrence, modification, termination of digital rights

1. Digital rights shall arise in cases provided for by this Code, by virtue of the creation or receipt of the corresponding object of relations in the digital environment. No registration or notification or other action shall be required to create digital rights.

2. The digital rights of subjects to the objects of legal relations created by them in the digital environment shall belong to each subject who independently created the same or similar objects. The identity or similarity of digital rights objects belonging to different subjects shall not in itself be a violation of the digital rights of another subject.

3. The ownership of digital rights can be evidenced by metadata, including those contained in distributed digital resources. In case of a dispute over the ownership of digital rights to digital records or digital resources, the obligation to prove the existence of digital rights rests with the owner of the digital records or digital resources, respectively.

4. When digital rights are alienated, including based on a court decision, they shall not be terminated, but transferred to the new owner.

Article 54. Occurrence, modification, termination of rights of the data principal

1. The data principal’s rights shall arise by virtue of the existence of a link between him/her and the data relating to him/her.

2. For the occurrence and exercise of the data principal's rights, no notification, registration or other actions shall be required, however, the digital records owner shall have the right to demand evidence from the data principal that such digital records relate to this principal.

3. The data principal’s rights shall terminate in the following cases:

1) destruction of digital records that relate to this principal;

2) depersonalization of digital records in such a way that the link between these digital records and this data principal is destroyed.

Article 55. Trusted digital services

1. Trusted digital services shall include:

1) digital authentication services;

2) digital signature services;

3) digital archive services;

4) guaranteed message delivery services;

5) website authentication services.

2. This Code shall establish requirements for trusted digital services.

Article 56. Recognition of foreign trusted digital services

1. In accordance with this Code, trusted digital services that meet the requirements established in other states (hereinafter referred to as “foreign trusted services”) shall be recognized as trusted services in cases where:

1) a foreign trusted service is included in the Register of Foreign Trusted Digital Services, which is formed and maintained by the national ecosystem industry regulator;

2) the court has established in its decision on the case that the foreign trusted service used by the party meets the criteria established by part 3 of this Article.

2. Decision to include a foreign trusted service in the register shall be made by the national ecosystem industry regulator. The decision of the national ecosystem industry regulator to include or refuse to include a foreign trusted service in the register should indicate the grounds for such decision. The refusal to recognize a foreign trusted service as trusted may be appealed in court.

3. The basis for the national ecosystem industry regulator’s decision to include foreign trusted digital services in the Register of Foreign Trusted Digital Services, and the basis for a

court's ruling on a foreign trusted service's compliance with the established requirements, is its simultaneous fulfillment of the following criteria:

1) actual compliance of the foreign trusted service with the requirements of this Code, including based on the expert examination results;

2) compliance of the digital service with generally accepted international practice relating to trusted services and containing requirements equivalent to or higher than the requirements of this Code, primarily in terms of information disclosure; documentation; digital resilience; technical control and supervision;

3) availability of certificates or statements of conformity issued by other states or organizations;

4) existence of an agreement between the subjects of legal relations in the digital environment, which provides for the use of a foreign trusted service and consequences of such use.

4. A court decision recognizing that a foreign trusted service complies with the requirements of this Code shall be the basis for inclusion in the Register of Foreign Trusted Digital Services.

5. Foreign trusted digital signature services will only be recognized if the authenticity of the digital signature is recognized in accordance with Article 140 of this Code.

Article 57. Features of automatic decision-making based on digital data

1. Subjects of legal relations in the digital environment shall have the right to automate decision-making based on digital data in such a way that the digital data processing results are formed and used for the occurrence, change, and termination of legal relations without human participation (automatic decisions).

2. Data principals whose interests are affected by automated decisions that have legal consequences for or similarly significantly impact them, shall have the right to demand the following from the subject using the automated decisions:

1) to stop making automatic decisions in relation to this data principal;

2) with human intervention review the automated decisions previously made with respect to this data principal.

3. A subject of legal relations in a digital environment using an automatic decision should be obliged to comply with the requirements established by this Code regarding the adoption of automatic decisions in the relevant areas of activity.

Article 58. Smart contract

1. Based on an agreement, Subjects of legal relations in the digital environment shall have the right to set out all or part of the terms of this agreement in a special programming language in the form of code. This code will subsequently be executed without the parties' participation upon the occurrence of certain conditions agreed upon by the parties, as confirmed by relevant digital data (smart contract), which can result in the occurrence, change, and termination of relations between the parties.

2. An agreement that provides for the use of smart-contracts should contain rules for resolving disputes between the parties, stipulating the human making decision on the dispute.

3. Requirements regarding the use of smart contracts in certain activities shall be established by this Code and the legislation on virtual assets.

Chapter 9. Exercising Rights and Fulfilling Obligations in the Digital Environment

Article 59. Public and open data

1. Digital data can be used by any persons at their discretion, subject to the exclusive rights to intellectual property objects, and restrictions established by law on the distribution, provision, use, and other processing of certain types of data or access to them.

2. Digital records shall be presumed to be publicly available unless their metadata contain indications that access to them is restricted by law, contract, or the owner's decision.

3. The digital records owner may, by indicating this in the digital records metadata, make further distribution of the digital records conditional with obligation to indicate himself/herself as the data source.

Article 60. Digital records distribution and access

1. Digital records shall be distributed at the initiative of their owner or the digital resource owner. Users shall initiate access to digital records.

2. Digital records shall be distributed freely in compliance with the requirements established by this Code. Access to digital records shall be granted under conditions determined by the relevant digital records owner or the digital resource owner.

3. The digital records metadata that are distributed or accessed should include reliable information about their owner in the form and volume that is sufficient to digitally identify that person or to enable contacting with that person in the digital environment.

4. Unless otherwise provided by law, a person who distributes digital records shall be obliged to provide the user with the opportunity to opt out of receiving digital records.

5. Cases and conditions for the mandatory distribution of digital records or access to them shall be established by law.

Article 61. Restriction of distribution of digital records and access to digital records

1. Access to or distribution of digital records may be restricted in accordance with the metadata of such records by law only in the following cases:

1) if the access restriction is the exercise of digital rights;

2) if the digital records metadata indicate that they are classified as a legally protected secret;

3) if the distribution of digital records or access to them is prohibited by law or a court decision.

2. The restrictions introduced should comply with the principles of regulation of relations in the digital environment. Arbitrary restrictions on access to digital records and their distribution shall not be permitted.

3. Researchers and scientific organizations shall have the right to access digital records containing personal data or classified as secrets protected by law for scientific, statistical or other research purposes, provided that their confidentiality is ensured.

4. Authorized persons, including scientific organizations, researchers and industry regulators, who, in accordance with this Code, access digital records containing personal data or classified as a secret protected by law, shall be required to comply with the procedure for such access established by the Cabinet of Ministers.

5. Persons who violate restrictions on access to records established by law or by the owner's decision shall bear liability established by law.

Article 62. Access to digital records in state and municipal digital resources

Unless otherwise provided by law, digital records from state and municipal digital resources shall be provided to users free of charge and without restrictions. A user who requests such records shall not be required to justify the need to obtain them.

Article 63. Digital resilience

1. The state shall regulate digital resilience to ensure continuity of activities of objects and entities and recover them after incidents in the digital environment, in light of the practical impossibility of providing full protection from them.

2. Digital resilience shall be achieved through implementation by subjects of legal relations in the digital environment of the following measures:

1) ensuring the integrity and availability of objects of legal relations in the digital environment, and confidentiality of the processed digital data;

2) monitoring and preventing incidents in the digital environment and exchanging data about them;

3) risk management in the digital environment based on the risk management system;

4) management of resources necessary to ensure the continuity of activities of subjects of legal relations in the digital environment.

3. The Kyrgyz Republic legislation in the field of cybersecurity shall establish the procedure and methods for ensuring the integrity, availability and confidentiality of critical information infrastructure facilities, the procedure for monitoring incidents in the digital environment and exchanging data on them.

4. Within the limits of their authority, industry regulators shall ensure the exchange of data on incidents in the digital environment, as well as other data affecting digital resilience, between subjects of legal relations in the digital environment. Within the limits of their authority, industry regulators shall summarize the data obtained in accordance with part 5 of this Article and ensure that measures are taken to prevent incidents in the digital environment. Participants of legal relations in the digital environment shall be required to implement measures specified by the relevant industry regulator to prevent incidents in the digital environment and mitigate their negative consequences.

5. The records owner or the digital service provider shall be obliged to notify the industry regulator of any incident in the digital environment that affects digital resilience or the rights and legitimate interests of subjects of relations in the digital environment no later than seventy two hours after the incident is discovered. If notification is not made within seventy hours, it should be accompanied by an explanation of the delay reasons.

6. The processor shall be obliged to notify the records owner about incidents within the time period established by the agreement between them or a legal act, but no later than forty eight hours after the incident is discovered.

7. The notification should contain the following:

1) description of the incident and an estimate number of users whose rights and legitimate interests it affects;

2) contact information of the person responsible for processing personal data or another person authorized to provide information about the incident;

3) description of the incident consequences;

4) description of measures taken to eliminate the incident, including measures aimed at minimizing its possible negative consequences.

8. As new information about incident or its consequences becomes known, the records owner or the digital service provider shall be obliged to update the information in the notification.

Article 64. Risk management system in the digital environment

1. For each object of legal relations in the digital environment to which it applies, the risk management system in the digital environment should determine the following:

1) list of risks, including assessment of the likelihood and scale of negative consequences;

2) risk management measures, that is, measures to reduce the likelihood and scale of negative consequences for each of the identified risks;

3) procedure for assessing effectiveness of the existing risk management system and modifying it based on the collected data on its implementation.

2. Unless otherwise stipulated by law, the owner (supplier) of the object of legal relations in the digital environment shall develop and implement the risk management system according to his/her own methodology, taking into account generally recognized world practice.

3. In cases established by this Code and the Kyrgyz Republic legislation in the field of cybersecurity, owners (suppliers) of objects of legal relations in the digital environment shall be obliged to conduct tests to determine the most appropriate risk management measures. The tests shall be considered successful if, based on their results, the object can be used for its intended purpose and meets the requirements imposed on it.

4. All data on the risk management system, its implementation methodology, and the test results of the high-risk artificial intelligence system should be presented in the form of digital records. Any information not classified as state secret by law shall refer to publicly available digital data and should be published on the website of the owner (supplier) of the object of legal relations in the digital environment.

Article 65. Risk management

1. Subjects of legal relations in the digital environment shall independently determine the resources (human, financial, technical and others) necessary to ensure digital resilience.

2. It shall be prohibited to establish requirements for subjects of legal relations in the digital environment, the fulfillment of which creates threat to their digital resilience.

3. When deciding on the resources needed to ensure digital resilience, the following factors shall be taken into account:

1) level of development of science and technology;

2) level of knowledge and skills of people involved in the creation and use of the relevant object;

3) nature, scope and purposes of processing digital data, providing digital services or operating digital technological systems;

4) life cycle of objects of legal relations in the digital environment, starting from the design stage of the relevant object;

5) rights and legitimate interests of subjects of legal relations in the digital environment who are owners, users or consumers of the relevant object.

Article 66. Ways to protect the rights of subjects of relations in the digital environment

1. Protection of the rights of subjects of legal relations in the digital environment shall be provided through:

1) technical, organizational and legal measures to protect the objects of legal relations belonging to them in the digital environment;

2) restoration of the situation that existed before the right violation, and suppression of actions that violate the right or threaten to violate it;

3) coercion of the user to fulfill his obligation or the owner’s legal requirement;

4) compensation for losses, including those caused by violation of legally established restrictions on access to digital records, and requirements to maintain the confidentiality of information and indicate the source of digital data;

5) compensation of the moral damage;

6) non-application by the court of an act of a state body or local government body that contradicts the law;

7) other methods provided for by this Code.

2. The measures provided for in paragraphs 4 and 5 of Part 1 of this Article shall not apply to suppliers whose digital services are:

1) to transfer digital data provided by another person, provided that they are transferred without changes and corrections;

2) to store digital data and provide access to them, provided that this provider was not aware of illegality of the processed information.

Article 67. Dispute resolution in the digital environment

1. Decisions and actions (inaction) of state bodies and local government bodies, organizations, officials that violate the rights of subjects of legal relations in the digital environment may be appealed in the manner established by the legislation on fundamentals of administrative activity and administrative procedures.

2. Disputes related to violation of the digital communities rules shall be considered according to the digital communities rules, which should provide for:

1) obligation to notify all persons affected by the dispute and obligation to provide them with access to all digital records relating to them and to the dispute substance;

2) opportunity for any person affected by the dispute to raise objections to substance of the claims brought against him/her or otherwise present his/her relevant arguments and evidence about the dispute;

3) consideration of the dispute on its merits by a person who is not interested in a particular outcome of the dispute (an independent arbitrator), or adoption of decision on the dispute by all participants in digital communities by voting, if this is stipulated by the digital communities rules.

3. Decision on a dispute made within the digital community following this digital community rules shall be binding on all the digital community members. The community of participants in the digital ecosystem shall ensure implementation of solutions based on the digital ecosystem.

Article 68. Liability for offenses in the digital environment

1. Committing offenses in the digital environment shall entail liability in accordance with applicable law. Separate chapters of this Code establish the specifics of liability for offenses committed in the relevant areas of the digital environment activity.

2. If damages resulted from unlawful denial of access to objects of relations in the digital environment, untimely provision of access, provision of knowingly incomplete, unreliable or outdated digital records, violation of the requirements established by this Code or an agreement for the availability and reliability of digital services and digital technological systems, or violation of digital rights, then they shall be subject to compensation in accordance with civil legislation.

3. Compensation to an individual for moral damage caused by violations specified in Part 2 of this Article shall be made regardless of compensation for property damage and losses incurred.

SPECIAL PART

SECTION III
DIGITAL DATA PROCESSING.
DIGITAL RESOURCES

Chapter 10. General Provisions on the Digital Data Processing

Article 69. Fundamentals of legal regulation of the digital data processing

1. In the Kyrgyz Republic, the industry principles for regulating relations on the digital data processing shall refer to:

1) a set of rights of records owners to determine the composition of the digital data to be processed, the purposes and methods of their processing at their own discretion, on the one hand, and rights of data principals to access their data, and in cases established by this Code, also the rights to object to the data processing and deletion, on the other (voluntary participation principle);

2) obligation of subjects of legal relations in the digital environment, when determining the volumes of digital data to be processed and choosing the goals and methods of processing digital data, to ensure that the rights and legitimate interests of other subjects are respected (good faith principle);

3) possibility of processing digital data created for certain purposes for other purposes, provided that the new processing purposes are compatible with the original ones (reuse principle);

4) possibility to use digital data from different sources and at the data principal's discretion, to transfer digital records between records owners due to the use of compatible data formats and record formats that enable interaction without any additional restrictions (the compatibility and portability principle).

2. Relations on the processing of digital data in certain types of legal relations in the digital environment shall be regulated according to this chapter rules, taking into account the requirements and restrictions established by the relevant chapters of this Code. Subjects of all types of legal relations in the digital environment shall enjoy all the rights provided for in this chapter and bear the relevant obligations.

Article 70. Processing digital data using big data and internet of things technologies

1. In the Kyrgyz Republic, technologies that involve processing large amounts of unrelated and constantly updated digital data to analyze the links between them (big data technologies) can be created and used without restrictions. Such data principals shall enjoy all the rights stipulated by this Code, including in case of data depersonalization.

2. Digital rights to digital records created by digital devices automatically without human involvement (by internet of things devices) shall belong to owners of such digital devices, unless otherwise established by an agreement between the device owner and other subjects of legal relations in the digital environment.

3. Persons using the big data and internet of things technologies shall be required to consider generally accepted international practice when choosing the formats of records created using such technologies.

Article 71. Prohibition of unfair processing

1. Unfair processing of digital data shall not be permitted.

2. Digital data processing shall be unfair if:

1) incomplete, inaccurate and/or irrelevant digital data are processed, making decisions based on which would be illegal or unfair to the data principal;

2) digital data that violate the right to identity and/or in violation of the law place the data principals in an unequal position based on criteria such as gender, race, language, disability, ethnicity, religion, age, political or other beliefs, education, origin, property or other status, are processed;

3) digital data processing violates the principle of voluntariness and leads to the excessive processing of data about the principal, in particular, when entering into an agreement with him/her or providing access to a digital service;

4) the user's ability to process is dependent on actions unrelated to the goals and objectives of such access, including in case of imposition of services or data processing parameters;

5) data principals and/or users do not have complete, accurate and up-to-date information about the processing and actions necessary for it, before such processing begins.

Article 72. Digital data processing in digital communities

1. Digital communities shall process digital data following the digital community rules.

2. A digital record processor may be defined to organize digital data processing in the digital community. The processor's activities shall be regulated by a publicly available community legal act complies with this Code requirements. The digital community rules shall determine the procedure for approving and amending such a legal act.

Article 73. Processing information and access to data

1. The data principal shall have the right to receive the following information from the records owner (hereinafter referred to as processing information):

1) confirmation of the fact of processing the digital data related to this principal;

2) legal grounds and purposes of processing the digital data related this principal;

3) name and location of the records owner;

4) place or places where the digital data related to him/her are processed;

5) contact information of the person responsible for processing personal data (if appointed by the records owner);

6) about persons who have access to digital data related to that principal or to whom such digital data are transferred (other than employees of the records owner);

7) on the terms of processing the digital data related to this principal or the procedure for determining them;

8) on rights of the data principal, including those being the personal data subject;

9) on consequences of the principal's refusal to process digital data related to him/her;

10) on automated decision-making based on digital data, including information about the algorithm, as well as the significance and intended consequences of the decisions for the data principal.

2. The records owner shall be obliged to provide the data principal with information about the processing in the following cases and within the following time periods:

1) when collecting personal data from the personal data subject - until the receipt of personal data;

2) when receiving digital data from other sources – within seven business days from the date of receipt of the data by the records owner;

3) upon receipt of the data principal's request to provide the processing information – within seven business days from the date of the request receipt.

3. The processing information should be provided to the data principal by the records owner in an understandable form. The processing information may not contain personal data of other persons, except in cases where there are grounds for the data principal to have access to such data.

4. The data principal shall have the right to request access to all digital data related to him/her processed by the record owner, while the record owner shall be obliged to provide such access within seven business days of receipt of the request from the data principal. At the

records owner's discretion, a copy of all digital records pertaining to the data principal may be provided within the specified time period instead of granting access to the digital records.

5. The records owner shall not be obliged to provide the data principal with information on processing of or access to the digital records related to him/her if he/she can prove that they have already been provided to the data principal.

Article 74. Restrictions on the data principal's rights

1. Restrictions on the data principal's rights to receive information on processing of and access to data about him/her shall be established by law with respect to:

1) digital data obtained as part of operational, investigative, foreign intelligence, or counterintelligence activities, unless these activities are conducted in violation of the Kyrgyz Republic legislation;

2) digital data processed in accordance with criminal procedural legislation;

3) digital data processed in accordance with the Kyrgyz Republic legislation on protection of state secrets.

2. Restrictions on data principal's rights to receive information on processing of and access to data about him/her, not provided for in Part 1 of this Article, shall be prohibited.

3. If the records owner discovers that a violation of the Kyrgyz Republic legislation, as confirmed by a judicial act or prosecutorial act, has occurred when obtaining digital data as part of investigative, intelligence or counterintelligence activities, he/she shall be obliged to send the processing information to such data principal within seven business days, in the manner prescribed by this Code.

Article 75. Correcting and supplementing digital records

1. The records owner shall be obliged to make corrections to digital records and, taking into account the purposes of their processing, supplement them in the following cases:

1) receipt of a request from the data principal to correct or supplement the digital records related to him/her;

2) receipt of a request from the relevant authorized government body on the need to correct or supplement the digital records;

3) the records owner receives new data indicating the incompleteness and unreliability of the digital records, and their loss of relevance.

2. The records owner shall have the right not to make corrections and additions to digital records if the data contained therein are complete, reliable and relevant from the point of view of the purposes of their processing by the records owner.

3. The records owner shall provide the data principal with information about corrections or additions to the digital records related to the data principal within seven business days of receipt of the data principal's request or of amendments to the data on other grounds.

Article 76. Transferring digital records

1. Upon the data principal's request to transfer the records related to him/her to another digital records owner shall take one of the following actions:

1) transfer such digital records to the new owner named in the request;

2) transfer to the data principal the digital records related to him/her in a format that allows their transfer to a new owner.

2. When selecting a format for transfer, the records owner should consider the recommended digital record standards, information about formats used by the new owner, and other information available to the record owner about the formats of records used for data transfer, including as specified in the data principal's request.

3. A request to transfer records to another owner may only concern the records processed based on the contract with the data principal or the data principal's consent to processing of data related to him/her.

4. The national ecosystem industry regulator shall develop and publish on its website the recommendations on the digital records formats and their metadata, technical and (or) organizational solutions aimed at ensuring the digital records portability.

Chapter 11. Processing of personal data

Article 77. Legal regulation of the personal data processing

1. This Code shall apply to any relations involving the personal data processing, including as part of digital records and digital resources. This Code provides for the specifics of processing personal information that is not digital personal data.

2. This Code shall not apply to relations involving the personal data processing by an individual only with regards to his/her personal or family affairs.

3. The normative legal acts regulating the personal data processing that contradict this Code or are not published in the established manner shall not be applied.

Article 78. Industry principles for the personal data processing

1. Personal data should be processed lawfully, fairly and openly in relation to the subject of personal data (the legality, fairness, transparency principle).

2. The personal data processing should be limited to achieving specific, predetermined and legitimate purposes. Changing or expanding the purpose of the personal data processing by the records owner without the subject's consent shall not be permitted, except in cases established by law (the principle of limitation of purpose).

3. The content and scope of processed personal data should be consistent with the stated processing purposes. The personal data processed should not be excessive in relation to the stated purposes of their processing (the data minimization principle).

4. In personal data processing, the accuracy of personal data, their sufficiency, and, where necessary, relevance to the personal data processing purposes should be ensured. The records owner should take necessary measures to delete or clarify incomplete or inaccurate personal data (the accuracy principle).

5. Personal data should be stored in a form that allows to identify the personal data subject for no longer than required by the personal data processing purposes, unless the personal data storage period is established by law or by a contract binding on the subject. Processed personal data should be destroyed or depersonalized upon achievement of the processing purposes or in case of loss of the need to achieve these purposes, unless otherwise provided by law (the storage limitation principle).

6. Personal data should be processed in a manner that ensures their security, that is, with the mandatory organizational and technical measures that prevent unauthorized or illegal processing of personal data, their accidental or intentional destruction, loss, damage or modification (the integrity and confidentiality principle).

7. The records owner shall be responsible for complying with the principles of this Article and should be able to certify compliance with them.

Article 79. Grounds for the personal data processing

1. The personal data processing shall be permitted if there is at least one of the following grounds for processing:

1) processing is necessary for the conclusion or execution of a contract in which the personal data subject is a party, representative or other person acting on behalf of a party to the contract, or a beneficiary, or for taking measures at the subject's request prior to conclusion of the contract;

2) processing is necessary for the records owner to fulfill the duties (powers) established by law or normative legal acts adopted in accordance with it, including acts in the field of official statistics and the national ecosystem rules;

3) processing is necessary to protect the vital interests of the personal data subject or another individual;

4) processing is necessary for the implementation by the records owner of public or other socially useful tasks, including the protection of human life, the interests of society, humanitarian, environmental and other significant goals;

5) processing is necessary for realization of the legitimate interests of the records owner or a third party, while the legitimate interests, rights and freedoms of the personal data subject are not violated.

2. In cases provided for by law, the subject's consent for implementation of certain types of processing of his/her data in presence of grounds for processing stipulated by part 1 of this Article shall be obtained. In absence of the grounds provided for in part 1 of this Article, processing shall be performed upon receipt of the subject's consent to the personal data processing and only for those processing purposes for which the personal data subject's consent was obtained.

3. Consent shall be void if it is given in response to a request that:

1) is not distinguished from other requests to the subject, in particular, in which it is not expressly stated that this request is a request for consent;

2) is not clear and understandable to the subject, presented in complex language;

3) sent to the subject in the presence of other grounds for processing provided for in part 1 of this Article.

4. Consent to the personal data processing should be voluntary, specific, informed and conscious. Consent to the personal data processing may be given by the personal data subject in any form that allows confirmation of the fact of its receipt, unless otherwise established by legislation.

5. The personal data subject may withdraw consent to his/her personal data processing. The procedure for withdrawing consent should not be more difficult than the procedure for granting consent.

6. Consent to the processing of personal data may be issued and withdrawn by a subject's representative acting on his/her behalf based on a power of attorney, agreement, instruction of the law or an act of an authorized state body or local government body. In case of incapability of the personal data subject, consent to the personal data processing shall be issued and withdrawn by the legal representative of the personal data subject. In case of the personal data subject's death, consent to his/her personal data processing shall be issued and withdrawn by heirs of the personal data subject.

Article 80. Processing of special categories of personal data

1. Processing of the following special categories of personal data shall be prohibited:

1) revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership;

2) containing genetic information;

3) biometric data for digital identification of an individual;

4) data concerning the health, sex life or sexual orientation of an individual.

2. The prohibition on processing the listed special categories of personal data established by part 1 of this Article shall not apply in the cases specified below, if measures to protect

against unfair processing of data and measures to prevent harm to the subject of personal data are enshrined in law and applied:

1) processing is necessary for the conclusion or performance of a contract in which the personal data subject is a party, representative or other person acting on behalf of a party to the contract, or a beneficiary, or to take measures at the subject's request prior to the contract conclusion;

2) processing is carried out according to the law that directly provides for the need to process such personal data and defines the purposes of their processing;

3) processing is necessary to protect the vital interests of the personal data subject or another individual or group of individuals;

4) personal data records are processed that the data subject has explicitly made publicly available;

5) the processing is carried out for medical and preventive purposes, in order to establish a medical diagnosis, provide medical and health and social services, provided that the processing of personal data is carried out by a person professionally engaged in medical activities and obliged in accordance with the law to maintain medical confidentiality;

6) processing is performed to protect the public health interests, including monitoring and protecting from the spread of life-threatening epidemics, and for humanitarian aid purposes;

7) processing of personal data records of members (participants) of a public association or religious organization is carried out by the respective public association or religious organization, acting in accordance with the legislation to achieve the lawful goals set forth in their constitutive documents;

8) processing is necessary for the administration of justice, including arbitration proceedings;

9) processing is carried out for the protection of national security, defense, public safety, and the prevention, investigation and prosecution of criminal offenses, as well as the enforcement of criminal penalties;

10) processing is carried out in accordance with the official statistics acts and the national ecosystem rules;

11) processing is carried out for scientific or other research purposes, provided that personal data records are anonymized.

Article 81. Specifics of the processing of children's personal data

1. Processing of children's personal data shall be permitted only in cases listed in part 2 of this Article, under the following conditions:

1) processing is carried out in the child's interests;

2) guarantees for the protection of the children's fundamental rights and freedoms established by this Article apply to processing.

2. Processing of children's personal data shall be permitted if:

1) processing is carried out following the law that expressly provides for the need to process the children's personal data and defines their processing purposes;

2) processing is necessary to protect the vital interests of the child (personal data subject) or another individual or group of persons;

3) processing is carried out for medical and preventive purposes, to establish medical diagnosis, provide medical and health and social, provided that the personal data are processed by a professional engaged in medical activities and obliged to maintain medical confidentiality under the legislation;

4) processing is carried out to protect the public health interests, in particular, for the purpose of protecting from the spread of life-threatening epidemics, and for humanitarian aid purposes;

5) processing is necessary for the administration of justice, including arbitration proceedings;

6) processing is carried out for the protection of national security, defense, public safety, and the prevention, investigation and prosecution of criminal offenses, as well as the enforcement of criminal penalties;

7) processing is carried out for scientific, statistical or other research purposes, provided that appropriate measures are taken to protect the data and children's interests, or to depersonalize personal data records.

3. In absence of the grounds provided for in part 2 of this Article, processing of the child's personal data shall be allowed only if the child's legal representative has given consent for processing of the child's personal data and only for those processing purposes for which consent has been given. Children who have reached the age of fourteen shall have the right to independently give consent to processing of their personal data when exercising their rights or performing their duties within the framework of their legal capacity as established by civil legislation.

4. The request for consent to processing of children's personal data and information related to the children's personal data processing should be presented in clear and simple language that is understandable to the child.

5. The records owners shall be required to take measures necessary to prevent unlawful processing of children's personal data.

Article 82. Impact assessment

1. In the cases provided for in part 2 of this Article, the records owner should conduct an impact assessment before processing personal data. A single assessment may be made for a set of similar personal data processing operations.

2. Impact on the personal data protection shall be assessed in the following cases:

1) in systematic and comprehensive evaluation of individuals' personal characteristics for the purpose of automated decision-making in relation to the personal data subject, resulting in legal consequences for the individual or similarly significantly affecting the individual;

2) when processing special categories of personal data in relation to more than a thousand personal data subjects;

3) in case of systematic automatic outdoor monitoring of public places by technical means.

3. The industry regulator responsible for personal data shall determine the list of processing operations for which a personal data protection impact assessment is required, and the list of processing operations for which data protection impact assessment is not required.

4. The assessment of impact on the personal data protection shall include:

1) description of the system of planned operations and processing purposes;

2) evaluation of compliance with the processing purposes based on the criteria of necessity and proportionality of processing operations, and the sufficiency or redundancy of personal data;

3) description of the risk management system.

5. The risk management system should take into account the views of personal data subjects from the relevant target group regarding the planned processing of their personal data.

6. The records owner shall be obliged to revise the impact assessment if there is a significant change in the set of operations or lists of personal data.

Article 83. Deletion of personal data records

1. The records owner shall be obliged to immediately delete personal data records if there is at least one of the following grounds, including at the request of the personal data subject:

1) personal data records are no longer needed for the purposes of their processing;

2) the ground for personal data processing ceases to be valid (including when the personal data subject has withdrawn his consent and there are no other grounds for processing);

3) upon consideration of the personal data subject's objection to the processing of his/her digital data by all means and for any processing purposes, the records owner decided to delete the data.

2. In the cases provided for by paragraph 1 of this Article, the records owner shall have the right not to delete personal data and store them for the purposes of:

1) exercising his/her right to freedom of speech;

2) scientific, including historical or statistical research, and archival purposes;

3) presentation of claims and demands, their execution or defense against them;

4) if the obligation to store such data is provided for by legislation.

Article 84. Objection to processing

1. The personal data subject shall have the right to send objection to processing of his/her personal data in certain ways or for certain purposes, to the records owner. The records owner shall be obliged to immediately stop processing personal data in the specified ways or for the specified purposes if at least one of the following conditions are met:

1) processing is carried out for the purpose of automatic decision-making in relation to the personal data subject;

2) processing is unfair towards the personal data subject or results in discrimination on racial, national, gender, age, religious or political grounds;

3) objection to processing is raised as part of the waiver of receipt of digital records;

4) objection to processing is due to the subject's withdrawal from the digital community;

5) if processing violates the personal data subject's right to determine his/her identity within the digital community, except in cases established by law.

2. The records owner shall be obliged to consider objection to processing and, within seven business days from the date of its receipt, send a reasoned decision to the personal data subject.

3. The personal data subject shall have the right to appeal the records owner's decision to either the industry regulator responsible for personal data or the court.

Article 85. Processing restriction

1. The records owner shall be obliged to restrict the processing of digital records related to the personal data subject:

1) upon receiving an objection to processing - for the period of the objection consideration;

2) upon receiving a request from the industry regulator responsible for personal data to restrict processing – for the period specified in the request;

3) if there are grounds for correcting or deleting personal data records - until they are corrected or deleted.

2. The records owner shall be obliged to inform the personal data subject of the establishment or removal of restrictions on the processing of personal data records using the available information no later than one business day following the day when the restrictions were established or removed.

Article 86. Participation of the processor

1. The processor shall process personal data records in accordance with a legal act or an agreement with their owner on the same grounds for the personal data processing provided for by this Code as the personal data records owner.

2. The records owner shall be obliged to ensure that the processor complies with the requirements of this Code.

3. The processor may not engage another processor without prior written permission of the record owner.

4. The agreement between the processor and the records owner, or the legal act under which the processor shall be engaged, should contain the following provisions:

1) period during which the processing is carried out;

2) nature and purpose of the processing;

3) type of personal data and categories of personal data subjects;

4) obligation to process personal data records only based on written instructions from the records owner;

5) obligation to ensure the restriction of access to personal data records including by imposing obligations to restrict access to the processor's employees and third parties who have access to the processor's digital technological systems;

6) procedure for interaction between the records owner and the processor regarding the correction, addition, deletion of personal data and restriction of their processing;

7) procedure for recording operations with personal data records, allowing confirmation of fulfillment of the obligations established by this Code.

5. The industry regulator responsible for personal data shall develop and publish on its website the standard (recommended) forms of agreement between the processor and the records owner and the legal act in accordance with which the processor is engaged.

Article 87. Joint records owners

1. Records owners who jointly own digital rights to the same personal data records (personal resources) and who jointly determine the purposes and means of processing shall be considered joint records owners.

2. Joint owners should openly, including by concluding an agreement or a legal act, determine and publish the procedure for joint exercise of their rights and fulfillment of the obligations provided for by this Code with respect to records owners. At the same time the procedure for the joint exercising rights and performing obligations is published, contact information to contact the records owners in the digital environment should be published.

3. The data processing in digital communities shall be carried out in accordance with the community rules, which should determine the person responsible for the personal data processing in the digital community.

4. Data processing in digital ecosystems shall be carried out in accordance with the digital ecosystem rules. The digital ecosystem owner shall be obliged to ensure compliance with the requirements of this Code regarding the personal data processing in the digital ecosystem, and should be able to confirm their compliance and shall be liable for their non-compliance.

5. The personal data subject may exercise his/her rights in relation to any of the records owners at his/her choice, regardless of the agreements between the joint records owners.

Article 88. Protection of personal data

1. The records owner shall be obliged to protect personal data, personal data records, and personal resources.

2. To ensure digital resilience during the personal data processing, the records owner shall:

1) implement the constructive data protection when designing digital technological systems;

2) keep records of operations with personal data records in accordance with recommendations of the industry regulator responsible for personal data;

3) determine the person responsible for the personal data processing in the organization (for organizations with more than ten employees), from among the organization employees or engaged based on an agreement;

4) organize training on the rules and recommendations for personal data processing and factors that contribute to their effective application.

3. In accordance with the established levels of personal data protection, the Cabinet of Ministers shall establish requirements for the personal data protection during their processing in digital technological systems.

Article 89. Cross-border transfer

1. The industry regulator responsible for personal data shall approve and publish a list of foreign states that ensure adequate protection of the personal data subjects' rights on its website. A foreign state may be included in the abovementioned list provided that legal norms in force in such state and measures applied to ensure the personal data protection comply with provisions of this Code.

2. Cross-border transfer of personal data to the territory of foreign states included in the list of foreign states that ensure adequate protection of the personal data subjects' rights shall be carried out in accordance with this Code and may not be prohibited or restricted.

3. Prior to the transborder transfer of personal data, the records owner shall be obliged to ensure that the foreign state to which the personal data is transferred is included in the list provided for in this Article.

4. Cross-border transfer of personal data to foreign states that do not provide adequate protection of the personal data subjects' rights may be carried out in any of the following cases:

1) at the personal data subject's consent to cross-border transfer of his personal data;

2) stipulated by international treaties that have entered into force in accordance with the Kyrgyz Republic legislation;

3) provided for by the Kyrgyz Republic legislation, if necessary to protect foundations of the Kyrgyz Republic constitutional order, and to ensure the country defense and security of the state;

4) conclusion and/or execution of the agreement in which the personal data subject is a beneficiary or a party (representative or other person acting on behalf of the contracting party);

5) protection of life, health, other vital interests of the personal data subject or other persons if it is impossible to obtain the personal data subject's consent;

6) ensuring that terms of the agreement concluded between the records owners or the records owner and the processor, provide adequate protection of the personal data subjects' rights. The industry regulator responsible for personal data shall determine the necessary terms of the agreement to ensure adequate protection of the personal data subjects' rights.

5. In the event of cross-border transfer, personal data shall be processed in accordance with the legislation of the country which they are transferred to.

Article 90. Industry regulator responsible for personal data

1. The authorized state body established in accordance with the procedure outlined in Article 9 of this Code (industry regulator responsible for personal data) shall carry out regulation and supervision in the personal data field. The industry regulator responsible for personal data should be independent of the persons in relation to whom it exercises its powers.

2. The head of the industry regulator responsible for personal data should have the qualifications, experience and knowledge, including in the field of personal data protection, necessary to perform duties and exercise powers.

3. The industry regulator responsible for personal data shall exercise the following powers:

1) ensuring the application of this Code and supervising its application in the relevant area;

2) raising awareness of the personal data subjects regarding the risks, norms, guarantees and rights related to the personal data processing, including children's personal data processing;

3) raising awareness of personal data owners and processors of their obligations under this Code;

4) advising the state bodies and organizations on legislative and administrative measures related to the personal data processing;

5) implementing accreditation of individuals or legal entities to conduct inspections of compliance with requirements in the sphere of personal data, in the manner established by the Cabinet of Ministers;

6) informing the data subjects on issues related to the exercise of their rights provided for by this Code, including if this requires cooperation with supervisory authorities of other states for these purposes;

7) considering complaints and conducting inspections during the application of this Code in the sphere of personal data, including on its own initiative and based on information received from another supervisory authority or another state agency. Inspections of business entities shall be carried out in accordance with the Kyrgyz Republic legislation on the procedure for conducting inspections of business entities;

8) taking preventive, corrective and coercive measures in cases of violation of the principles and rules for the personal data processing, and of the rights and obligations under this Code;

9) publishing guidelines and recommendations for the personal data processing that comply with security measures and this Code.

4. The industry regulator responsible for personal data shall maintain a record owner register, where the following data are entered as received:

1) about incidents with personal data;

2) on verification of the records owners and processors' compliance with provisions of this Code and the issuance of binding decisions based on the verification results;

3) prosecution for violations in the field of personal data.

5. The industry regulator shall independently determine the procedure for maintaining the record owner register. The register shall be accessed through the industry regulator's website.

6. The industry regulator responsible for personal data shall publish an annual report on its activities and the results of its investigations on its website.

7. The industry regulator responsible for personal data shall be entitled to:

1) request information from individuals and organizations, including information related to state secrets or other secrets protected by law, necessary for exercise of their powers, and receive such information free of charge;

2) gain access to all premises, documents, equipment, employees and contractors of the personal data records owners that are related to their processing for the purpose of establishing facts that are significant for the control and supervisory actions being carried out;

3) monitor the personal data processing by state bodies and their subordinate organizations, except for the data obtained in the course of intelligence and counterintelligence activities and defense-related activities;

4) demand that the records owner should clarify, block or delete inaccurate or illegally obtained personal data;

5) demand suspension of the personal data processing carried out in violation of requirements of this Code;

6) apply to the court with claims in defense of the violated rights of personal data subjects, including in defense of the rights of an indefinite number of persons, and represent the personal data subjects' interests in court;

7) send materials related to violation of the personal data subjects' rights in accordance with subordination;

8) submit proposals to the Cabinet of Ministers for improving the regulatory framework for personal data. Normative legal acts adopted pursuant to this Code that are aimed at inspecting organizations whose activities are regulated by banking legislation shall be subject to mandatory approval by the National Bank of the Kyrgyz Republic;

9) bring to justice persons guilty of violating requirements of this Code in the relevant sphere.

8. The industry regulator responsible for personal data shall be obliged to prevent unauthorized access to personal data records processed during its activities. It is also for unlawful processing of such personal data records.

9. The industry regulator responsible for personal data shall be obliged to:

1) organize the observance of the personal data subjects' rights in accordance with provisions of this Code;

2) verify compliance by the record owners and processors with provisions of this Code regarding personal data processing and make binding decisions based on the verification results;

3) interact with other state bodies of the Kyrgyz Republic, including entering into memorandums on joint actions on control and supervision, in order to avoid duplication of control and supervision activities and take into account the specifics of conducting activities in the relevant sphere;

4) consider complaints and appeals from individuals and legal entities regarding the personal data processing, and within the limits of their authority, also make binding decisions based on the results of the consideration of such complaints and appeals;

5) provide explanations on the application of personal data legislation at the request of individuals and organizations, and publish these explanations on its website;

6) develop and publish recommendations on the accounting for personal data processing operations, and conduct training and educational activities in the field of personal data, develop and publish sample forms of agreements, legal acts and other documents in the field of personal data.

10. The industry regulator responsible for personal data shall cooperate with similar bodies in foreign countries and approve a list of foreign countries that ensure adequate protection of the rights of personal data subjects.

Article 91. Features of processing personal information that is not personal data

1. Personal information that is not digital data and is processed without digital devices should be processed in accordance with the processing principles established by this Code, and only if there are grounds for processing provided for by this Code.

2. If it is necessary to make hard copies of personal information to fulfill the personal data subject's requests, the personal data subject shall be obliged to pay the cost of making such copies.

3. Although the owner of tangible media containing personal information is not required to comply with the personal data protection requirements of this Code, they are required to limit access to such media and maintain records of those who have access to them.

Chapter 12. Spatial data

Article 92. Spatial data in the digital environment

1. Spatial data provide a link between legal relations in the digital environment and infrastructure.

2. Spatial data consist of the following types of digital data:

1) digital geodetic data, that is, the results of geodetic activities suitable for processing using digital devices;

2) digital cartographic data, that is, the results of cartographic activities suitable for processing using digital devices;

3) digital location data, that is, data suitable for processing using digital devices, including the spatial objects coordinates.

3. This Code shall govern the processing of spatial data within the legal framework of the digital environment, taking into account the restrictions established by this Code and the Kyrgyz Republic's legislation on certain types of secrets. The Kyrgyz Republic legislation on geodesy and cartography shall regulate activities in the field of geodesy and cartography, including for the functioning and interaction of government authorities in this field.

4. The procedure for the creation and use of the results of geodetic and cartographic activities classified as state secrets shall be established by the Kyrgyz Republic legislation on the protection of state secrets.

Article 93. Industry principles for regulating relations on the spatial data processing

1. The results of geodetic and cartographic activities, as well as other data on the location of spatial objects shall be used by subjects of relations in the digital environment, provided that they are brought into a form suitable for processing with digital devices (the digitization principle).

2. Spatial data shall form the basis for the developing infrastructure in the Kyrgyz Republic, replenishing and carefully using natural resources, and protecting the environment, which requires processing complete, up-to-date and reliable spatial data (the quality principle).

3. Subjects of legal relations in the digital environment shall process spatial data based on access to them by all interested parties, subject to restrictions established by the Kyrgyz Republic legislation on state secret protection (the principle of joint participation in processing).

4. The processing of spatial data may not violate the privacy or inviolability of the home, or restrict a person's freedom of movement (the principle of personal inviolability).

Article 94. Spatial metadata

1. Spatial records shall be processed, accessed and distributed based on spatial metadata.

2. Access to spatial metadata cannot be restricted, unless otherwise provided by law.

3. In the Kyrgyz Republic, owners of cartographic and geodetic collections shall be required to create and publish spatial metadata about their collections in an open data format, and submit spatial metadata for inclusion in the spatial data national resource of the Kyrgyz Republic.

4. The authorized state body responsible for developing state policy in the field of geodesy and cartography shall establish requirements for spatial metadata.

Article 95. National spatial data resource

1. The national spatial data resource of the Kyrgyz Republic (hereinafter referred to as the "Georesource") is a database of digital spatial data on the territory of the Kyrgyz Republic and spatial metadata, as well as processing standards and formats of digital spatial data that ensure their accessibility and compatibility.

2. The georesource shall not contain data related to state secrets.

3. Digital rights to the georesource shall belong to the Kyrgyz Republic. On behalf of the Kyrgyz Republic, the rights of the georesource owner shall be exercised by the authorized state body that performs functions related to the development of state policy in the field of geodesy and cartography.

4. The georesource owner shall ensure the completeness, reliability and relevance of the data in the georesource and for this purpose interact with other state digital resources owners.

5. The georesource shall include the following types of digital data:

1) spatial data of the state cartographic and geodetic fund of the Kyrgyz Republic, including data obtained during digitization of materials of the cartographic and geodetic fund of the Kyrgyz Republic;

2) spatial data obtained by implementation of license agreements for the use of georesources;

3) spatial data obtained from other state digital resources;

4) spatial metadata;

5) standards for processing and formats of spatial data.

6. Access to the georesource shall be provided based on a license agreement on the use of the georesource concluded between the georesource owner and the users, in accordance with civil legislation, under the following conditions:

1) there is no fee for accessing the georesource;

2) the right to use digital data from the georesource shall be granted to the user on the condition that the user grants the right to use any spatial data derived from data obtained from the georesource (derived spatial data) to the georesource owner;

3) within one year of its creation, the user shall be obliged to transfer the derived spatial data to the georesource owner in a format approved by the authorized state body responsible for developing the state policy in the field of geodesy and cartography;

4) the user shall be obliged to transfer the metadata of the derived spatial data together with the derived spatial data.

Article 96. Geosite

1. The site through which access to spatial records of the Kyrgyz Republic and their distribution is carried out (hereinafter “the geosite”) shall be intended to perform the following functions:

1) searching for spatial data using spatial metadata;

2) obtaining the location data in open data format;

3) gaining access to formats, standards and other regulatory and technical data related to geodesy and cartography.

2. The Cabinet of Ministers shall approve the list of location data, access to which is provided in the open data format using the geosite.

3. Access to the geosite shall be provided free of charge.

4. Digital rights to the geosite belong to the Kyrgyz Republic. On behalf of the Kyrgyz Republic, the geosite owner’s rights shall be exercised by the authorized state body responsible for developing the state policy in the field of geodesy and cartography.

Article 97. Processing spatial records

1. When processing spatial records, their owners should respect the data principals’ rights, including:

1) the principal's right to receive spatial metadata related to him/her;

2) the principal's right to make changes to spatial data related to them or to spatial objects or digital devices that belong to him/her;

3) the right to require the spatial data owner to delete digital records related to the principal or to delete any identifiers associated with the principal.

2. Creating derivative spatial data shall require observance of the digital and other rights of the spatial records owner used to create such derivative data.

3. Spatial records shall be processed independently of the rights to the infrastructure to which the spatial data relates.

Article 98. Ensuring compatibility and portability of spatial records

1. To ensure compatibility and portability of digital spatial records, they shall be processed in accordance with generally accepted international practice and taking into account the opinion of participating subjects of legal relations in the digital environment.

2. In accordance with the standards and formats contained in the georesource, spatial records shall be processed within the state services.

3. The authorized state body responsible for developing the state policy in the field of geodesy and cartography shall publish on the georesource the list of standards and formats used in the spatial records processing.

Chapter 13. Digital Registers

Article 99. Regulation of digital registers

1. This Code shall regulate the creation and use of digital registers confirming the ownership of rights to use the following accounting objects:

1) elements of the national ecosystem;

2) radio frequency spectrum;

3) numbering.

2. The Kyrgyz Republic is the owner of:

1) digital registry of the national ecosystem;

2) digital radio frequency register;

3) digital numbering register.

3. On behalf of the Kyrgyz Republic, the rights of the owner of the national ecosystem digital register shall be exercised by the national ecosystem industry regulator, and the rights of the owner of the digital radio frequency register and digital numbering register shall be exercised by the telecommunications industry regulator.

4. The procedure for making and changing entries in digital registers owned by the Kyrgyz Republic shall be established by the Kyrgyz Republic legislation, taking into account the provisions of international treaties and generally recognized international practice.

5. The radio frequency spectrum users, numbering users, the national ecosystem elements owners (suppliers) shall be the principals of records in the corresponding digital registries.

Article 100. Industry principles for maintaining digital registers

1. Records in digital registers shall be publicly available (except for records classified as state secrets in accordance with the procedure established by law), shall be created and changed based on the rules established by law, and form the basis for creation, change, and termination of legal relations in the digital environment (the publicity principle).

2. Records in digital registers shall be created and changed only at the secretion of the records principals; changing a record in digital registers against the will of its principal shall be possible only based on a court decision (the inalienability principle).

3. Only one record can be created in relation to one accounting object in one territory (the uniqueness principle).

4. If the purpose of the rights was not specified when the record was created in the digital register, then the rights confirmed by the record may be exercised for any purpose and using any technology (the target principle).

5. Records in digital registers shall be created in such a way that the exercise of the rights of some records principals does not interfere with the exercise of the rights of other records principals (the harmonization principle).

6. Digital registries should ensure the fairest and most efficient distribution of rights confirmed by records in them (the efficiency principle).

Article 101. Radio frequency register

1. The Kyrgyz Republic shall have the exclusive right to distribute the radio frequency spectrum, allocate and assign radio frequencies in the Kyrgyz Republic. The distribution, allocation and assignment of frequencies shall be carried out in accordance with the obligations set forth in the manner established by legislation due to international treaties to which the Kyrgyz Republic is a party, and according to the Kyrgyz Republic legislation. The results of radio frequency spectrum allocation shall be recorded in the National Radio Frequency Allocation Table. Digital records of radio frequency spectrum usage rights, which are obtained through radio frequency allocation and assignment, constitute the radio frequency register.

2. The right to use the radio frequency spectrum shall be granted based on the telecommunications industry regulator's decision to allocate or assign radio frequencies, adopted in the manner prescribed by this Code, and be confirmed by an entry in the radio frequency register. The record in the register on the right to use the radio frequency spectrum shall be formed using the data specified in the relevant decision of the telecommunications industry regulator and updated, if necessary, according to the procedure established by this Code. The entry in the register shall not include data on the location coordinates of the radio-electronic equipment or high-frequency device, or on their technical characteristics.

3. The right to use the radio frequency spectrum shall be changed or terminated from the moment changes are made to the relevant record in the manner prescribed by this Code.

4. The radio frequency register owner shall ensure the completeness, reliability and relevance of the data in it and, for these purposes, shall interact with other state digital resource owners and with the records principals in the radio frequency register.

5. Digital records in the radio frequency register shall be publicly available. The telecommunications industry regulator shall provide access to the radio frequency register through a digital interaction system, and through an application and the state service website.

Article 102. Radio spectrum allocation

1. Radio frequency spectrum shall be allocated among radio services in accordance with the Radio Regulations of the International Telecommunication Union. The allocation results shall be reflected in the National table of radio frequency allocation among radio services of the Kyrgyz Republic (the National Radio Frequency Allocation Table), harmonized with the International Radio Frequency Allocation Table as part of the Radio Regulations. In any radio frequency band or part thereof, only those radio services may operate that are specified for that frequency band in the National Radio Frequency Allocation Table.

2. Changes to the National Radio Frequency Allocation Table shall be made by decision of the National Radio Frequencies Commission. Changes to the National Radio Frequency Allocation Table shall enter into force on January 1 of the year following the expiration of two years from the date of the National Radio Frequencies Commission's affirmative decision.

3. The radio frequency bands or parts thereof defined in the National Radio Frequency Allocation Table may be used in accordance with one of the following three categories:

1) for government use only;

2) for civil use only;

3) for joint government and civil use.

4. This Code does not regulate the radio frequencies allocation and assignment in the radio frequency bands for government use. Radio frequencies in radio frequency bands for joint government and civil use shall be allocated and assigned by decision of the telecommunications industry regulator based on the results of interdepartmental coordination. Radio frequencies in radio frequency bands for civil use shall be allocated and assigned by decision of the telecommunications industry regulator.

5. The National Frequencies Commission shall carry out the conversion of radio frequencies. The administrative, economic or technical measures necessary to implement the National Radio Frequencies Commission's decision on conversion shall be determined and implemented by the telecommunications industry regulator.

Article 103. Ensuring electromagnetic compatibility

1. Ensuring electromagnetic compatibility shall be a service of the telecommunications industry regulator, which includes:

1) analysis of the electromagnetic compatibility of radio-electronic equipment using the digital radio frequency register and, if necessary, the National Radio Frequency Table;

2) interdepartmental coordination for radio frequency bands (nominals) for joint government and civil use;

3) international coordination of the radio frequency band (nominal) or radio frequency assignment in cases provided for by international treaties of the Kyrgyz Republic;

4) identification of the actual interference situation in relation to radio frequency ratings or bands.

2. Based on the results of the service provision, the telecommunications industry regulator shall issue a conclusion that specifies the bands or nominals of radio frequencies and the territory in which they may be used. The conclusion shall be valid for 180 calendar days.

3. Radio monitoring for the purpose of managing the use of the radio frequency spectrum shall not result in increased fees for ensuring electromagnetic compatibility.

4. Radio frequencies shall be allocated and assigned once and privately to ensure electromagnetic compatibility. In case of general radio frequency allocation, electromagnetic compatibility shall be ensured on a quarterly basis. The electromagnetic compatibility conclusion shall specify the conditions under which the operation of radio-electronic equipment is permitted, as set out in the general assignment.

5. Radio frequency nominals and/or bands may not be used in the relevant territory if there is electromagnetic incompatibility, or in case of failure to obtain interdepartmental approval and/or international coordination.

6. The Cabinet of Ministers shall determine the procedure for calculating the amount of payment for ensuring electromagnetic compatibility.

7. The records principals using the radio frequency spectrum to fulfill public obligation, as well as those using the radio frequency spectrum for the amateur radio service and the amateur radio satellite service shall be exempt from the electromagnetic compatibility fees.

Article 104. Radio frequency allocation

1. The right to use a radio frequency or radio frequency band in a certain territory shall be granted by the telecommunications industry regulator decision to allocate them.

2. The allocation decision should contain:

1) the radio frequency nominals or bands in respect of which the right to use the radio frequency spectrum is granted;

2) spatial data that uniquely define the territory in respect of which the right to use the radio frequency spectrum is granted;

3) indication of the radio service in accordance with the National Radio Frequency Allocation Table.

3. Radio frequencies shall be allocated based on the results of tenders if the requested radio frequencies are classified as service frequencies in accordance with the telecommunications industry regulator's decision.

4. The telecommunications industry regulator shall make a decision to recognize radio frequencies as service frequencies if they simultaneously meet all of the following criteria:

1) radio frequencies are classified as for civil use;

2) radio frequencies shall not be used by existing radio electronic equipment;

3) the right to use the radio frequency does not belong, in whole or in part, to other persons;

4) the right to use radio frequencies is not disputed, and there are no restrictions or encumbrances imposed on them that prevent their intended use;

5) radio frequencies are not redistributed in the manner established by this Code;

6) radio frequencies are not intended for the state television and radio broadcasts;

7) radio frequencies are allocated for use in the technology that provides access to telecommunications services for an unlimited number of users.

5. Radio frequencies shall be allocated for a period of 10 years with the possibility of extension. For purposes not related to the telecommunications services provision, radio frequencies shall be allocated for a period of no more than 5 years with the possibility of extension.

6. The right to use radio frequencies may not be alienated by the record principal to other persons **except** in the manner prescribed by this Code.

Article 105. Assignment of radio frequencies

1. The operation of a radio-electronic equipment or high-frequency device shall be permitted only if there is the telecommunications industry regulator's decision to assign a radio frequency, with the exception of radio-electronic equipment and high-frequency devices included in the list of radio-electronic equipment and high-frequency devices for which no allocation or assignment of radio frequencies is required, approved by the Cabinet of Ministers. The assignment decision is made in relation to radio frequencies allocated in accordance with the National Radio Frequency Allocation Table.

2. Radio frequencies shall be assigned to radio-electronic equipment and high-frequency devices by the telecommunications industry regulator's decision and shall be private or general.

3. The industry regulator shall make decision on the general assignment of radio frequencies to radio-electronic equipment based on technology that prevents harmful interference during their simultaneous operation (cellular networks, broadband networks and other similar digital devices). In all other cases, the industry regulator shall make decision on private assignment. Radio-electronic devices in cases requiring international recognition of such devices shall be used based on private assignment, regardless of existence of the general assignment decision.

4. The decision to assign radio frequencies shall establish the following conditions, specified by the radio electronic equipment owner (high-frequency devices), under which the operation of such equipment (devices) is permitted:

1) telecommunication services provided using radio-electronic devices;

2) data on the permissible location of radio-electronic equipment (high-frequency devices) by indicating the coordinates (for private assignment) or territory (for general assignment), as well as the maximum and minimum number of radio-electronic equipment on the territory;

3) technical parameters of the radio-electronic device (high-frequency device).

5. The radio-electronic devices owner, operating them in accordance with the general assignment, shall interact with the telecommunications industry regulator by exchanging digital data that are important for assessing the electromagnetic environment around the radio-electronic equipment, namely:

1) data on the technologies used;

2) coordinates where the electronic equipment is installed;

3) data on operating frequencies;

4) data on the radiation power of the radio-electronic device and antenna parameters.

6. Radio frequency shall be assigned for a period of not less than 5 years with the possibility of extension, with the exception of service radio frequencies, in which a radio frequency is assigned for the duration of the right to use radio frequencies in accordance with the decision on their allocation.

Article 106. Radio spectrum usage fee

1. To use the radio frequency spectrum, the records principals should pay an annual fee calculated based on the methodology established by the Cabinet of Ministers. The fee for use of the radio frequency spectrum should encourage the records principals to:

1) efficiently and economically use the radio frequency spectrum;

2) introduce new digital technologies.

2. The fee calculation method shall directly or indirectly take into account the following factors:

1) location of the radio electronic device or the declared territory of use;

2) population density;

3) width of the radio frequency band used or the radio frequencies nominal;

4) weighting coefficient that includes commercial price and social factor;

5) calculation indicator;

6) efficiency factor of using the radio frequency nominal or band.

3. When a new frequency band is allocated or new technologies that use the radio frequency spectrum are applied requiring replacement of the radio-electronic equipment of the network in operation, an additional reduction coefficient shall be applied to calculate the annual fee, taking into account the time required for the development of the telecommunications network (no more than three years).

4. The fee for use of the radio frequency spectrum shall be sent to the republican budget and is taken into account when determining the amount of funding for the telecommunications industry regulator’s activities.

5. The records principals shall be exempt from paying fees for certain radio frequency bands when using them exclusively for the following:

1) amateur radio service and amateur radio satellite service;

2) fulfillment of public obligations imposed on them in accordance with the legislation.

6. No fee shall be charged for the use of frequency assignments within the radio frequencies allocated in accordance with part 3 of Article 104 of this Code.

Article 107. Use of radio spectrum

1. The radio frequency spectrum shall be used in the Kyrgyz Republic by the records principals in accordance with the parameters of records in the digital radio frequency register.

2. The records principals should limit the number of frequencies and the width of the radio frequency spectrum used to the minimum required to achieve the purposes for which the radio frequency spectrum is used.

3. Distress calls should be given absolute priority, and all such data should be responded immediately, and the required measures should be taken without delay. Subject of legal relations in the digital environment should take measures to prevent dissemination of false or misleading distress, urgency, security or identification signals and cooperate, where necessary, with other subjects of legal relations in the digital environment in determining the location of such signal's sources.

4. The President shall determine the procedure for using the radio frequency spectrum in the interests of national security and defense. When using the radio frequency spectrum for the specified purposes, the following should be observed:

1) provisions of part 3 of this Article regarding distress signals and adoption of measures to prevent interference;

2) provisions of the Radio Regulations of the International Telecommunication Union.

Article 108. National Radio Frequencies Commission

1. The National Radio Frequency Commission is a collegial body that coordinates interdepartmental activities in the radio frequency spectrum allocation process. The composition of the National Radio Frequency Commission and the procedure for its work shall be determined by the Cabinet of Ministers; its chairman is the head of the telecommunications industry regulator.

2. The National Radio Frequency Commission shall maintain the National Radio Frequency Allocation Table by performing the following tasks:

1) allocation of radio frequencies based on a reasonable balance between civil and governmental use of the radio spectrum, both of which are of equal importance for the country;

2) harmonization of the National Radio Frequency Allocation Table with the International Frequency Allocation Table;

3) radio frequency conversion;

4) formation of principles for the radio frequency resources use on the territory of the Kyrgyz Republic.

3. The National Radio Frequency Commission shall prepare proposals for the Cabinet of Ministers regarding amendments to normative legal acts that address the tasks assigned to the National Radio Frequency Commission.

4. Draft normative legal acts of the Cabinet of Ministers affecting the radio frequency use spectrum shall be subject to discussion at the National Radio Frequency Commission.

5. When making decisions, the National Radio Frequency Commission shall be guided by:

1) provisions of this Code and other normative legal acts of the Kyrgyz Republic affecting the radio frequency spectrum use;

2) intergovernmental and regional agreements affecting the radio frequency spectrum use;

3) decisions of world and regional radiocommunication conferences;

4) current and future needs of the Cabinet of Ministers for the radio frequency spectrum for the purposes of national security, defense, law enforcement and emergency response, as well as for other government purposes;

5) existing and future needs of telecommunications operators, mass media and other radio frequency spectrum users.

6. The National Radio Frequency Commission shall carry out its activities free of charge. The telecommunications industry regulator shall be responsible for preparing the necessary documents and providing organizational, methodological, and other assistance to the National Radio Frequency Commission.

7. Decisions of the National Radio Frequency Commission shall be formalized by a decision of the Cabinet of Ministers or an act of a state body determined by the Cabinet of

Ministers, and be published on the website of the telecommunications industry regulator within three business days after their adoption.

Article 109. Digital numbering register

1. In accordance with the international obligations of the Kyrgyz Republic, the exclusive right to allocate the numbering included in the National Numbering Plan approved by the Cabinet of Ministers shall belong to the Kyrgyz Republic. Digital records of ownership of rights to use numbering obtained through the numbering range allocation shall constitute the numbering register.

2. The right to use numbering shall arise, change or cease from the moment the corresponding entry is created in the numbering register or changes are made to it in the manner prescribed by this Code.

3. The digital numbering register owner shall ensure the completeness, reliability and relevance of the data in the digital numbering register and, for these purposes, shall interact with the owners of other state digital resources.

4. Digital records in the digital numbering register shall be publicly available. The telecommunications industry regulator shall provide access to the digital numbering register through the digital interaction system, and through the state services application and website.

Article 110. Using numbering

1. The records principals should pay an annual fee for the numbering use, in the amount established by the Cabinet of Ministers. There shall be no charge for using short numbers by emergency services.

2. The use of numbering that is not included in the digital numbering register, or the use of numbering by a person who is not the record principal shall be prohibited. Information regarding the numbering allocation, change, re-registration or withdrawal may not be considered as commercial secret.

3. In case of full or partial termination of the right to use the numbering, the fee for using the numbering shall not be refunded.

4. If decision is made to change the national numbering plan, resulting in significant change in the structure or format of a number or code, such a decision should be published at least 2 years before the planned changes take effect. The telecommunications industry regulator should notify all affected parties of the procedure for re-registering the relevant decisions on the numbering allocation, to all records principals affected by the decision within three business days of the decision being made.

5. The decisions specified in part 4 of this Article shall constitute grounds for changing the number of telecommunications service users without their consent. Notification of them of the timing and reason for such a change shall be provided via the website or application of the telecommunications operator (virtual operator), as well as by sending messages. Notification should be given at least 6 months prior to the planned change of user numbers.

Article 111. The national system digital register

1. The national ecosystem digital register shall provide the possibility of using the national ecosystem elements, the possibility of their interaction, and their compatibility.

2. The national ecosystem digital register shall consist of digital records of the national ecosystem elements, each containing data:

1) about the owner (supplier) of the national ecosystem element;

2) about the users (consumers) of the national ecosystem element;

3) about state services in which the national ecosystem element is used;

4) about other national ecosystem elements with which this national ecosystem element interacts (interacting elements);

5) on the methods of using the national ecosystem element;

6) on the results of using the national ecosystem element, including in interacting elements;

7) about persons responsible for ensuring protection of the national ecosystem element, their contact information;

8) on indicators characterizing the availability of the national ecosystem element (maximum period of unavailability per year, timeframe for restoring availability in case a failure, simultaneous number of users);

9) about the data formats and data exchange interfaces used.

3. An object of legal relations in the digital environment shall be included in the national ecosystem digital register on a voluntary basis and free of charge. The owner (supplier) of an object of legal relations in the digital environment shall have the rights and obligations of a participant in the national ecosystem from the date of inclusion of his/her object in the national ecosystem digital register and until the record is made in the corresponding national ecosystem element on his/her exclusion from the national ecosystem elements.

4. The conditions for inclusion of an object of legal relations in the digital environment in the national ecosystem digital register shall include:

1) ensuring compatibility and interaction of the object of legal relations in the digital environment with other elements of the national ecosystem;

2) presenting positive results of testing the functionality and digital resilience of the object of legal relations in the digital environment using the state services factory;

3) providing data specified in part 2 of this Article and necessary to create a digital record on a national ecosystem element.

5. Within 5 business days of receiving data from the owner of the object of legal relations in the digital environment confirming that the conditions for inclusion of the object of legal relations in the digital environment in the national ecosystem digital register have been met, the national ecosystem industry regulator shall create a digital record of the new element in the national ecosystem digital register.

6. The national ecosystem industry regulator shall make changes to a digital record in the national ecosystem digital register upon request of the owner (supplier) of the corresponding national ecosystem element. In case of exclusion of an object of legal relations in the digital environment from the national ecosystem elements, the relevant data shall be entered into the record of this element.

7. Digital records in the national ecosystem digital register shall be publicly available. The national ecosystem industry regulator shall provide access to the national ecosystem digital register through the digital interaction system, and through the state services application and website.

SECTION IV
DIGITAL SERVICES AND ECOSYSTEMS

Chapter 14. General Provisions on Digital Services

Article 112. Legal regulation of digital services

1. Digital services shall be provided to users according to the rules established by the providers of such services, in compliance with the mandatory requirements stipulated by this Code.

2. The rules of digital services established by their providers should take into account generally accepted international practice when choosing technologies or methods of digital identification and digital authentication of users and their access to their data.

3. The provision of digital welfare services, telecommunication services, trusted services and state services shall be regulated in accordance with the rules of this chapter, taking into account the additional requirements and restrictions established by the relevant chapters of this Code. The subjects of such relationships shall enjoy all the rights provided for in this chapter and shall bear the responsibilities associated therewith.

Article 113. Industry principles for digital services regulation

1. The ability to use digital services should be available to all persons in need, including disabled persons (the inclusiveness principle).

2. The legal regulation of digital services shall protect the interrelated interests of providers and users of such services in receiving the benefits of digital data processing (the mutual protection principle).

3. Digital service providers may not be required to obtain a license or other prior approval from the authorized state bodies (the principle of no prior authorization).

4. To be able to use digital services the users should not be required to purchase a digital device from the service provider (the principle of freedom of user devices).

5. The ability to use digital services may not be dependent on the location of user data (the principle of geographic non-discrimination).

6. Rules for using the service should not discriminate against users based on gender, race, language, disability, ethnicity, religion, age, political or other beliefs, education, origin, property or other status, other circumstances, and unless expressly stated in the user agreement, the location of users or user data used by the digital device users (the principle of non-discrimination of users).

7. Digital service providers and their users shall be jointly responsible for ensuring digital resilience of a digital service (the reciprocity principle).

Article 114. User agreement

1. Use of a digital service shall be based on an agreement between the provider and the service user (user agreement), in which the user undertakes to comply with the service use rules. Using the digital service without a user agreement shall not be permitted, except when the service use rules are established by law or normative legal acts adopted in accordance with it.

2. All information that the digital service provider is obliged to provide to the user in accordance with the legislation should be available before concluding a user agreement.

3. In accordance with applicable law, a user agreement may be concluded in any form that enables to identify the user, and confirm the agreement conclusion and its terms.

4. The digital service provider should store digital records that confirm the terms of the user agreement regarding a specific user and the fact of execution of the user agreement by the parties for the entire term of the user agreement and for three years after its termination. The terms of the user agreement and other digital records regarding the conclusion and execution of the user agreement should be made available to the user in a manner that allows the user to retain and reproduce them.

5. If it is necessary to make changes to the user agreement, the supplier shall be obliged to notify the user of the changes being made by any available means and set a period of at least one month. The user agreement shall be considered to be amended from the date specified in the notification, unless the user has received a refusal to amend the user agreement prior to that date. If before expiration of the specified period the user declares disagreement with the proposed changes, the user agreement shall be terminated, and the digital service provider shall

be obliged to return the funds paid by the user, minus the cost of the digital service up to the moment of receiving the user's statement of disagreement with the changes being made, taking into account the specifics established by other normative legal acts for certain types of digital services.

6. The digital service provider may not restrict access to digital records related to the user agreement or its performance by the parties in a manner that prevents the automatic translation of these records content into the state or official language, unless this information is already presented in the state and official languages.

Article 115. Digital service provider

1. A subject of legal relations in the digital environment that provides a digital service and determines the rules for using such service shall be obliged to clearly and in a way that users understand identify himself/herself as a digital service provider and make the information about the digital service provided for by this Code publicly available.

2. If several subjects are involved in providing a digital service or determining the rules for its use, they should determine which of them is authorized to enter into a user agreement. Unless otherwise specified in the user agreement, all subjects of legal relations in the digital environment, providing a digital service and defining the rules for its use, shall be liable to the user jointly and severally.

3. A digital service provider shall be prohibited to:

1) process users' digital data for purposes other than those specified in the user agreement, except as required by the applicable legislation;

2) engage in unfair competition, perform actions restricting competition;

3) restrict the users' rights provided for by this Code and other legislation of the Kyrgyz Republic, including by taking technical measures that impede access to digital data necessary for users to exercise and protect their rights.

Article 116. Digital services users and consumers

1. The user shall be obliged to maintain his identity during the term of the user agreement. Digital identification and digital authentication of the user shall be performed in accordance with the digital identification system rules used by the service provider in accordance with this Code.

2. Unless otherwise provided in the user agreement, the digital rights to digital records created by the user when using the digital service shall belong to the user.

3. Users shall be obliged to respect the intellectual property rights of others when using digital services and be responsible for their non-compliance.

4. Consumers shall have the following additional rights:

1) to refuse a digital service at any time at the consumer's discretion with the right to a refund of all funds paid minus the cost of the digital service before the consumer refuses it, taking into account the specific features established by other normative legal acts for certain types of digital services;

2) to receive sufficient information, free of charge, to set up the consumer's digital device for the purpose of receiving digital service and resolving malfunctions caused by the settings of the consumer's digital device (consumer support);

3) to request that all digital records relating to the consumer be deleted after opting out of the digital service, except for records that the service provider is required to keep under the Kyrgyz Republic laws.

Article 117. Protecting competition in digital services

1. When providing digital services, the prohibited actions, in addition to those provided for by the antimonopoly legislation of the Kyrgyz Republic, shall include:

1) manipulation of the search results algorithm;

2) prioritization of own digital services or goods, works, services of this provider;

3) ability to receive a digital service only if certain goods (digital devices), works, services or digital services of the provider or others are purchased;

4) requirement of transfer of intellectual property rights as a condition for the digital service use;

5) limited ability to use other digital services or transfer the user's digital records to other digital services;

6) requirement of compulsory participation in marketing promotions or other similar activities of the digital service provider or others;

7) creation of priority for some users over others based on the user’s location or digital data;

8) deletion of messages and comments that do not contain information, the distribution of which is prohibited by law;

9) dumping or cross-subsidization.

2. The digital service provider shall not acquire digital rights or intellectual property rights to objects of legal relations in the digital environment belonging to users. Such objects may only be used upon conclusion of an agreement for their use, in the manner established by this Code or the civil legislation of the Kyrgyz Republic. The supplier shall be obliged to keep digital records confirming the fact of conclusion of the agreement for the use of the relevant objects and the conditions of their use.

Article 118. Right to refuse service

1. If under the user agreement, this Code or applicable law, the user has declared his/her refusal of the digital service, the digital service provider shall be obliged to:

1) calculate the payment received under the user agreement, the cost of the digital service up to the moment of receiving the refusal message and determine the amount to be returned to the user or the amount to be paid to the supplier for the digital service used;

2) provide the user with data about the user's digital records held by the digital service provider;

3) inform the user of possible options for obtaining a copy of all digital user records available with the digital service provider, as well as the possibility of transferring digital records to other digital services;

4) provide the user with the opportunity to delete his digital records and ensure such deletion;

5) until the user's decision regarding his/her digital records is obtained - keep all of the user's digital records in an unaltered form.

2. If, after the user's refusal, the digital service provider has not received the user's decision regarding their digital records, the digital service provider shall be obliged to delete all of the user's records at the end of one calendar year following the year in which the user refused the digital service.

3. The provider shall not be entitled to delete the digital user’s records containing information that provider is required to keep under the Kyrgyz Republic laws. The provider should notify the user of the digital records composition that will continue to be stored.

Article 119. Dispute consideration

1. The digital service provider shall be obliged to provide the ability to submit complaints via its website or application:

1) regarding the digital service quality;

2) on violations of intellectual property or digital rights;

3) on violations of the rules of the service use;

4) regarding the digital records distribution or the provision of access to them, if such actions are restricted under the Kyrgyz Republic legislation;

5) other violations of the existing Kyrgyz Republic legislation.

2. If the complaint relates to the digital service users' actions, the service provider shall be obliged to inform each of them of receipt of the complaint and provide all data related to the received complaint.

3. The digital service provider shall be obliged to take necessary measures to eliminate the violations specified in the complaint within five business days. If a longer period of time is required to correct the violations specified in the complaint, the provider shall notify the user within five business days, with justification for the period required to correct the violations. The digital service provider should inform the complainant in the same way as the complaint was sent, unless the complainant has requested another form of notification.

4. The digital service provider that enables users to exchange digital data with other users shall be obliged to ensure that disputes between users are resolved according to the service use rules specified in the user agreement and/or published on the provider's website or application.

5. The digital service provider's decisions on a complaint or dispute may be appealed in a mandatory pre-trial procedure to the industry regulator, and in case of disagreement with the industry regulator's decision - in court, in accordance with the Kyrgyz Republic legislation or other applicable legislation based on the parties' agreement. The industry regulator, as part of the consideration of complaints and disputes, verifies the compliance of the parties' actions with the user agreement and the compliance of the user agreement with the Kyrgyz Republic legislation. When making decision on a complaint or dispute, the industry regulator may not be guided by the user agreement provisions that contradict the Kyrgyz Republic legislation.

Article 120. Responsibility

1. The digital service provider may suspend a user's access to the service if he/she violates the user agreement until the violation is resolved.

2. Unless otherwise specified in the user agreement, the digital service provider shall be liable to the user for unavailability of digital service at double price of the service, calculated for each full hour, in which the digital service was unavailable to the user. When determining the extent of the provider's liability, time spent on emergency or repair and maintenance work in the volumes and procedure stipulated by the user agreement shall not be considered.

3. If a digital service is delayed or a digital service is of inadequate quality, the digital service provider shall be liable to the user in an amount not exceeding the price of the relevant digital service for that period, in proportion to the delay or deterioration.

4. If the user is not provided with data necessary for calculating the cost of the digital service for the relevant period, the provider shall be liable to the user for the cost of the digital service for that period.

5. The digital service provider shall fully compensate any damage caused to the user by unavailability of the information provided for by this Code or by the provision of an inadequate digital service, including that which led to the loss of the user's digital records, based on a court decision.

Chapter 15. Digital Wellness services

Article 121. Legal regulation of digital wellness services

1. Digital wellness services may be freely created and used in the Kyrgyz Republic, subject to the restrictions established by this Code.

2. The Kyrgyz Republic legislation on the protection of citizens' health shall regulate the use of digital wellness services by medical organizations and private medical practitioners. The use of digital wellness services as part of medical activities should not lead to the infringement of the individuals' rights and legitimate interests.

3. In cases where the Kyrgyz Republic legislation permits the provision of medical and sanitary assistance subject to the establishment of an individual's identity, the digital authentication of the service consumer shall be carried out using digital authentication services in accordance with this Code.

4. The use of digital welfare services may not be restricted based on the location of their providers, users or places where digital records are processed.

Article 122. Industry principles for regulating digital wellness services

1. Decisions concerning an individual's health, including diagnosis, can only be made by a human (the human decision-making principle).

2. Before using the digital wellness service, the consumer should have full information about the service capabilities and limitations, and terms of its use (the consumer awareness principle).

3. The results of the digital wellness service, including those realized automatically, should be accompanied by data accessible to the consumer on the consequences of using or not using each of the service results (the result predictability principle).

4. Data disseminated about the service of digital wellness cannot contain unsubstantiated guarantees or assurances of improvement in the consumer's quality of life and health (the substantiated result principle).

5. Data on the performance of the digital wellness service in relation to a particular consumer should be available to the consumer in the form of digital records (the accountability principle).

Article 123. Using digital services for health care purposes

1. Except where expressly prohibited by law, the digital services may be used as part of health care for the following purposes:

1) counseling;

2) the patient's condition monitoring;

3) exchange of experience and mutual consultation between medical professionals;

4) training of healthcare workers;

5) compliance with sanitary and hygienic, sanitary and anti-epidemic regimes.

2. Digital records should be taken into account when providing health care if they are created as part of digital services.

Article 124. Data processing as part of digital wellness services

1. The Kyrgyz Republic provides processing of digital data on the health of citizens of the Kyrgyz Republic within the national ecosystem.

2. The digital data of consumers of a digital wellness service may be used to improve the service for all its consumers.

3. The digital wellness service provider may process the consumers' digital data for the purposes of other digital services, as well as the transfer such data to other persons (except the processor), only if there is a basis for processing provided for in this Code, and if such basis is a legitimate interest, only if the data is depersonalized.

4. The digital wellness service provider should ensure data quality based on its approved methodology, which includes:

1) description of the ways of processing digital data to prepare them for use;

2) description of the models and hypotheses within which the digital data are used;

3) preliminary assessment of availability, sufficiency and suitability of the necessary digital data;

4) ways of checking the sample for bias (for sampling bias and for sampling error);

5) methods of identifying gaps in the data quantity and quality, and ways addressing these gaps.

5. Digital data for digital wellness services should be relevant, representative, error-free, and complete. They should take consider the purpose of the digital service and the intended conditions of its use, including the statistical characteristics of individuals and groups of service users, to the extent necessary.

6. The service provider should make the data quality assurance methodology publicly available on its website or in the application through which the digital service is accessed.

Article 125. Digital wellness devices

1. Requirements for digital technological systems and their elements used within the digital wellness services (digital wellness devices), as well as forms of conformity confirmation shall be established in accordance with the Kyrgyz Republic technical regulation legislation.

2. Consumers may use digital wellness devices that do not involve penetration through the body's natural external barriers (non-invasive digital devices) without prior approval or verification of compliance.

3. A digital wellness service provider shall be required to make the following data on the digital wellness devices publicly available on its website or application:

1) a list of digital devices that can be used within the service, or requirements for such devices;

2) rules of use of digital wellness devices within the service;

3) references to standards, specifications or other similar documents, which the devices comply with, and information on the confirmation of the device compliance with provisions of such documents.

4. The digital wellness service provider shall be obliged to ensure that consumers can use any devices that meet the provider’s published requirements without any discrimination against their manufacturer or model.

5. When determining the device requirements, formats, and interfaces for data exchange with devices, the digital wellness service provider shall consider the internationally recognized practices.

Article 126. Using the artificial intelligence systems for digital wellness

Artificial intelligence systems used to ensure digital wellness shall be classified as high-risk artificial intelligence systems. A digital welfare service provider that uses artificial intelligence systems as part of the service shall comply with the requirements for high-risk artificial intelligence systems set forth in this Code.

Article 127. Protecting the rights of the digital wellness services consumers

1. The digital wellness service consumer shall have the right to compensation for damage (including moral damage) caused to him/her resulting from the use of the digital wellness service or from the unavailability of data that should be available to consumers in accordance

with this Code. Compensation for moral damage shall be paid regardless of compensation for the property damage and losses incurred by the consumer.

2. The digital wellness service consumer may demand compensation from the provider in the amount one hundred to four hundred calculation indices instead of receiving for damage and/or moral damage. Compensation shall be paid upon proof of the fact of a violation committed by the provider and occurrence of damage to the consumer. The amount of compensation shall be determined at the court's discretion based on nature of the violation and other circumstances of the case and should be reasonable and fair.

3. The digital wellness service provider shall be exempt from the damage compensation if he/she proves that there is no causal link between the use of his/her digital service and the damage occurred to the consumer.

Chapter 16. Telecommunication services

Article 128. Legal regulation of telecommunication services

1. The Kyrgyz Republic shall regulate telecommunications services based on international treaties and decisions of international telecommunications organizations, of which the Kyrgyz Republic is a member. Unless otherwise specified in this Code, terms related to telecommunication services shall be used in the meaning established in the documents of the International Telecommunication Union.

2. The telecommunications services should be provided and regulated taking into account the generally accepted international practice in the field of telecommunications. If the Kyrgyz Republic legislation requires confirmation of compliance with the requirements established by this Code, documents obtained in accordance with the legislation of foreign states may be used if they confirm compliance with requirements that are equivalent to or higher than the requirements established by this Code.

Article 129. Industry principles for regulating telecommunications services

1. Subjects of legal relations in the digital environment shall have the right to freely provide telecommunications services and use them in the Kyrgyz Republic (the freedom of telecommunications principle).

2. Regulation of telecommunications services shall ensure the continuity of their provision to providers and users, and it prohibits the arbitrary termination of telecommunications services (the continuity principle).

3. Regulation of activities related to the provision of telecommunications services and their use shall ensure their continuous development and the introduction of advanced technologies for their provision in accordance with generally accepted international practice (the development principle).

4. Telecommunication services and their regulation should be organized in such a way as to increase the number of users who can interact with each other using telecommunication services (the interaction principle).

5. Sustainable development of telecommunications services and the implementation of the regulation principles shall only be possible if the compatibility of services and digital devices used to provide services and use them is ensured (the compatibility principle).

6. When providing telecommunications services and using them, the integrity and inviolability of the transmitted digital data shall be ensured, while telecommunications service providers should not control the transmitted digital data content and bear liability in connection with their content (the inviolability principle).

7. The telecommunications service providers shall independently set prices and tariffs for telecommunications services, taking into account the requirements established by the Kyrgyz Republic legislation in the area of pricing (the pricing freedom principle).

Article 130. Protecting the privacy of digital data transmitted via telecommunications service

1. The Constitution and this Code shall protect privacy of correspondence, telephone and other conversations, as well as other messages transmitted using telecommunications services.

2. Access to data constituting such secret shall be granted only to the senders and recipients of such data (messages), and also to persons involved in the functioning and operation of the telecommunications network and (or) the provision of telecommunications services, when technically possible.

Access to data constituting such secret by other persons shall be permitted only in accordance with the law and based on a court act. Access to data shall be provided for each user separately based on a court order issued regarding him/her and for the period specified in such act.

3. Unauthorized connection or other interference with telecommunications services for the purpose of obtaining, changing or otherwise processing data transmitted using them shall be prohibited.

4. If a telecommunications service is used for the purpose of providing public access to data (in particular, when broadcasting or posting on a website), such data shall not refer to the privacy of correspondence, telephone and other conversations, as well as other messages transmitted using the telecommunications service.

Article 131. Provision of telecommunication services

1. Telecommunication services shall be provided around the clock, unless otherwise expressly stated in the user agreement. Telecommunications service providers shall be required to take measures to ensure the digital resilience of telecommunications services, and to promptly identify and eliminate interruptions in their provision.

2. At least three business days before maintenance and repair work that may cause interruptions in the provision of telecommunications services begins, the telecommunication service providers should inform user on their website or in their application.

3. In case of an accident or other incident affecting the provision of a telecommunications service, the service provider should inform users on its website or in the application about the incident, its impact on the service and the planned time frame for its resolution.

4. Users of telecommunication services shall be provided with 24/7 technical support. The provider shall be obliged to post the contact information of the technical support service on its website or in the application.

5. If the cost of a telecommunications service is calculated based on the usage volume, the provider shall be obliged to publish information about the manufacturer and the model of the billing system used to calculate the usage volume of the telecommunications service.

6. When providing telecommunications services in the territory of the Kyrgyz Republic, Bishkek accounting and reporting time shall apply, unless otherwise established by an international treaty that has entered into force in accordance with the Kyrgyz Republic legislation.

Article 132. Purposes of using telecommunication services

1. The user shall have the right to use telecommunications services for any purposes, unless this Article or the user agreement provides that a telecommunications service may be used for certain purposes only with the express consent of the service provider.

2. The user shall be obliged to store digital records allowing to confirm the service provider's consent to use the service for any of the following purposes:

1) lotteries, voting, competitions, quizzes, surveys of other users of this telecommunications service;

2) distribution of advertisements among this telecommunications service users or mass mailing of digital records to them;

3) installation of gateways between different telecommunication services;

4) research of the telecommunications service, including by testing its protection.

3. A provider or user of a telecommunications service who uses it to distribute advertisements to that telecommunications service users should be obliged to obtain the prior consent of the users to do so and to store digital records allowing to confirm the users' consent to receive advertisements.

Article 133. Broadcasting services

1. Broadcasting services used for distribution in the Kyrgyz Republic include:

1) television and radio channels registered in the territory of the Kyrgyz Republic as mass media and having the appropriate permit for placement in analogue broadcasting and (or) in a digital broadcasting package, issued in accordance with the television and radio broadcasting legislation;

2) foreign TV and radio channels.

2. Television and radio channels shall be formed in accordance with the Kyrgyz Republic television and radio broadcasting legislation and other mass media normative legal acts of the Kyrgyz Republic.

3. Broadcasting service providers shall be obliged to distribute the received television and radio channels in their original form. Television and radio channels may be changed only if they are registered as a broadcasting organization in accordance with the television and radio broadcasting legislation.

Article 134. Provision of telecommunication services under special conditions

1. Telecommunication services shall be used on a priority basis for transmitting messages in cases of:

1) threat to life and health of people;

2) emergency situations and rescue operations.

2. The law shall establish conditions for sending messages for the needs of public administration, national security, defense, law enforcement and other similar purposes.

3. The telecommunications operators shall transmit the messages provided for in part 1 of this Article and call the emergency services free of charge.

4. The telecommunications operator shall be obliged to provide spatial data of the user equipment (terminal equipment) from which calls were made or messages about an incident were transmitted, and other data necessary to ensure a response to a call or message about an incident to dispatchers of emergency services (fire and rescue services, public order services, emergency health care, rescue services).

5. The Cabinet of Ministers shall determine national telecommunications operators that:

1) perform a special procedure for working with and interacting with subjects of legal relations in the digital environment in accordance with their assigned rights and obligations, as approved by the Cabinet of Ministers;

2) ensure the continuity of the existing telecommunications infrastructure, create and maintain the necessary reserve of telecommunications equipment and materials in emergency situations for the purposes of public administration, national security, defense, and law enforcement at the expense of the republican budget;

3) provide telecommunications services for the purposes of implementing state social projects to ensure the telecommunications services availability throughout the Kyrgyz Republic territory, including in hard-to-reach and sparsely populated areas;

4) may not suspend or interrupt the operation of telecommunications networks or the provision of telecommunications services without prior permission from the telecommunications industry regulator for the purposes of public administration, national security, defense, law enforcement, and emergency situations.

Chapter 17. Trusted services

Article 135. Legal regulation of trusted services

1. This Code and normative legal acts adopted in accordance with it shall regulate relations regarding the use of digital signatures and digital archives.

2. The procedure for using a digital signature in a digital ecosystem shall be established by the owner of this system or by an agreement between the digital interaction participants in the digital ecosystem.

3. The types of digital signatures used by executive authorities and local government bodies, as well as requirements for ensuring the compatibility of such digital signatures, shall be established by the Cabinet of Ministers.

4. The Kyrgyz Republic laws may establish specifics for the trusted services use in the following types of relationships:

1) preparation and holding of elections and referendums;

2) execution of civil law transactions;

3) provision of state services;

4) implementation of payments and banking operations;

5) accounting and tax records management.

Article 136. Digital signature and digital archive services

1. Digital signature services and digital archive services shall refer to trusted digital services aimed at certifying the occurrence, change, and termination of legal relations in the digital environment.

2. To work with digital signatures, their provider and users shall use digital signature tools, which are encryption (cryptographic) digital technological systems.

3. Digital archives shall store digital records containing digital signatures, together with the digital signature tools needed to work with such signatures.

Article 137. Industry principles for regulating relations on the trusted services use

1. Subjects of legal relations in the digital environment shall have the right to use any trusted service at their own discretion, unless the use its specific type in accordance with the purposes of their use is provided for by law or an agreement of subjects of legal relations in the digital environment.

2. Subjects of legal relations in the digital environment shall have the right to use any technology and (or) technological system that allows them to fulfill the requirements of this Code in relation to digital signatures, digital archives or other trusted services.

3. The requirements for the use of a specific type of digital signature or digital archive established in legislative and other normative legal acts should correspond to the purposes of their use.

4. A digital signature and (or) digital record, the integrity of which is ensured by the digital signature, cannot be recognized as having no legal force solely on the grounds that the digital signature is not a handwritten signature or that the document is stored in a digital archive.

Article 138. Types of digital signatures

1. The types of digital signatures are unqualified digital signature (hereinafter referred to as unqualified signature) and qualified digital signature (hereinafter referred to as qualified signature).

2. An unqualified signature shall be a digital signature that meets the following criteria:

1) is obtained as a result of cryptographic transformation of digital data using a digital signature key;

2) uniquely associated with the signer;

3) allows to uniquely identify the person who signed the digital record;

4) allows to detect the fact that changes have been made to a digital record after it has been signed;

5) is created using digital signature means that the person who signed the digital record is able to keep under his/her control.

3. If the digital signature can be verified as an unqualified signature without using a signature verification key certificate, then a signature verification key certificate may be not created when using an unqualified signature.

4. A qualified signature shall be a digital signature that meets all the features of an unqualified signature and the following additional features:

1) the digital signature verification key is specified in the qualified certificate;

2) to create and verify a digital signature, digital signature tools that have received confirmation of compliance with the requirements established in accordance with this Code are used.

5. A legal entity's digital signature shall serve as confirmation that the digital record originates from the legal entity and serves as proof of the document's integrity after the digital signature is created.

6. Signature verification key certificates, in relation to which verification is carried out by a trusted third party of the Kyrgyz Republic, and in case of technical impossibility of using a trusted third party - by a foreign trusted service included in the Foreign Trusted Digital Services Register, shall be equivalent to the qualified certificates issued by an accredited certification center.

Article 139. Conditions for recognition of digital records signed with a digital signature as being equivalent to paper documents signed with a handwritten signature

1. A digital record signed with a qualified signature shall be recognized as a digital document equivalent to a paper document signed with a handwritten signature, except in cases where legislation prohibits the preparation of such a document in digital form.

2. A digital record signed with an unqualified signature shall be recognized as a digital document equivalent to a paper document signed with a handwritten signature in the cases established by:

1) normative legal acts;

2) agreement of the subjects of legal relations in the digital environment, unless normative legal acts prohibit such a document to be developed in a digital form.

The specified normative legal acts and agreements of subjects of legal relations in the digital environment should provide for the procedure for verifying a digital signature.

3. If, in accordance with normative legal acts or business practices, a paper document should be certified with a seal, a digital document signed with a digital signature shall be recognized as equivalent to a paper document signed with a handwritten signature and certified with a seal. Normative legal acts or agreements between subjects of relations in the digital environment may provide for additional requirements for a digital document to recognize it as equivalent to a paper document certified by a seal.

4. A package of digital documents i.e., several interconnected digital documents can be signed with one digital signature. When signing a package of digital documents with one digital signature, each document in it shall be considered as signed with a digital signature of the type with which the digital documents package is signed.

5. If the Kyrgyz Republic normative legal acts impose special requirements on paper documents using strict reporting forms, then a digital document signed with a qualified digital signature is considered to comply with these requirements.

Article 140. Foreign digital signatures and archives

1. In the Kyrgyz Republic, any methods of creating a digital signature and digital archives that comply with the requirements established by this Code, as well as international standards in the field of digital signatures and digital archives, may be used.

2. Digital signatures created in accordance with the legal norms of a foreign state shall be recognized in the Kyrgyz Republic as digital signatures of the type that they correspond to in accordance with this Code.

3. A digital signature and a digital document signed by it cannot be considered invalid solely because the signature verification key certificate was issued in accordance with the laws of a foreign state, even such a signature does not comply with the digital signature requirements established by this Code.

4. Recognition of the authenticity of foreign digital signatures shall be carried out:

1) by a trusted third party, and in case of technical impossibility of using a trusted third party, by a foreign trusted service included in the Foreign Trusted Digital Services Register, in the manner established by this Code;

2) by a court, in the context of determining whether a foreign trust service use by a party meets the criteria established by this Code.

5. The procedure for exercising the functions of a trusted third party of the Kyrgyz Republic shall be established by the Cabinet of Ministers.

Article 141. Obligations of subjects of legal relations in a digital environment when using a digital signature

Subjects of legal relations in the digital environment when using a digital signature shall be obliged to:

1) ensure confidentiality of the digital signature key, including preventing the use of their digital signature keys without their consent;

2) exercise reasonable care to prevent unauthorized use of the digital signature or the data required to create it;

3) immediately, but no later than one business day following the day of receipt of information about the breach of confidentiality of the signature key, notify the certification center that issued the signature verification key certificate and other participants in legal relations about such breach;

4) not to use the digital signature key if there is reason to believe that its confidentiality has been violated;

5) use digital signature tools that have received confirmation of compliance with the requirements established in accordance with this Code to exchange digital documents signed with a qualified signature;

6) ensure the accuracy and timely updating of the data required for the use of the digital signature verification key certificate;

7) take reasonable measures to verify the digital signature authenticity.

Article 142. Recognition of the qualified signature authenticity

1. Until a court decision establishes otherwise, a qualified signature shall be considered authentic if the following conditions are simultaneously met:

1) a qualified certificate containing a signature verification key has been created and issued by an accredited certification center, and the accreditation of such certification center shall be valid (not suspended, terminated, or revoked) on the date of issue of the said certificate;

2) a qualified certificate containing a signature verification key is valid (has not expired, has not been canceled) on the day of signing a digital document (if there is reliable information about the moment of signing a digital document) or on the day of verification - if the moment of signing is not defined;

3) the ownership of the specified qualified digital signature certificate used to sign the given digital document has been verified, as well as the absence of changes made to this document after it was signed, while the verification is carried out using digital signature tools that have been confirmed as complying with the requirements established in accordance with this Code, and using the qualified certificate of the person on whose behalf the document is signed.

2. A trusted third party or the relevant service provider listed in the Foreign Trusted Services Register shall verify the authenticity of signatures based on certificates issued by a foreign certification center. The result of verification by the trusted third party shall be reflected in a receipt signed with the qualified signature of the trusted third party.

Article 143. Digital signature tools

1. To create and verify a digital signature, create signature keys and signature verification keys, digital signature tools should be used that:

1) allow to establish the fact of change in the signed digital document after its signing;

2) ensure the practical impossibility of calculating the signature key from the digital signature or its verification key.

2. When creating a digital signature, the digital signature tool should:

1) show the content of the digital record to the person signing it;

2) create a digital signature only after confirmation of the operation to create a digital signature by the person signing the information;

3) unambiguously and clearly show that the digital signature has been created.

3. When verifying a digital signature, the digital signature tool should:

1) show the content of a digital document signed with a digital signature;

2) show whether changes have been made to a digital document signed with a digital signature;

3) indicate the person whose signature key was used to sign the documents.

4. Digital signature tools intended for creating a digital signature in digital documents containing information constituting state secrets, or intended for use in a digital resource containing state secrets, shall be subject to mandatory certification for compliance with the requirements for protecting information of the corresponding secrecy level.

5. Digital signature tools intended to create a digital signature in digital documents containing confidential information should not violate the confidentiality of such information.

6. The requirements of parts 2 and 3 of this Article do not apply to digital signature tools used for automatic (without human intervention) creation or verification of digital signatures.

Article 144. Certification center

1. The certification center shall:

1) create a digital signature verification key certificate and issue it to the person who has applied for such a certificate (hereinafter referred to as the applicant);

2) establish the validity periods of certificates of the digital signature verification key;

3) revoke the digital signature verification key certificates issued by it;

4) at the request of the applicant, issue digital signature tools containing a digital signature key and a digital signature verification key (including those created by the certification center) or providing the possibility for the applicant to create a digital signature key and a digital signature verification key;

5) maintain a register of certificates of the signature verification key issued and canceled by it (hereinafter referred to as the "certificates register"), including, among other things, the information contained in the digital signature verification key certificates issued by it, as well as information on the date of termination (revocation) of the digital signature verification key certificate and the grounds of such termination;

6) establish the procedure for maintaining the register of non-qualified certificates and access to it, ensure access of persons to the information contained in the register of certificates, including via the Internet;

7) at the request of applicants, create digital signature keys and digital signature verification keys;

8) ensure the confidentiality of digital signature keys (if such keys are created);

9) check uniqueness of the digital signature verification keys in the registry of certificates of this certification center;

10) check the digital signature at the request of the participants in digital interaction;

11) engage in other activities related to the digital signature use.

2. The certification center shall be obliged to:

1) inform applicants about the conditions and procedure for using a digital signature and digital signature tools, about the risks associated with the digital signature use, and the measures necessary to ensure the security of digital signatures and their verification;

2) ensure the relevance of the digital data contained in the register of certificates and their protection from unauthorized access, destruction, modification, blocking, and from other illegal actions in relation to such information;

3) provide any person with the data contained in the certification center register, including data on the revocation of the digital signature verification key certificate, free of charge and upon request and in accordance with the procedure established for access to the certificate register.

3. In accordance with the Kyrgyz Republic legislation, the certification center shall be liable for harm caused to other persons as a result of:

1) failure to perform or improper performance of obligations arising from agreement for the provision of services by the certification center;

2) failure to perform or improper performance of the duties provided for in paragraph 10 of part 1, paragraphs 2 and 3 of part 2 of this Article.

4. The certification center shall have the right to empower other persons (hereinafter referred to as trusted persons) with the authority to create and issue the digital signature verification key certificates on behalf of the certification center, signed with a digital signature based on the digital signature verification key certificate issued to such a trusted person by this certification center.

5. The certification center that has granted authority to trusted persons shall be the root certification center in relation to such trusted persons and shall implement the following functions in relation to them:

1) perform verification of digital signatures, for which the digital signature verification keys are specified in the digital signature verification key certificates issued to the trusted persons;

2) ensure digital interaction among trusted persons and between trusted persons and the certification center.

6. Digital records entered into the register of certificates should be stored for the entire period of the certification center activity, unless shorter period is established by normative legal acts. If certification center ceases its operation without transferring its functions to other persons, it should notify the owners of the digital signature verification key certificates issued by it that have not expired in advance, but no later than one month before the date of termination of the activities. In this case, after the certification center ceases its operation, the digital records entered in the register of certificates should be deleted.

If certification center ceases its operation with the transfer of its functions to other persons, it should notify the owners of the digital signature verification key certificates issued by it that have not expired, in advance, but not less than one month before the date of transfer of its functions. In this case, after the certification center ceased its operation, the digital records entered in the register of certificates should be transferred to the person that has taken over functions of the certification center that ceased its operation.

7. The certification center shall independently determine the procedure for performing its functions, exercising its rights and fulfilling the obligations established by this Article, unless otherwise established by a normative legal act or agreement of subjects of legal relations in the digital environment.

8. An agreement for the provision of services by the certification center that carries out its activities in relation to an unlimited number of persons shall be a public agreement.

Article 145. Digital signature verification key certificate

1. The certification center shall generate and issue a digital signature verification key certificate based on an agreement between the certification center and the applicant.

2. The digital signature verification key certificate should contain the following information:

1) start and end dates of its validity;

2) last name, first name, middle name (if any) – for individuals, name – for legal entities, or another identifier of the ownerof a digital signature verification key certificate;

3) digital signature verification key;

4) name of the digital signature tool used and (or) the standards which the digital signature key and digital signature verification key comply with;

5) name of the certification center that issued the certificate.

3. When issuing a digital signature verification key certificate to a legal entity, the owner of such certificate, along with its name, shall also indicate the individual acting on its behalf based on constituent documents or a power of attorney.

4. The certification center shall have the right to issue digital signature verification key certificates both in the form of a digital document and in the form of a paper document. The owner of the digital signature verification key certificate issued in the form of a digital document shall also be entitled to receive a signature verification key certificate on paper signed by the certification center.

5. The digital signature verification key certificate shall be valid from the date of its issue, unless different date is specified in the signature verification key certificate itself.

Information about the digital signature verification key certificate should be entered by the certification center into the register of certificates no later than the effective date of the signature verification key certificate specified in it.

6. The digital signature verification key certificate shall expire:

1) upon expiration of its validity period;

2) at the request of the digital signature verification key certificate owner submitted in form of a paper document or in digital form;

3) in case of termination of the certification center operation without transfer of its functions to other persons;

4) in other cases, established by law or by agreement between the certification center and the owner of the digital signature verification key certificate.

7. Data on the termination of the digital signature verification key certificate should be entered by the certification center into the register of certificates within one business day from the moment when the certification center became aware of the occurrence of circumstances that led to the termination of the digital signature verification key certificate. The digital signature verification key certificate ceases to be valid from the moment an entry about it is made in the register of certificates.

8. The certification center shall revoke the digital signature verification key certificate by entering a revocation record into the register of certificates based on a court decision that has entered into legal force, in particular if the court decision establishes that the digital signature verification key certificate contains inaccurate data.

9. The use of a revoked digital signature verification key certificate shall not entail legal consequences, except for those associated with its revocation.

Before entering information on revocation of the signature verification key certificate into the register of certificates, the certification center should notify the owner of the signature verification key certificate about the revocation of his/her signature verification key certificate.

Article 146. Accredited certification center

1. A certification center that has received accreditation shall be an accredited certification center.

2. The accredited certification center shall be required to store the following data:

1) details of the main document that certifies the identity of the qualified certificate owner who is an individual;

2) information about the name, number and date of issue of the document confirming the right of the person acting on behalf of an applicant, a legal entity, to apply for a qualified certificate;

3) information on the name, number and date of issue of the documents confirming the authority of the qualified certificate owner to act on behalf of third parties, if information on the authority of the qualified certificate owner to act on behalf of third parties is included in the qualified certificate.

3. The data specified in part 2 of this Article should be stored by the accredited certification center for the duration of its activity, unless normative legal acts provide for a shorter period.

Digital data should be stored in a form that allows verification of their integrity and validity.

The certification center shall provide the qualified certificate owner with access to digital records related to the qualified certificate owner and stored in the accredited certification center.

4. If the accredited certification center ceases its operation, it shall be obliged to:

1) notify the national ecosystem industry regulator about this no later than one month before the date when the certification center ceases its operation;

2) transfer the register of certificates to the national ecosystem industry regulator in the established manner;

3) transfer digital records to be stored in the accredited certification center to the national ecosystem industry regulator in the established manner.

Article 147. Accreditation of the certification center

1. The national ecosystem industry regulator shall carry out accreditation of certification centers that are legal entities.

2. Accreditation of a certification center shall be carried out on a voluntary basis.

Accreditation of a certification center shall be carried out for 5 years, unless a shorter period is specified in the certification center application.

3. Accreditation shall be granted if the certification center meets the following requirements:

1) the net assets value of the certification center is at least one million soms;

2) availability of financial security for liability for damages caused to other persons as a result of their trust in the information specified in the digital signature verification key certificate issued by such certification center, or the data contained in the register of certificates of this certification center, in the amount of no less than one and a half million soms;

3) availability of digital signature tools and certification center tools that have been certified as compliant with the requirements established by the national security authorized state body;

4) the certification center has at least 2 employees directly involved in the creation and issuance of digital signature verification key certificates, who have higher professional education in information technology or information/cybersecurity, or higher or secondary professional education, who have undergone retraining or advanced training in the use of digital signatures.

4. Accreditation of a certification center shall be carried out upon its application submitted to the national ecosystem industry regulator.

The application shall be accompanied by the documents confirming compliance of the certification center with the requirements established by part 3 of this Article.

5. Based on the submitted documents, no later than thirty calendar days from the date of their receipt, the national ecosystem industry regulator shall make decision on the accreditation of the certification center or on the refusal of accreditation.

Within 10 days from the date of the decision to accredit the certification center, the national ecosystem industry regulator shall notify the certification center of the decision made and issue an accreditation certificate in the established form. Simultaneously with the accreditation certificate, the accredited certification center shall receive a qualified certificate created using the root certification center means.

If a decision is made to refuse accreditation of a certification center, the national ecosystem industry regulator shall send or deliver a notification of the decision made to the certification center, indicating the reasons for the refusal, no later than ten calendar days from the decision date.

6. Non-compliance of the certification center with the requirements established by part 3 of this Article, or the presence of false information in the submitted documents shall be the basis for denial of accreditation.

7. The accredited certification center should comply with the requirements for which it is accredited during the entire accreditation period. In case of circumstances that make it impossible to comply with them, the certification center should immediately notify the national ecosystem industry regulator.

When performing its functions and fulfilling its obligations, the accredited certification center should comply with the requirements established for certification centers by this Code.

If the accredited certification center fails to comply with the specified requirements, the national ecosystem industry regulator shall be obliged to issue an order to the certification center to eliminate the violations, setting a deadline for their elimination, and suspend the accreditation for the specified period. The accredited certification center shall notify the national ecosystem industry regulator in writing about elimination the violations that served as the basis for the suspension of its accreditation. The national ecosystem industry regulator shall have the right to verify the actual elimination of violations, after which it shall make a decision to renew the accreditation, and if they are not eliminated within the time period specified in the order, it shall cancel the certification center accreditation.

8. The requirements established by paragraphs 1 and 2 of part 3 of this Article shall not apply to state bodies, local governments, state and municipal institutions that perform the functions of a certification center.

9. The root certification center, the functions of which are carried out by the national ecosystem industry regulator, shall not be subject to accreditation in accordance with this Code.

10. The certification centers should pay an annual fee for accreditation calculated according to the methodology established by the Cabinet of Ministers.

Article 148. Qualified certificate

1. A qualified certificate shall be created using facilities of the certification center that has received confirmation of compliance with the requirements established in accordance with this Code.

2. The qualified certificate should contain the following information:

1) a unique number of a qualified certificate, the start and end dates of its validity;

2) last name, first name and middle name (if any), date and place of birth of the qualified certificate owner for an individual or name (company name), registration number and place of registration and (or) actual location of the executive body of the qualified certificate owner if a legal entity;

3) digital signature verification key;

4) name of the digital signature tools and the certification center means that were used to create the digital signature key, the digital signature verification key and the qualified certificate, as well as the details of the document confirming the compliance of these means with the requirements established in accordance with the Code;

5) name and location of the certification center that issued the qualified certificate, number of the qualified certificate of the certification center and details of the accreditation certificate of this center;

6) other information about the applicant (at the applicant's request).

3. If the applicant submits to the certification center documents confirming his/her right to act on behalf of third parties, the qualified certificate shall include information evidencing such powers of the applicant and the validity period of these powers.

4. A qualified certificate shall be issued in a form as required by the authorized state body responsible for the national security.

5. In case of revocation of the qualified certificate issued to the accredited certification center that issued the qualified certificate to the applicant, and in case of revocation or expiration of the certification center's accreditation, the qualified certificate issued by the accredited certification center to the applicant shall cease to be valid.

6. The qualified certificate owner who has reasons to believe that the confidentiality of the digital signature key has been compromised shall cease using that key and immediately contact the certification center that issued the qualified certificate to revoke it.

Article 149. Issuance of a qualified certificate

1. When issuing a qualified certificate, an accredited certification center shall be required to perform digital identification and digital authentication of the applicant in accordance with the digital identification system rules used under this Code, or based on the main document certifying identity of the applicant as an individual.

2. An applicant acting on behalf of another person shall submit the following to the accredited certification center:

1) power of attorney (if the applicant acts on behalf of another person based on a power of attorney);

2) appointment document, constituent documents and state registration document of the applicant - legal entity (if the applicant acts on behalf of a legal entity without power of attorney).

3. After receiving a qualified certificate, the applicant shall be familiarized with the information contained in the qualified certificate by the certification center.

4. Simultaneously with issuance of a qualified certificate, the certification center shall issue guidelines for ensuring the security of the qualified signature and digital signature means use to the qualified certificate holder.

5. When a qualified certificate is reissued for a new term, digital identification and digital authentication of the applicant shall be performed based on the previously issued qualified certificate.

Article 150. Digital archives and digital archive services

1. The digital archive as a digital technological system shall ensure the integrity and inalterability of digital records processed with it while limiting access to them. The archiving legislation shall establish the types of digital records subject to archival storage, the procedure for their creation and storage.

2. Based on legislation or agreement with the user, the digital archive service provider shall be obliged to ensure the integrity and inalterability of the digital records transferred for storage in the digital archive, and to ensure access to them by persons who are authorized to do so in accordance with the legislation or agreement.

3. Types of digital archives, depending on the technologies used, shall include:

1) simple digital archives, in which the integrity and inalterability of digital records are ensured by the digital technological system means;

2) qualified digital archives in which the integrity and inalterability of digital records are ensured by the qualified signature tools.

4. To fulfill their obligations for archival storage of documents, subjects of legal relations in the digital environment shall have the right to organize digital archives of digital records or use the digital archive service. The rules for the creation and use of state digital archive services shall be an integral part of the national ecosystem rules.

5. The legal significance of a digital record in the digital archive shall be recognized as unaltered if the digital archive ensures the following:

1) inalterability and integrity of the digital record after its inclusion in the digital archive;

2) possibility of access to it by persons who have the right to do so in accordance with the legislation or agreement;

3) automatic registration of actions performed with a digital record during the period of its storage.

6. Digital documents signed with a qualified signature should be stored in qualified digital archives, which should ensure:

1) signing of the digital document with the qualified signature of the person storing the digital document;

2) confirmation that the qualified signature with which the digital document transferred for storage was originally signed is valid.

Article 151. Storing a digital duplicate of the document

1. A digital record that reproduces in full the information originally contained in the original document on paper or other tangible media signed with a handwritten signature, including its details, shall be recognized as a digital duplicate of the document.

2. A digital duplicate of a document stored in a digital archive in accordance with this Code shall certify legal facts that are the grounds for occurrence, change, and termination of legal relations, instead of the original document, if the owner can confirm its compliance with the following requirements:

1) information primarily contained in the original document on paper or other tangible medium, signed with a handwritten signature, including its details, is reproduced in full in a digital duplicate of the document;

2) inalterability and integrity of the document digital duplicate after its creation was ensured.

3. Information originally contained in several related documents on paper or other tangible medium (package of documents) may be included in a single digital duplicate of the document. In this case, the information should be arranged in the chronological order of signing the original documents.

4. The digital duplicate of the document should contain the following information:

1) information originally contained in the original document on paper or other tangible medium, in full and without changes (in an uncorrected form);

2) image of the handwritten signature of each person from among those who signed the original document;

3) metadata for the purposes of digital identification and retrieval of the document digital duplicate.

5. If there is discrepancy between the digital duplicate of a document and the original document, the original document shall prevail.

6. Persons who have created a digital duplicate of the document shall have the right to stop storing the original document on a tangible medium. The Cabinet of Ministers shall approve the list of types of documents that should continue to be stored in their original form after their digital duplicates have been made. It is not allowed to recognize a digital duplicate of a document as invalid only based on the absence (destruction) of the original document based on which it was created.

Article 152. Trusted storage of digital records

When storing digital records in distributed digital resources, including using smart contracts, the rules for storing digital records and accessing them shall be determined by the parameters of such a distributed digital resource and (or) smart contract.

Article 153. Powers of state bodies in the sphere of digital signature and digital archives use

1. The Cabinet of Ministers shall:

1) establish the procedure for transferring registers and other data to the national ecosystem industry regulator in case of termination of the accredited certification center;

2) establish the procedure for formation and maintenance of registers of qualified certificates, as well as the provision of information from such registers;

3) establish the rules for accreditation of certification centers, including the procedure for verifying compliance by accredited certification centers with the requirements for compliance with which these certification centers were accredited;

4) determine the list of types of documents that should continue to be stored in the original after the production of their digital duplicates;

5) determine the procedure for performing functions of the trusted third party of the Kyrgyz Republic, including the procedure for its interaction with trusted third parties and certification centers of other states.

2. The national ecosystem industry regulator shall:

1) accredit certification centers and verify compliance by accredited certification centers with the requirements for compliance with which these certification centers were accredited, and, in case of detection of non-compliance, issue instructions to eliminate violations;

2) perform functions of the root certification center with respect to accredited certification centers;

3) perform functions of a trusted third party of the Kyrgyz Republic.

3. The authorized state body responsible for ensuring national security shall:

1) establish requirements for the form of a qualified certificate;

2) establish requirements for digital signature tools and certification center tools;

3) confirm the compliance of digital signature facilities and certification center facilities with the requirements established in accordance with this Code and shall publish a list of such facilities.

4. The national ecosystem industry regulator shall be required to ensure storage and unobstructed 24-hour access to the following digital records:

1) names, addresses of accredited certification centers;

2) register of issued and canceled qualified certificates;

3) list of certification centers which accreditation has been canceled;

4) list of accredited centers which accreditation has been suspended;

5) list of accredited certification centers which activities have been terminated;

6) registers of certificates transferred to the national ecosystem industry regulator.

Chapter 18. State Services

Article 154. Legal relations on the creation and use of state services

1. State services shall be provided within the national digital ecosystem (national ecosystem), except for state services provided through digital technological systems of the authorized state body responsible for ensuring national security.

2. The rules for creation and use of state services shall be part of the national ecosystem rules and be established by this Code.

3. The state service providers shall be the state agencies and local self-governments of the Kyrgyz Republic, and legal entities - participants of the national ecosystem. Providers shall be required to ensure the digital resilience of state services.

4. State and local government bodies, legal entities regardless of their organizational and legal form, as well as individuals (consumers) shall be the state service users. Depending on the type of users they vary as follows:

1) interaction state services, i.e., state services designed for data processing by state bodies, local government bodies of the Kyrgyz Republic and legal entities involved in the provision of state services;

2) user services, i.e., state services for users, including individuals (consumers).

Article 155. Industry principles for the state services creation and use

1. State services should be created in accordance with national strategies and plans as state and local governments undergo digital transformation (the proportionality principle).

2. State services should build on elements of the national ecosystem, sources and formats of digital data used within other state services, and allow for the use of digital records by other state services (the compatibility principle).

3. The rights and interests of a man and citizen, the ease of use of services, and their safety for consumers shall be unconditional priorities in the creation of state services (the consumer interests principle).

4. State services should be designed and created so as to be as accessible as possible to consumers, taking into account their education and property status, as well as their age and physical characteristics (the accessibility principle).

5. The state services users should reasonably trust their reliability and security and that their data are processed based on and in accordance with the law (the confidence principle).

6. State services should be designed so that the services and functions based on them become accessible to users as a result of digital transformation (the simplification principle).

7. The state service use data, including user feedback and complaints, should be kept in accordance with the law and used to evaluate the effectiveness of state services and continuously improve (the feedback principle).

Article 156. State service users

1. An individual whose data are processed as part of a state service shall be considered to be its consumer, regardless of whether the processing is initiated of the individual or by the state service provider.

2. The basis for processing personal data as part of the state service shall be the state service provider's performance of duties (powers) established by this Code, the law or normative legal acts adopted in accordance with it. An individual's consent shall not be required for processing of personal data necessary for the performance of such duties. It shall be prohibited to process personal data as part of the state services that are not required for the provision of state services.

3. Consumers shall have the right to choose to use state services in any way they can or not to use them.

4. If several state bodies, local government bodies or legal entities are involved in the provision of a state service, the consumer shall have the right to interact with any of them at his or her choice, except in cases where the law or normative legal acts adopted in accordance with it provide that the rights and obligations of the state service provider are performed by a specific state body or legal entity.

5. Consumers shall have the right to submit feedback and complaints regarding the state service use. The state service provider should provide an opportunity for feedback and complaints to be sent to it via the state service application or website, and for the consumer to choose whether their feedback or complaints should be published. Feedback (complaints), which the consumer decided to publish, should be published on the website of the state service provider no later than one business day after they were sent by the consumer.

6. The consumer shall have the right not to provide the state service provider with data already contained in state digital resources.

Article 157. Participation of state bodies, local self-governments and legal entities in the state service creation and use

1. The coordinating body shall coordinate the state service creation in accordance with this Code.

2. The national ecosystem industry regulator shall:

1) ensure the creation of state services and account for them, create and operate the state digital technological system for the creation and development of state services (the state service factory), exercise the rights and responsibilities of the state service factory owner;

2) on behalf of the Kyrgyz Republic exercise the rights and responsibilities of the state service applications and website owner;

3) participate in the development of documents formalizing the state service creation or modification;

4) assist the state and local government bodies in the digital transformation process, including the development and coordination of documents and procedures related to state services, provision of access to open data;

5) develop and publish on its website the requirements for feasibility studies, technical specifications, technical tasks for creating digital services for state agencies, local government bodies and legal entities authorized by them;

6) define the key performance indicators of state services and monitor them;

7) assess the digital resilience of state services and issue mandatory instructions to the state service providers to improve their digital resilience;

8) participate in the development of methods of training, professional development of state and municipal employees and other persons in terms of the state services use.

3. Public authorities, local government bodies, legal entities shall create state services and use them in accordance with their powers under the Kyrgyz Republic laws, regulations and agreements between such bodies and legal entities.

Article 158. Rules for the state services creation

1. Decision to create a state service or to change it shall be made by a participant of the national ecosystem interested in its creation or change.

2. The decision to create a state service should include:

1) reference to the state service provider;

2) data on the state service users and consumers;

3) indication of the functions and powers under which the state service is used;

4) data on digital technology systems, used to provide state the public service;

5) indication of sources of data processed as part of the state service, including those resulting from the use of other state services;

6) description of how to access the state service;

7) description of results of the state service use and the procedure for their use, including the use in other state services.

3. Before the state service use, its provider should:

1) ensure compatibility and interaction of the created state service with other state services;

2) conduct functionality and digital resilience testing of the state service using the state service factory and provide its results to the national ecosystem industry regulator;

3) provide the regulator with the data necessary to account for the state service, if the test result is positive, confirmed by the national ecosystem industry regulator.

4. For the purpose of state service accounting the national ecosystem industry regulator shall include the data specified in part 2 of this Article in the digital register of the national ecosystem, as well as the following data:

1) persons responsible for ensuring digital resilience of the state service and their contact information;

2) indicators that characterize the state service quality (maximum period of service unavailability during the year, time required to restore service availability in case of failure, simultaneous number of users);

3) used data formats and data exchange interfaces.

5. When changes are made to the state service, its provider shall, prior to using the updated state service, perform the actions stipulated in part 3 of this Article.

Article 159. State service factory

1. The state service factory is a state digital technological system for the creation and development of state services.

2. The state service factory shall provide:

1) access of the public service owner to the common space of the national ecosystem digital data;

2) testing the state service before using it;

3) monitoring the state service performance;

4) interaction of the state service with other state services and other objects of legal relations in the digital environment within the national ecosystem;

5) development of the state service and changes to it.

3. The Cabinet of Ministers shall determine the state service factory operation rules. The rules may provide for other functions to be performed by the state services factory.

Article 160. Rules for using the state service

1. The rules for using the state service shall be approved by its provider based on the legislation governing the exercise of its respective functions or powers.

2. No user agreement shall be concluded when using state services, unless otherwise provided for by the Kyrgyz Republic legislation.

3. The rules for using the public service should describe the rights and obligations of all categories of its users, and the procedure for their actions to achieve each of the possible goals of its use.

4. The rules for using the state service should provide the possibility of data processing within the state service, both at the initiative of the user and proactively, at the initiative of its provider. The rules for using the state service should provide guarantees of the user's rights when processing his/her data at the state service provider’s initiative.

5. The rules for using the state service should describe the procedure and consequences of data processing within the state service:

1) indication of the types, sources of raw data processed within the state service, and their principals;

2) description of possible data processing options (creation, update, refinement, modification, search);

3) indication of the digital resources or digital records that are modified as a result of data processing.

6. The rules for using the service shall be posted on the state service provider's website and should be available to service users on the website or in the application before using the service.

Article 161. State service applications and website

1. The state service applications and website shall be intended to provide access to user state services.

2. The state services applications and website shall provide:

1) users' access to information about state services and rules for using them;

2) possibility of using state services to obtain relevant services;

3) possibility to download data, including digital documents and digital duplicates of documents, for their processing within the state service;

4) possibility to monitor the progress of the user data processing, including obtaining data on the progress of providing state services;

5) possibility of obtaining the results of the state services use, except where such obtaining is prohibited by law;

6) possibility to pay for state services and make other mandatory payments, unless otherwise provided by law;

7) possibility of filing complaints about the state service providers performance and obtaining decisions on such complaints.

3. The Cabinet of Ministers shall approve the Regulations on the state service applications and website. The Regulations may allow for other functions that are carried out by the state service applications and website.

Article 162. Dispute consideration

1. The national ecosystem industry regulator shall consider complaints and disputes regarding state services by using the state services website or application.

2. Within three business days of receiving a complaint, the industry regulator should inform state bodies, local government bodies and legal entities involved in the provision of state services and provide all data related to the complaint received.

3. Within fourteen business days after receipt of a complaint, the industry regulator shall review the complaint and, if the information in the complaint is confirmed, shall issue binding orders to the state service providers to eliminate the complaint reasons. When considering the complaint, the industry regulator shall request the necessary data from the service provider.

4. The state service provider shall be obliged to take measures necessary to eliminate the violations specified in the complaint within five business days after receiving the industry regulator's order. The public service provider should inform the user about the measures taken.

5. Decisions by the state service provider on the complaint or dispute may be appealed to the court at the provider's location.

Chapter 19. The National Ecosystem

Article 163. National ecosystem architecture

1. **The national ecosystem** is designed to provide digital services, including state services. The national ecosystem provides general rules for the creation and use of the following objects of legal relations in the digital environment (the national ecosystem elements):

1) state (municipal) digital resources, the state service applications and websites;

2) state services and trusted services;

3) state (municipal) digital technological systems and their elements;

4) lands, buildings, structures, facilities and other similar objects in terms of access to them by the state digital technological systems owners.

2. The national ecosystem elements shall be accounted in the national ecosystem digital register, in accordance with this Code. The digital technological systems of the authorized state body responsible for ensuring national security shall be included into the national ecosystem elements exclusively by decision of the head of the said authorized state body.

3. The national ecosystem rules shall be established in accordance with this Code and shall include rules for:

1) development of the national ecosystem;

2) interaction of the national ecosystem participants;

3) formation of data sources and data processing;

4) creation and use of state services;

5) trusted services and digital identification systems;

6) creation and use of state and municipal digital technology systems.

4. Coordination of activities for the creation and development of the national ecosystem shall be carried out by the coordinating body. In course of the national ecosystem development, state services shall be created and used in accordance with the rules established by the relevant chapter of this Code.

5. The national ecosystem owner shall be the Kyrgyz Republic, on behalf of which the national ecosystem industry regulator acts.

6. The national ecosystem participants shall be the national ecosystem owner represented by the industry regulator, state bodies, legal entities regardless of their organizational and legal form, and individuals who are owners (suppliers) of the national ecosystem elements or their users.

7. Digital identification and digital authentication of the national ecosystem participants shall be carried out using digital identification systems according to the rules established by the relevant chapter of this Code.

Article 164. The national ecosystem principles

1. Each subject of legal relations in the digital environment shall be entitled to become a national ecosystem participant, subject to its rules (the public accessibility principle).

2. The national ecosystem elements shall be designed and operated in such a way that the consequences of incidents in the digital environment for each of the elements, their replacement or development do not have a negative impact on the national ecosystem as a whole (the modularity principle).

3. The national ecosystem elements shall be designed and created in such a way as to function independently of specific digital devices and their location (the cloud principle).

4. Based on their own needs, the national ecosystem participants shall have the right to determine the composition of the national ecosystem elements created and used by them in their activities, taking into account the provisions of this Code and the national ecosystem rules (the variability principle).

5. The functions of each element of the national ecosystem can be performed simultaneously by other national ecosystem elements, if doing so increases the national ecosystem overall efficiency (the parallelism principle).

6. The national ecosystem elements should primarily be based on open data formats (records) and data exchange interfaces. They should not depend on particular digital devices supplier, data formats (records) and data exchange interfaces, the rights to which belong to third parties (the principle of independence on the provider).

Article 165. Development of the national ecosystem

1. The national ecosystem shall be developed in accordance with programs and plans for the development of the national ecosystem and its individual elements, approved by the Cabinet of Ministers.

2. Plans and programs for the development of the national ecosystem and its individual components should consider the needs for the state services provision and generally accepted international practices in digital governance.

3. Participants of the national ecosystem shall have the right on their own initiative to create the national ecosystem elements, not provided for by the plans and programs of its development, but necessary for the national ecosystem participants' activities. In accordance with the procedure established by this Code, the national ecosystem elements created on an initiative shall be entered into the national ecosystem digital register.

Article 166. Interaction of participants of the national ecosystem

1. Participants of the national ecosystem shall be obliged to interact with each other within the national ecosystem in accordance with its rules and interaction agreements between participants.

2. The Cabinet of Ministers shall establish the rules for interaction between the national ecosystem participants.

3. The participants interaction in the national ecosystem shall be free of charge.

4. When providing state services, state bodies, local government bodies, state and municipal institutions and organizations shall interact using the digital interaction system, which is a national ecosystem element.

5. The Kyrgyz Republic shall be the digital interaction system owner, on behalf of which the national ecosystem industry regulator acts.

6. Lists of digital data transmitted using the digital interaction system shall be established by normative legal acts defining the relevant powers of the Kyrgyz Republic state bodies.

Article 167. Data processing and data sources of the national ecosystem

1. The digital resources of the national ecosystem participants shall be the sources of digital data processed within the national ecosystem, and form common space of the national ecosystem digital data.

2. Only the law can restrict the national ecosystem participants' rights to process data in the common digital data space. A national ecosystem participant should provide access to its digital resources for the purposes of processing data from them in the shared digital data space in cases established by law or by agreement of such participant with other national ecosystem participants.

3. The digital records processing within the national ecosystem takes into account their metadata, that define the digital records owners or principals, the permissible processing purposes and methods, digital record formats and data exchange interfaces, and other characteristics important to the digital records processing.

4. Digital data should be processed within the national ecosystem, regardless of their format. Unless otherwise established by laws and regulations adopted in accordance therewith or by agreement the national ecosystem participants, the national ecosystem participants shall be free to process digital data in such a format, in such a manner and in such sequence of operations as best achieves the purpose of processing.

5. Unless otherwise stipulated by laws and regulations adopted in accordance therewith or by agreement of the national ecosystem participants, data in the common digital data space shall be open data.

6. Within the national ecosystem, personal data and digital records classified as legally protected secrets can be processed on the grounds provided for by this Code and the laws on the relevant types of secrets. The national ecosystem participants processing such data shall be obliged to take the following measures to prevent harm to the personal data subject or the person in whose interest the legally protected secret is kept:

1) access of authorized persons to such data shall be provided in accordance with the procedure established by the Cabinet of Ministers;

2) the data shall be processed exclusively for the purposes established by legislation and shall not be transferred by one national ecosystem participant to another, except in cases established by law;

3) data intended for publication or other dissemination shall be presented in an aggregated form that prevent attribution to a specific data principal without additional information;

4) employees who have access to such data by virtue of their official duties and processors of such data shall be obliged to ensure their confidentiality and shall be held liable for breach of these obligations;

5) records of all operations with such data and of all persons accessing such data shall be kept.

6) free access shall be provided (including by publishing on the national ecosystem participant's website or in the application) to information on the composition of the processed data, purposes and methods of their processing, methods for data principals to obtain the processing information in accordance with this Code.

7. The Cabinet of Ministers shall determine requirements for the procedure of creation, actualization and use of state (municipal) digital resources. Information about state (municipal) digital resources, digital resources of other national ecosystem participants and the procedure of access to them shall be included in the national ecosystem digital register.

Article 168. Creation and use of state and municipal digital technology systems

1. Digital technological systems and telecommunication networks connecting them can be used as part of the national ecosystem, both those built at the expense of the republican and local budgets and those used on a contractual basis.

2. The state (municipal) digital technological system owner shall be obliged to approve its rules and ensure their compliance with provisions of this Code, if such rules or regulations on the state (municipal) digital technological system are not approved by the law or normative legal acts adopted in accordance with it.

3. The Cabinet of Ministers shall establish requirements for state (municipal) digital technological systems.

4. Information on state (municipal) digital technological systems shall be included in the national ecosystem digital register.

Article 169. The national ecosystem industry regulator

1. The authorized state body determined in accordance with the procedure established by Article 9 of this Code (the national ecosystem industry regulator) shall regulate and supervise activities related to the national ecosystem. The national ecosystem industry regulator shall be independent in its activities of the persons over whom it exercises its powers.

2. The head of the national ecosystem industry regulator should have the qualifications, experience and knowledge, including in the field of digital technology, necessary to perform the duties and exercise the powers.

3. The national ecosystem industry regulator shall exercise the following powers:

1) implement development plans for the national ecosystem and its individual elements;

2) exercise the rights and obligations of the digital interaction system owner, unified digital identification system, application and website of state services, state services factory, national ecosystem digital register shall be their processor, and operate, develop and provide their technical support and maintenance, ensure implementation, monitoring and uninterrupted functioning;

3) provide technical coordination, methodological support and monitoring of the effectiveness of the national ecosystem participants and the quality of digital services;

4) ensure compatibility of digital technological systems at the technical and technological level, methodological support and development of the national ecosystem architecture;

5) develop, test, modernize its own digital services, applications, digital technological systems;

6) perform the functions of a root certification center, carry out accreditation of certification centers in accordance with this Code;

7) participate in the development of documents defining the creation, modification and procedures for the provision of state services as they relate to the creation or modification of the national ecosystem elements;

8) provide for the development of the national ecosystem rules;

9) assist the state and local self-governments in the process of digital transformation, including the creation, development and use of state (municipal) digital technology systems and the processing of digital data using them;

10) provide interaction of participants of the national ecosystem;

11) develop, approve and publish on its website the recommendations on formats of digital data and records used in the national ecosystem;

12) determine the key performance indicators of the national ecosystem and monitor them;

13) assess the digital resilience of the national ecosystem and issue prescriptions mandatory for the state (municipal) digital technology systems owners to improve their digital resilience;

14) participate in the development of methods for training, advanced training of state and municipal employees and other persons in the development and use of the national ecosystem;

15) maintain the national ecosystem digital register, other registers in accordance with the procedure established by this Code.

4. To achieve transparency of its regulatory functions, the national ecosystem industry regulator should publish an annual report on its activities and results of assessment of the digital resilience of the national ecosystem on its website.

5. The national ecosystem industry regulator shall have the right to:

1) request and obtain free of charge the necessary information for exercising their powers from individuals and organizations, including information relating to state secrets or other secrets protected by law;

2) require the owner of the state (municipal) digital technological system to take measures to restore its digital resilience;

3) apply to court with statements of claim in defense of the national ecosystem participants' rights, including in defense of rights of an indefinite group of persons, and represent the interests of the national ecosystem participants in court;

4) forward materials to law enforcement agencies in accordance with jurisdiction to decide whether to initiate criminal proceedings for crimes related to violations of the national ecosystem rules;

5) submit proposals to the Cabinet of Ministers for improving the national ecosystem rules, plans, programs for development of the national ecosystem and its certain elements;

6) bring to justice the persons guilty of violating this Code.

6. The national ecosystem industry regulator should:

1) ensure compliance with the national ecosystem rules and their development in accordance with the provisions of this Code;

2) regularly check compliance by the owners of state (municipal) digital technology systems with this Code and make binding decisions based on the check results;

3) consider complaints and appeals of the national ecosystem participants regarding their interaction within the national ecosystem, and based on make binding decisions within its authority;

4) give explanations on application of the national ecosystem rules at the request of individuals and organizations with the publication of such explanations on its website;

5) develop and publish recommendations regarding development of the national ecosystem, creation and use of state (municipal) digital technological systems, develop and publish sample forms of contracts, legal acts and other documents for the national ecosystem participants.

Article 170. Dispute resolution within the national ecosystem

1. In case of disputes regarding interaction between the national ecosystem participants, both parties shall be obliged to apply to the national ecosystem industry regulator for pre-trial consideration. The telecommunications industry regulator shall consider such an application within two months from the date of its receipt.

2. For the purpose of dispute resolution, the national ecosystem industry regulator shall have the right to request any data that cannot be refused.

3. The national ecosystem industry regulator shall not consider a dispute in the following cases:

1) if subject of the dispute is not an interaction using the national ecosystem;

2) if the dispute concerns conclusion of an interaction agreement or less than 3 months have passed from the moment of sending a request for the agreement conclusion by one national ecosystem participant to another;

3) If more than 1 year has passed from the date of the last action in the negotiation process.

4. In cases stipulated by paragraphs 1 and 3 of part 3 of this Article, the national ecosystem participant shall have the right to apply directly to court.

5. To resolve the dispute, the national ecosystem industry regulator shall have the right in its decision to establish technical and (or) financial conditions of interaction, mandatory for the parties.

6. The national ecosystem industry regulator's decision shall be issued in the form of an administrative act and can be appealed in court.

7. If the national ecosystem industry regulator fails to make decision within the term specified in part 1 of this Article, the dispute shall be considered unresolved, and the head of the national ecosystem industry regulator shall be held liable for inaction in accordance with the legislation on offenses.

SECTION V
DIGITAL TECHNOLOGICAL SYSTEMS

Chapter 20. General Provisions on Digital Technological Systems

Article 171. Legal regulation of digital technological systems

1. In the Kyrgyz Republic, digital technological systems can be created and used without restrictions. This Code shall regulate the use of certain types of digital technological systems for the sole purpose of preventing harm to human life, health, environment, property, public and state security, and enabling interaction in the digital environment using digital technological systems.

2. This Code shall regulate the use of the following types of digital technology systems:

1) telecommunication networks;

2) radio-electronic means and high-frequency devices;

3) state and municipal digital technological systems;

4) artificial intelligence systems.

3. In the Kyrgyz Republic, the possibility of interaction in the digital environment using digital technological systems shall be provided based on generally recognized international practice in accordance with the procedure established by the relevant chapter of this Code.

4. In the Kyrgyz Republic, any persons, regardless of their citizenship, country of origin or form of ownership, and the technologies they use in digital technological systems may the digital technological systems owners and users.

Article 172. Radio-electronic means and high-frequency devices

1. Regardless of their purpose, the radio-electronic means and high-frequency devices should be installed and operated in a manner that does not cause harmful interference to other operating radio-electronic means and high-frequency devices. They should not hinder or interrupt the use of digital services or digital technological systems, including those recognized in the Kyrgyz Republic under the international treaties that have entered into force in accordance with the Kyrgyz Republic legislation.

2. Radio-electronic means shall be used in accordance with the conditions defined in the decision on the assignment of radio frequency. The radio-electronic means owner operating them in accordance with the general designation shall be obliged to independently interact with the owners of other operating radio-electronic means to prevent and eliminate harmful interference to other operating radio-electronic means, that may include switching off their radio-electronic means causing harmful interference. If the radio-electronic means owners fail to independently agree on a set of measures to eliminate harmful interference within one month from the date of commencement of negotiations on such agreement, any of them shall have the right to refer the dispute to the telecommunications industry regulator for consideration.

Article 173. Access to infrastructure for the digital technology systems owners

1. The digital technological systems elements shall be placed, constructed, and operated by the digital technological systems owners under an agreement with the owners or other owners of buildings, structures, transmission line supports, railway contact lines, pole supports, bridges, collectors, tunnels, railroads and highways and other engineering facilities and technological sites. At the same time, the owner or other owner of the said objects shall have the right to demand from the digital technological systems owners a proportionate fee for the use of this property, unless otherwise provided for by this Code.

2. In accordance with the Kyrgyz Republic legislation, the need to place digital technological systems should be taken into account in territorial planning and architectural and construction design. The authorized state body in charge of architecture and construction shall establish requirements for buildings, structures and facilities for placement of digital technological systems.

3. The construction customer shall carry out reconstruction and relocation of the digital technological systems caused by new construction, expansion, reconstruction of settlements and certain types of infrastructure, rearrangement of roads and bridges, development of new lands, rearrangement of land reclamation systems, development of minerals at own expense following the applicable standards in accordance with the technical specifications of owners of these objects. At the same time, owners of such digital technology systems achieve the necessary improvements in the digital technology systems characteristics.

4. Buildings and structures constructed, reconstructed, overhauled and not complying with the approved requirements for buildings, structures and facilities for the purpose of accommodating digital technological systems shall not be allowed to be put into operation.

Article 174. Digital resilience of technological systems

1. Telecommunications operators and owners of state (municipal) digital technological systems shall be obliged to ensure digital resilience of their telecommunications networks and state (municipal) digital technological systems.

2. In accordance with the land and town-planning legislation of the Kyrgyz Republic, protection zones shall be established for telecommunication networks and state (municipal) digital technological systems.

3. Persons engaged in the design and construction, when designing, constructing, repairing, reconstructing and restoring buildings, structures and facilities, should obtain written permission from the owners of digital technological systems and telecommunication facilities

located in the buildings (structures, facilities) to carry out works and take all necessary measures to preserve digital technological systems and telecommunication facilities affected by the works.

4. In accordance with the Kyrgyz Republic legislation, violation of measures to ensure digital resilience of technological systems shall entail liability. Damage caused by unauthorized connection to, interference with or damage to digital technological systems shall be fully compensated to the system owner by the person who caused the damage.

Chapter 21. Telecommunications networks

Article 175. Legal regulation of telecommunication networks

1. The Kyrgyz Republic shall regulate the use of telecommunications networks based on the Constitution, this Code and laws of the Kyrgyz Republic, international treaties and decisions of international organizations in the field of telecommunications to which the Kyrgyz Republic is a party. Unless otherwise established by this Code, terms related to telecommunication networks shall be used in the meaning established in the documents of the International Telecommunication Union.

2. The use of telecommunication networks and their regulation should be in line with generally recognized international telecommunication practices.

3. If under the Kyrgyz Republic legislation, it is necessary to confirm compliance with the requirements established by this Code, documents obtained under the legislation of foreign countries may be used if they confirm compliance with the requirements that are equivalent to or higher than the requirements established by this Code.

Article 176. Sector-specific regulatory principles

1. Subjects of legal relations in the digital environment shall have the right to freely create and use telecommunications networks in the Kyrgyz Republic (the freedom of telecommunications principle).

2. Regulation of activities related to the creation and use of telecommunications networks shall ensure continuity of their operation and inadmissibility of arbitrary termination or suspension of the telecommunications networks' operation or interference in their operation (the continuity principle).

3. Regulation of the establishment and use of telecommunications networks shall ensure their continuous development and interaction with telecommunications networks of other countries in accordance with generally recognized international practice (the development principle).

4. Telecommunication networks and their regulation should be organized in such a way as to facilitate an increase in the number of users who are able to interact with each other using telecommunication networks (the interconnection principle).

5. Sustainable development of telecommunication networks and implementation of their regulation principles shall only be possible if telecommunication networks and their elements are compatible (the compatibility principle).

6. In the operation and use of telecommunications networks, the integrity and inviolability of transmitted digital data shall be ensured, and the telecommunications networks owner shall not have the right to control the content of transmitted digital data, nor are they liable for their content (the inviolability principle).

7. The Kyrgyz Republic shall ensure and maintain equal competition conditions for all telecommunications operators regardless of their form of ownership by regulating and suppressing monopolistic activities, providing equal access to radio frequency resource and

numbering resource, and protecting the records principals' interests in such resources (the non-discrimination principle).

Article 177. Categories of telecommunication networks

1. In the Kyrgyz Republic, telecommunication networks shall be divided into the following categories based on their purpose:

1) public, intended for provision of publicly available telecommunication services to an unlimited number of people;

2) internal, designed to provide telecommunication services to a limited number of users in the interests of one or a group of legal entities;

3) closed, designed to provide telecommunication services to a limited number of users in the interests of one or a group of legal entities without access to them from public telecommunication networks;

4) classified, intended to provide telecommunication services to a limited number of users in cases stipulated by the Kyrgyz Republic legislation on protection of state secrets;

5) television and radio broadcasting intended for the provision of broadcasting services.

2. Closed and classified telecommunications networks shall not be subject to Articles 176, 178, 181-184 of this Code.

3. The Kyrgyz Republic normative legal acts on the protection of state secrets shall regulate requirements for the organization, operation of classified telecommunication networks and the procedure for the provision of telecommunication services in such networks. The authorized state body responsible for ensuring national security shall control over the fulfillment of the requirements.

4. The government communications network of the Kyrgyz Republic shall refer to classified telecommunication networks.

Article 178. Placement of telecommunication networks

1. Telecommunications operators shall have the right of way (the right to construct, install, operate, maintain and repair telecommunications networks and their elements, and telecommunications facilities) in relation to land plots allocated for public use (including public roads, sidewalks or other public land or facilities).

2. Telecommunications operators shall have the right to construct, install and operate supports, lines and other telecommunications facilities on the land plots, buildings and structures, pole supports, bridges, pipelines, roads, collectors, railroad tunnels, and other places, based on an agreement with owners of such land plots or facilities. Under the civil legislation, owners of land plots, buildings and structures should conclude agreements as provided for in this part.

3. Any construction and operation of telecommunication networks or facilities shall be carried out following the environmental safety standards and architectural and artistic requirements for the infrastructure in respect of which such works are carried out. In doing so, measures shall be taken to mitigate possible damage to the owner's property or rights regarding the construction and operation of telecommunications networks or facilities, and in connection with the rights-of-way granted. Upon completion of any construction, installation or repair of telecommunications networks or facilities, the telecommunications operator shall, at its own expense, restore the affected infrastructure to its original condition.

4. A telecommunications operator shall be obliged to compensate for damage caused to the building, land plot or structures as a result of construction, installation, repair, as well as operation of telecommunications networks or structures, including any reduction in the value of these facilities.

5. In emergency cases, when a telecommunications operator needs to carry out urgent work to restore or install telecommunications networks or structures on the land, in the building or other structures that are not the property of such operator, the telecommunications operator shall be obliged to make every effort to promptly notify the owner of the land, building or other structures and obtain his/her consent to carry out such work. The absence of the owner's consent shall not constitute an obstacle to these works and shall not exempt the telecommunications operator from compensation for any damage caused in the performance of such works. In accordance with the legislation, the cost of damage shall be determined by the independent appraisal commission.

6. Telecommunications operators shall be required to enter into and execute agreements to provide other telecommunications operators with access to conduits, collectors, rights-of-way, poles and other telecommunications facilities where technically feasible. Any telecommunications operator utilizing such conduits, collectors, rights-of-way, supports and other structures shall:

1) ensure that its own facilities and services do not cause technical or physical obstacles or interference with the operation of systems, provision of services and other activities of the owner of said facilities;

2) take immediate action to remove any such obstruction or hindrance;

3) fully compensate all costs, damages or other economic losses incurred as a result of the aforementioned obstacles or hindrances.

7. The telecommunications operator shall dismantle telecommunications networks, facilities and equipment independently and at its own expense. Forced dismantling of telecommunication networks, structures and equipment shall be carried out only by court decision, unless otherwise stipulated by the agreement provided for in paragraph 2 of this Article.

Article 179. Telecommunications industry regulator

1. Activities related to telecommunications networks and supervision of such activities shall be regulated by the authorized state body created in the manner established by Article 9 of this Code (the telecommunications industry regulator). The telecommunications industry regulator shall be independent in its activities on the persons over whom it exercises its powers.

2. The head of an telecommunications industry regulator should have the necessary qualifications, experience and digital expertise to perform their duties and exercise their powers.

3. The telecommunications industry regulator shall:

1) implement the state programs and plans for the development of telecommunications in the Kyrgyz Republic;

2) perform functions of the communications administration of the Kyrgyz Republic when implementing the international activities in the field of telecommunications;

3) in the manner prescribed by law, interact with self-regulatory bodies in the field of telecommunications;

4) organize the collection of statistical and other information on the telecommunications operators’ activities;

5) perform functions of the telecommunications licensing authority;

6) take measures provided for by the antimonopoly legislation to protect and develop competition in the telecommunications sector, including regulating the prices (tariffs) of natural monopolies, including their establishing, revising, or approving them;

7) organize compulsory confirmation of conformity of digital devices used within telecommunication networks, including radio-electronic means;

8) develop, update draft technical regulations and national standards, and in cooperation with the state standardization body register national standards with the establishment of technical requirements and norms of application of international (regional) standards;

9) assess the digital resilience of telecommunications networks of telecommunications operators and publish its results;

10) conduct state supervision over compliance of the principals' activities with the entries in the radio frequency register and the numbering register with conditions of such entries;

11) create, develop and operate the state radio control system in the territory of the Kyrgyz Republic for general measurements of radio frequency use, verification of technical and operational characteristics of transmitted radio signals, detection and identification of interference, unauthorized radio transmitters and sources of high-frequency electromagnetic radiation;

12) participate in the development of methods of training, advanced training of state and municipal employees and other persons in the field of telecommunications;

13) identify and eliminate radio interference or unauthorized signals in the territory of the Kyrgyz Republic, interact with authorized telecommunications bodies of other states aimed at eliminating the interference effect of radio-electronic means of other states on the Kyrgyz Republic radio-electronic means of telecommunications operators.

4. The telecommunications industry regulator’s activities shall be financed from the state budget funds and from annual deductions from telecommunications operators in the amount of 0.9 percent of their revenue from the telecommunications services they provide (to be fully credited to the republican budget, of which 40 percent is directed to the telecommunications sector development, 60 percent - to the digitalization development), and from other sources of financing not prohibited by the Kyrgyz Republic legislation.

5. To achieve transparency of its regulatory functions, the telecommunications industry regulator should publish an annual report on its activities and results of the digital resilience assessment of telecommunications networks on its website.

6. In connection with its activities the telecommunications industry regulator shall have the right to:

1) request and receive from individuals and legal entities the information necessary for exercise of its powers, including information classified as state secrets or other secrets protected by law, free of charge;

2) demand from the telecommunications operator to take measures to comply with license requirements;

3) apply to the court with claims in defense of the rights of telecommunications operators or telecommunications services users, as well as the records principals in the radio frequency resource and numbering resource, including in defense of rights of an indefinite number of persons, and represent their interests in court;

4) forward materials to law enforcement authorities in accordance with the jurisdiction, to decide whether initiate criminal proceedings from crimes in the field of telecommunications;

5) submit proposals to the Cabinet of Ministers on adoption, amendment or repeal of telecommunications normative legal acts.

6) hold liable the persons guilty of violating this Code.

7. The telecommunications industry regulator shall be obliged to:

1) ensure compliance with license requirements and conditions for the use of radio frequency resource and numbering resource;

2) carry out regular inspections of compliance by telecommunications operators and records principals in the radio frequency resource and numbering resource with provisions of this Code and issue binding decisions based on the inspections results;

3) ensure the implementation of decisions of the National Radio Frequency Commission;

4) ensure the fulfillment of obligations imposed on telecommunications operators in the interests of national security, defense, law enforcement and emergency situations;

5) consider complaints and appeals of telecommunications operators and users of their telecommunications services, and, based on the consideration results, take binding decisions within its powers;

6) give explanations on application of this Code and normative legal acts adopted in accordance therewith in the field of telecommunications at the request of individuals and organizations, with publication of such explanations on its website;

7) develop and publish recommendations for developing telecommunications, develop and publish standard forms of agreements, legal acts and other documents in the field of telecommunications.

Article 180. Participation in international telecommunications regulation

1. The Kyrgyz Republic is a member of the International Telecommunication Union and shall recognize its basic documents:

1) Charter of the International Telecommunication Union;

2) Convention of the International Telecommunication Union;

3) administrative regulations – International Telecommunication Regulations, Radio Regulations.

2. Within the scope of its powers and in accordance with international treaties in force under the laws of the Kyrgyz Republic, the telecommunications industry regulator shall:

1) ensure, where necessary, the international recognition of radio frequency assignments of the Kyrgyz Republic by taking measures to enter them into the International Reference Register of Radio Frequencies with positive conclusion;

2) protect radio frequency assignments from harmful interference created by owners of radio-electronic equipment and high-frequency devices from other countries, by analyzing international information circulars on frequencies of the Radiocommunication Bureau of the International Telecommunication Union and taking measures to prevent interference in accordance with the Radio Regulations or intergovernmental agreements on the use of the radio frequency spectrum, if any;

3) cooperate with communication administrations of other countries in coordination and (or) mutual recognition of allocated radio frequencies and frequency assignments based on the Radio Regulations or intergovernmental agreements on the use of radio frequency spectrum;

4) harmonize the National Radio Frequency Allocation Table of the Kyrgyz Republic with the International Radio Frequency Allocation Table;

5) harmonize the National Numbering Plan with decisions of international organizations;

6) ensure participation of the sector specialists and scientific and educational organizations engaged in the training of telecommunications personnel in the conferences and research commissions of the International Telecommunication Union.

3. Membership fees for participation of the Kyrgyz Republic in the international telecommunications organizations' activities shall be paid from the budget of the sector telecommunications regulator.

Chapter 22. Interaction of Digital Technology Systems Owners Among Themselves and with Government Agencies

Article 181. Licensing of the telecommunication operators' activity

1. A subject of legal relations in the digital environment shall be recognized as a telecommunications operator and shall be obliged to act based on a license if it simultaneously meets the following three criteria:

1) is or intends to become the owner of a public telecommunication or broadcasting network located in the Kyrgyz Republic;

2) provides or intends to provide telecommunication services to users in the Kyrgyz Republic using such telecommunication network;

3) uses or intends to use radio frequency spectrum and/or numbering and/or infrastructure in the Kyrgyz Republic to provide telecommunication services.

2. A subject of legal relations in the digital environment intending to operate as a telecommunications operator should apply to the telecommunications industry regulator for a license. A subject of legal relations in the digital environment that received a license to operate as a telecommunications operator shall be obliged to begin providing telecommunications services and ensure compliance with licensing requirements within two years from the date of receipt of the license.

3. The procedure for obtaining a license for telecommunications operator activity, as well as its suspension, renewal, termination, reissuance shall be determined by the Regulation on licensing the telecommunications operator activity approved by the Cabinet of Ministers. In accordance with the non-tax revenue legislation of the Kyrgyz Republic, when issuing, re-issuing a license and (or) permit and issuing duplicates thereof, a state duty shall be charged. The license for the telecommunications operator activity shall be perpetual.

4. Licensing requirements shall be established by the Cabinet of Ministers and shall include:

1) ownership and operation of a telecommunication network in the Kyrgyz Republic;

2) use of radio frequency spectrum, numbering or infrastructure in accordance with this Code;

3) interaction with public networks in the Kyrgyz Republic in accordance with this Code;

4) interaction with state bodies of the Kyrgyz Republic in accordance with this Code;

5) transfer of payment for the use of radio frequency spectrum and numbering in accordance with this Code;

6) annual contributions of 0.9 percent of revenue from telecommunications services.

5. Establishment of other licensing requirements, except those stipulated by this Code and relevant acts of the Cabinet of Ministers, shall not be allowed.

6. Virtual operators cannot operate without interaction with a telecommunications operator.

7. The telecommunications licensing control shall be carried out in accordance with the Licensing Regulation approved by the Cabinet of Ministers.

Article 182. Bidding for the right to use radio frequencies

1. In its decision, the telecommunications industry regulator shall determine the form of bidding for service radio frequencies:

1) bidding shall be conducted in the form of a tender, if in order to implement the principles of regulation established by this Code, radio frequencies shall be allocated to the participant who proposed the best investment project;

2) in all other cases of the service radio frequencies allocation, bidding shall be conducted in the form of an online auction.

2. The tender winner shall be determined by the tender committee consisting of at least 7 persons, formed by the Cabinet of Ministers decision from representatives:

1) Jogorku Kenesh of the Kyrgyz Republic;

2) Cabinet of Ministers;

3) National Radio Frequency Commission;

4) Telecommunications industry regulator;

5) professional associations of telecommunications operators.

3. Persons who are personally interested in the tender results (including individuals who have submitted applications to participate in the tender or who are in employment relationships with persons who have submitted such applications), or individuals who may be influenced by the tender participants (including individuals who are participants (shareholders) of legal

entities, members of their management bodies, or creditors of the tender participants) may not be members of the tender committee.

4. The starting price of an online auction shall be calculated based on:

1) the nominal bandwidth or radio frequency band (reception-transmission);

2) geographic coverage area;

3) commercial attractiveness coefficient;

4) calculation coefficient.

5. To be admitted to the auction, bidders shall pay a guarantee fee of 5% of the lot starting price. The online auction step shall make 5% of the lot starting price.

6. The guarantee fee shall be refundable:

1) when tenders are recognized as invalid;

2) to bidders who were not recognized as the auction winners.

7. The tender date and terms shall be set by the telecommunications industry regulator and published on its website no later than thirty calendar days before the tender date.

8. The auction winner shall be the person who offered the highest price for the lot. The bidding winner shall be the person that proposed the best investment project in accordance with the published terms and conditions of investment project evaluation.

9. The bidding results shall be formalized by a protocol signed by all members of the tender committee. The online auction results shall be determined based on the online auction system reporting form, which has the force of a protocol.

10. The bidding shall be recognized as failed in the following cases:

1) either no bids were submitted or no bidders registered for the online auction;

2) none of the bids complies with the tender terms and conditions;

3) no reporting form was created as a result of the online bidding;

4) none of the online auction registered participants raised the starting price within thirty minutes from the start of the online auction.

11. Data on the bidding results shall be posted on the website of the telecommunications industry regulator no later than one business day following the day of its completion.

12. The auction winner shall be obliged to pay the lot price within seven banking days after the day of publication of the auction results. If the winner fails to pay the established price within the stipulated period, the right to use the radio frequency spectrum shall be transferred to the second-place winner. If the set price is not paid by any of the bidders, the bidding shall be repeated.

13. The Cabinet of Ministers shall establish the procedure for bidding.

Article 183. Interaction with the telecommunications industry regulator in maintaining digital registries

1. Decision to allocate or assign radio frequencies or to allocate a numbering band shall be made based on an application submitted in a form approved by the telecommunications industry regulator and published by it on its website. The time period for making decision and creating a corresponding entry in the digital register may not exceed:

1) One business day from the date of payment of the full value of the lot price determined based on the bidding results - in case of allocation of radio frequencies based on the bidding results;

2) Ninety calendar days from the date of the application receipt (including the deadline for provision of electromagnetic compatibility service) - for allocation or assignment of radio frequencies in other cases;

3) 15 business days from the date of receipt of the application - in case of allocation of numbering.

2. The telecommunications industry regulator shall make decision to refuse to allocate or assign radio frequencies in cases where it is impossible to ensure electromagnetic compatibility

of the radio frequency with the characteristics specified in the application and the data in the submitted application are unreliable. If the decision was made based on the bidding results, the decision on allocation of radio frequencies shall be made only in favor of the bidder recognized as the winner.

3. The industry regulator shall amend the record in the relevant register no later than three business days following the day of receipt of the data on:

1) reorganization of the legal entity;

2) changes in the name of the legal entity;

3) change of the last name, first name, patronymic of an individual;

4) redistribution, joint use, alienation of the relevant accounting object;

5) changes in the radio service due to transition to new technologies that improve the characteristics of the telecommunication services provided;

6) extension of the right to use radio frequencies;

7) changes in the conditions of use specified in the record;

8) amendments to the National Table of Radio Frequency Allocation or the National Numbering Plan;

9) termination of the right to use the relevant accounting object in full or in part;

10) detection of errors after creation of the record, including in case of inconsistency of the record data with decision of the communications industry regulator, based on which the record was created or amended.

4. If amendments to a record in the radio frequency register are related to changes in the National Table of Radio Frequency Allocation, to changes in the ratings or radio frequencies bands or to changes in the established conditions for their use, the telecommunications industry regulator shall take measures to ensure electromagnetic compatibility of radio frequencies before the record is amended. There is no charge for ensuring electromagnetic compatibility. The state shall compensate the costs incurred by the record principal in transition to other frequencies by decision of the telecommunications industry regulator before expiration of the allocation or assignment.

5. The radio service due to transition to new technologies may be changed following the generally recognized international practice and only if the electromagnetic compatibility is ensured.

6. The right to use the radio frequency spectrum shall be extended based on the corresponding record principal's application. The right to use the radio frequency spectrum shall be extended for a period of not less than 5 and not more than 10 years. At the same time, the right to use the radio frequency spectrum may be extended for a period of less than 5 years solely at the principal’s initiative, if in the application the principal has indicated the extension period of less than 5 years.

7. A fee shall be charged for extension of the right to use the radio frequency spectrum, calculated depending on the requested extension period, in the following amounts:

1) for each full calendar year - in the amount of 1% of the estimated starting price of such frequencies;

2) for each calendar day in the amount of 0.00273973% of the estimated starting price of such frequencies (when calculating for incomplete calendar year).

8. If the requested extension period consists of a full calendar year(s), calendar months and calendar days, calendar months shall be converted to calendar days, and the extension fee shall be calculated in accordance with subparagraphs 1 and 2 of paragraph 7 of this Article.

The estimated starting price of frequencies shall be calculated at the time of the extension decision in accordance with the Regulations on the procedure for bidding for the right to use the radio frequency spectrum, approved by the Cabinet of Ministers.

9. When extending the right to use the radio frequency spectrum exclusively for purposes not related to the provision of telecommunication services and/or fulfillment of public

obligations imposed in accordance with the legislation, the respective records principals shall be exempted from paying the fee provided for in part 7 of this Article.

10. The right to use the radio frequency spectrum shall be terminated in cases of:

1) the record principal's application to terminate the right;

2) termination of the record principal’s activity, including in case of liquidation of a legal entity without legal succession, death of an individual or recognition of an individual as legally incapable;

3) expiration of the term for which the right was granted, in the absence of an application by the record principal for its extension;

4) entry into legal force of a court decision to cancel the telecommunications industry regulator decision based on which the record was created in the register;

5) failure to use radio frequencies within two years from the date when the right to use them arose.

11. The right to use numbering shall be terminated completely in the following cases:

1) the record principal's application for the right termination;

2) failure to use the allocated numbering range within one year from the date of creation of the corresponding record in the digital numbering register;

3) use of numbering in violation of the Kyrgyz Republic National Numbering Plan.

12. The right to use numbering shall be terminated in a separate part of the numbering range by making appropriate changes in the record in the digital numbering register in the following cases:

1) the record principal’s application with statement of refusal of part of the numbering range;

2) use of numbering in the volume less than 20% of the range specified in the respective record within two years from the date of creation of the respective record in the digital numbering register. In such case, 80% of the unused numbering shall be excluded from the right of use;

3) use of numbering in violation of the Kyrgyz Republic National Numbering Plan.

13. Upon application by the record principal in the digital register, the telecommunications industry regulator shall create and transmit to him copies of the records relating thereto in the form of paper documents or digital documents signed by an authorized officer of the telecommunications industry regulator. The time period for creating and transmitting copies may not exceed five business days from the date of receipt of the record principal's application.

14. The procedure for interaction in maintaining digital registers shall be determined by the telecommunications industry regulator, complying with requirements of this Code.

Article 184. Interaction of telecommunications operators in the process of redistribution, joint use and transfer of radio frequencies and numbering

1. The record principals in digital registers may interact for the following purposes:

1) redistributing among themselves the radio frequencies allocated to them;

2) joint use of radio frequencies allocated to them;

3) alienation of radio frequencies allocated (assigned) to them.

2. The redistribution, joint use and transfer of relevant accounting objects shall be carried out based on an agreement between the record principals with mandatory notification to the telecommunications industry regulator. In case of redistribution, the notification shall be accompanied by a draft agreement describing the purposes and terms of such redistribution.

3. In accordance with paragraph 2 of this Article, the telecommunications industry regulator shall take one of the following actions within thirty days from the date of receipt of the notification:

1) decide to hold an online auction (if the telecommunications operator decides to alienate radio frequencies);

2) make changes to the record in the relevant register (in case of redistribution or joint use of radio frequencies, alienation of numbering);

3) decide to prohibit the redistribution, joint use or alienation of the relevant objects (in case if the goals or conditions of redistribution, joint use or alienation of the accounting objects fail to comply with the Kyrgyz Republic National Table of Radio Frequency Allocation or the National Numbering Plan).

4. The alienation of radio frequencies, the right to use of which was obtained through tenders, shall be carried out by a single lot at an online auction in the procedure established in accordance with this Code. The industry regulator shall decide on the online auction at the same time as issuing consent to the agreement. The agreement on the alienation of radio frequencies shall be concluded with the online auction winner. The online auction winner shall pay the lot price to the record principal, who alienates the right to use radio frequencies, and also shall pay fee to the telecommunications industry regulator in the amount of 5% of the final lot price, which shall be channeled to the telecommunications industry regulator development.

Article 185. Interoperability with digital technology systems for mobile device identification

1. Mobile devices used to receive services in the networks of telecommunications operators of the Kyrgyz Republic shall be subject to mandatory registration in the state digital technological system of the mobile devices identification.

2. Telecommunications operators shall be obliged to provide telecommunications services to registered mobile devices.

3. The Cabinet of Ministers shall determine the procedure for functioning of the state digital technological system for mobile devices identification, their interaction with telecommunications operators, mobile devices registration procedure, terms for imposing restrictions on servicing of unregistered mobile devices.

Article 186. Interaction of telecommunication operators in the digital technological system to counter fraud

1. To protect rights and legitimate interests of citizens and legal entities from fraudulent actions committed using telecommunications networks and services, digital financial services, an interaction system shall be established between telecommunications operators, law enforcement agencies, commercial banks, microfinance organizations (microcredit and microfinance companies), and other payment service providers (hereinafter referred to as “interaction participants”).

2. The digital technology system for combating fraud shall aim at promptly identifying, preventing, suppressing and investigating the fraud cases related to:

a) unauthorized access to remote banking systems or electronic wallets;

b) telephone fraud (vishing);

c) sending phishing or malicious messages via telecommunications networks (SMS phishing, smishing);

d) creation of fake (phishing) web resources of financial and other organizations;

e) other types of fraud, using telecommunications for the purpose of committing or facilitating unlawful financial acts.

3. Telecommunications operators shall be required to:

a) implement and use technical devices and software to detect and block fraudulent traffic, including calls and messages from falsified numbers, unauthorized mass mailings, and traffic

re-directing to known phishing resources, in accordance with procedures established by the Cabinet of Ministers;

b) immediately, upon a lawful and reasonable request from law enforcement agencies, provide the information necessary to identify, prevent, suppress and investigate fraud, including data on connections, subscriber numbers, location of equipment at the time of suspicious actions, in strict compliance with the Kyrgyz Republic legislation on the protection of personal data;

c) participate in the automated exchange of information with other participants of interaction on the detected fraudulent numbers, malicious links, signs and schemes of fraud, in the order and formats determined by the Cabinet of Ministers;

d) inform users about fraud risks and precautions.

4. Commercial banks, microfinance organizations and other payment service providers shall:

a) implement and use the digital anti-fraud technology system to identify suspicious and unauthorized customer transactions that have signs of connection with fraud committed using telecommunications;

b) immediately upon a lawful and reasonable request from law enforcement agencies, provide information on suspicious transactions, accounts and electronic wallets allegedly used for fraudulent purposes, in strict compliance with the Kyrgyz Republic legislation on banks and banking activities, commercial secrets and the personal data protection;

c) participate in the automated exchange of information with other participants in the interaction on identified fraudulent transactions, accounts, methods used and signs of fraud in the manner and formats determined by the Cabinet of Ministers in agreement with the National Bank of the Kyrgyz Republic;

d) inform customers about fraud risks, measures for safe use of remote financial services and actions in case of suspicion of fraud;

e) apply measures to suspend or block suspicious transactions in accordance with the Kyrgyz Republic legislation and regulatory acts of the National Bank of the Kyrgyz Republic.

5. All actions on exchange and processing of information under this Article shall be carried out in strict compliance with the Kyrgyz Republic legislation on personal data protection, banks and banking activities, telecommunication secret and other legally protected secret.

Article 187. Interaction with law enforcement agencies

Legislation on counterintelligence and intelligence activities, as well as operational-investigative activities shall establish interaction between telecommunications and virtual operators and authorized state bodies engaged in the operational-investigative and counterintelligence activities.

Article 188. Interaction between virtual operators and telecommunication operators

1. The interaction of virtual operators with telecommunications operators shall be based on an agreement providing for:

1) the virtual operator’s right to use the telecommunications network of the telecommunications operator;

2) the procedure for interaction of the telecommunications operator with the virtual operator users;

3) requirements to the terms and conditions of the virtual operator's user agreement;

4) the procedure for interaction of the virtual operator with law enforcement authorities using the telecommunications operator’s telecommunications network;

5) procedure for accounting of the volume of telecommunication services and settlements for them;

6) distribution of responsibility between the parties in the course of interaction;

7) grounds and consequences of the agreement termination.

2. Upon conclusion of an agreement under this Article, the parties shall transmit a copy thereof to the telecommunications industry regulator within thirty calendar days from the date of conclusion of such agreement.

Article 189. Interconnection

1. A telecommunications operator shall have the right to interact with other telecommunications operators in the Kyrgyz Republic using telecommunications networks.

2. Interaction between telecommunications operators using telecommunications networks shall be carried out based on an interconnection agreement concluded in the manner established by this Code.

3. A telecommunications operator that has received a request to enter into an interconnection agreement shall provide response specifying the terms and conditions of the interconnection, namely:

1) technical conditions concerning the network connection;

2) location of the network connection points;

3) procedure for traffic transmission through telecommunication networks;

4) cost of network connection, traffic transmission and the procedure of settlements for them;

5) procedure for interaction of the telecommunication network management systems.

4. If telecommunications operators have failed to conclude an interconnection agreement within three months from the date of the initial request, each of the telecommunications operators shall be entitled to apply to the telecommunications industry regulator to resolve the interconnection dispute in accordance with the procedure established by this Code.

5. Telecommunications operators shall be obliged to submit the signed interconnection agreement or amendments thereto to the telecommunications industry regulator within a period not exceeding one month from the date of signing or amending it.

6. The telecommunications operator recognized as an economic entity occupying a dominant position in accordance with the antimonopoly legislation shall be obliged to establish equal terms of interconnection with any telecommunications operator, including its affiliates. For the telecommunications operator recognized as an economic entity occupying a dominant position under the antimonopoly legislation, conclusion of an interconnection agreement shall be mandatory.

7. After signing the interconnection agreement, telecommunications operators may not unilaterally interrupt interaction in full or in part, or terminate the interaction agreement, except for the cases listed in this part of the Article.

The interconnection may be partially terminated:

a) based on a judicial act that has entered into legal force;

b) in case of detection of the fact of modification, suppression and (or) other way of changing the number data transmitted via telecommunications networks;

c) in case of revealing the fact of conducting lotteries, voting, contests, quizzes, polls, mass calls or mailings of messages, dissemination of advertising information not coordinated between telecommunications operators;

d) in case of failure to reach an agreement on financial conditions of traffic transmission within two months, if both parties provide connection to their network users through the networks of other telecommunications operators;

The interconnection can be terminated in full:

a) based on a judicial act that has entered into legal force;

b) in case of arrears under the interconnection agreement for a period of three months or more.

An interconnection agreement may be terminated in the following cases:

a) termination or revocation of the telecommunications operator's license;

b) termination of the telecommunications operator’s operation;

c) complete withdrawal of the numbering resource used within the interconnection;

d) in case continuous absence of user traffic for sixty consecutive calendar days. In this case, the telecommunications operator that initiates termination of the interconnection agreement should have data from the billing system and data on interconnection channel utilization confirming absence of user traffic for sixty consecutive calendar days.

8. A telecommunications operator terminating an interconnection unilaterally shall notify the telecommunications industry regulator no later than the business day following the day of the interconnection termination.

9. The telecommunications operator shall notify the telecommunications industry regulator of all instances of arrears under the interconnection agreement exceeding the two-month interconnection period.

Article 190. Dispute consideration

1. In case of disputes arising on the interaction between telecommunications operators, either party shall be obliged to apply to the telecommunications industry regulator as a pre-trial procedure.

2. To achieve peaceful resolution of the dispute, the parties shall conduct preliminary negotiations and correspondence.

3. The telecommunications industry regulator shall consider a request for pre-trial dispute resolution within two months from the date of its receipt.

4. For the purpose of dispute consideration, the telecommunications industry regulator shall have the right to request any data the provision of which cannot be refused.

5. The telecommunications industry regulator shall not consider dispute in the following cases:

1) if the dispute subject matter does not involve the use of digital technology.

2) if the dispute subject is conclusion of an interconnection agreement, and less than 3 months have passed from the moment when one telecommunications operator sent a request for agreement conclusion to the other operator;

3) If more than 1 year has passed since the date of the last action taken during the negotiation process.

6. In the cases specified in paragraphs 1 and 3 of part 5 of this Article, telecommunications operators shall have the right to apply directly to the court.

7. To resolve the dispute, in its decision, the telecommunications industry regulator shall have the right to set technical and (or) financial terms of interaction that will be binding on the parties in its decision.

8. The telecommunications industry regulator shall make a decision on the dispute based on the available and provided data related to the dispute subject. The telecommunications industry regulator’s decision shall be issued in the form of an administrative act and may be appealed in court.

9. In accordance with the legislation on offenses, if the telecommunications industry regulator fails to make a decision within the specified timeframe outlined in part 3 of this Article, the dispute will not be considered resolved, with the head of the regulator held liable for inaction.

Chapter 23. Artificial Intelligence Systems

Article 191. Principles of design, development and application of artificial intelligence systems

1. Artificial intelligence systems shall be designed, developed and applied in the Kyrgyz Republic without restrictions, except in cases established by this Code.

2. The way in which artificial intelligence systems are designed, developed and applied shall be determined by their owners, taking into account internationally recognized practices, based on the following sector principles:

1) regulation, development and use of artificial intelligence systems taking into account the need to reduce the risks of harm to protected goods (the risk reduction principle);

2) clarity and predictability of the characteristics of the artificial intelligence system, availability of technical documentation for it (the openness principle);

3) clarity of the grounds for decisions or recommendations of the artificial intelligence system, the possibility of re-checking such grounds (the explainability principle);

4) effective human control over the use of artificial intelligence systems (the principle of controllability);

5) accuracy of the results of application of artificial intelligence systems corresponding to the purposes of their application (the accuracy principle);

6) resilience of artificial intelligence systems to random failures and malfunctions based on taking measures to prevent disruptions in the system operation and preservation of its main functions in case of failures or unplanned external influences (the reliability principle);

7) protection of artificial intelligence systems from unauthorized external influence (the security principle).

3. The principles defined in this Article shall form the basis of legal regulation of relations on design, development, application of artificial intelligence systems, and determining the requirements for artificial intelligence systems. Fulfillment of the established requirements for artificial intelligence systems shall ensure compliance with the principles stipulated in this Article.

Article 192. Limitations and liability related to the design, development and use of artificial intelligence systems

1. This Code may establish mandatory requirements or other restrictions with respect to high-risk artificial intelligence systems only for the purpose of minimizing the risk of harm to the following goods (protected goods):

1) human life and health;

2) human and civil rights and freedoms;

3) environment;

4) defense capability of the state;

5) national security of the state;

6) public order.

2. The design, development or use of artificial intelligence systems for the purposeful and knowingly unlawful infliction of harm to protected goods shall be prohibited.

3. The artificial intelligence systems owners and users, regardless of the degree of their danger, shall be obliged to take all reasonable and necessary measures to minimize the risks of

harm to protected goods when designing, developing or using such systems. They shall be liable for the harm caused in accordance with the Kyrgyz Republic legislation.

4. The rules and standards for the design, development and application of artificial intelligence systems may be established by the regulations of a professional association of the artificial intelligence systems owners and include requirements to professional ethics, risk assessment of artificial intelligence systems, risk management, design and development of artificial intelligence systems, digital data management and quality management system, as well as other requirements that do not contradict this Code and are mandatory for execution.

Article 193. Artificial intelligence system risk assessment

1. All artificial intelligence (AI) systems used in the Kyrgyz Republic shall be subject to assessment of risk their use may pose to protected goods.

2. The AI system owner shall perform the risk assessment:

1) at the stage of designing an AI system or planning changes to it;

2) upon completion of development and before the start of application of the AI system or planned changes made to it;

3) in case of any unplanned change in the AI system or in its application environment, of which the system owner or user becomes aware, and which may affect the risk assessment result.

3. The AI system owner shall carry out a risk assessment according to his or her own methodology, in accordance with the requirements established by the Cabinet of Ministers and taking into account generally recognized world practice.

4. The results of the AI system risk assessment and the assessment methodology shall be posted on the AI system owner's website in a form that is simple, understandable to individuals, as well as in open data format, except for information related to state secrets.

Article 194. High-risk AI system

1. High-risk AI systems are those systems which use, compared to alternative methods, increases the risk (likelihood or extent) of harm to protected goods to a level that requires risk management measures.

2. An AI system, which is classified as a high-risk AI system based on the risk assessment results, may be designed, developed and used subject to compliance with the requirements established by this Code throughout the life cycle of such system.

3. An AI system may not be classified as a high-risk system if its use in making relevant decisions or performing actions is of an auxiliary nature only and does not result in an increased risk of harm to protected goods.

4. The Cabinet of Ministers shall establish, with respect to high-risk AI systems, requirements for:

1) risk management;

2) characteristics of the specified systems that ensure the openness, explainability, controllability, accuracy, reliability and digital stability of such systems;

3) quality of the digital data for such systems;

4) technical documentation for such systems.

5. The owner of high-risk AI system owner shall:

1) ensure that such a system complies with mandatory requirements;

2) implement and maintain throughout the life cycle of such system a risk management system that complies with requirements of this Code;

3) develop proper technical documentation of such system;

4) ensure that the logs of the system's operation are safeguarded while it is under his/her control;

5) confirm the system compliance with the requirements established by this Code before its use;

6) take measures to eliminate the identified non-compliances of the system with the established mandatory requirements;

7) at the request of the relevant authorized state body, suspend, and based on a judicial act that has entered into legal force, terminate the design and development of the system if such actions are carried out in violation of requirements of this Code.

Article 195. Confirmation of compliance of high-risk AI systems with mandatory requirements

1. Prior to the use of a high-risk AI system, its owner shall be obliged to confirm its compliance with the requirements established by this Code by adopting a declaration. The form of the said declaration as well as the requirements for its content shall be approved by the Cabinet of Ministers.

2. The adopted declaration should be set forth in the form of a digital document, signed with a qualified digital signature and posted on the website of the owner of the AI system. The said declaration applies to publicly available digital records.

Article 196. Use of high-risk artificial intelligence systems

1. The high-risk AI system user shall be obligated to:

1) use it in accordance with the operating instructions;

2) ensure the relevance of digital data processed using such a system;

3) ensure effective control of the system's operation during its use, including allocation of necessary resources for this purpose and identification of persons responsible for such control;

4) if there are reasons to believe that using the system in accordance with the operation manual may result in harm to protected goods, immediately notify the system owner and suspend its use;

5) ensure safety of the system's operation logs while it is under his/her control;

6) use the information provided by the system owner to fulfill the duties provided for in this Code;

7) at the authorized state body’s request suspend, and based on a judicial act that has entered into legal force terminate application of such system, if such actions are carried out in violation of requirements of this Code.

2. When using a high-risk AI system to obtain results that are used to make a decision that could result in violation of the rights, freedoms or legitimate interests of individuals or legal entities, the user of the said system shall be obliged:

1) in cases of designing, developing or applying a system for interacting with individuals - consumers, place on its website, and in other cases - provide general information on the system characteristics, principles of its operation, and the principles of obtaining and applying the relevant results in a comprehensible and understandable form;

2) at request of persons whose interests are affected by such decision, provide them with information free of charge in a comprehensible and understandable form that allows them to understand and verify the prerequisites and ways of obtaining the result related to them obtained with use of such system.

3. The high-risk AI system user or another person shall be subject to obligations of the owner of such system if:

1) the system is put into operation on behalf of such a person (under its name, trademark or other similar designation);

2) such person changes the purpose of the system after it has been placed in service, or makes substantial changes to it;

3) the system is put into operation, or its purpose is changed so that it becomes a high-risk AI system or part of such a system.

4. In cases provided for in paragraphs 3 and 2 of part 3 of this Article, the original owner of a high-risk AI system shall be exempt from performing the duties provided for in this Chapter.

5. If a high-risk AI system is used by a user solely for personal or family needs, such user shall be exempt from fulfilling the obligations established by paragraphs 2–6 of part 1 and part 2 of this Article. In cases where the rights, freedoms or legitimate interests of third parties are violated as a result of such use, the user and the person who provided them with access to the relevant system shall be jointly responsible for fulfilling these obligations.

Article 197. Disclosure of information in the application of certain types of AI systems

1. The AI systems owners and users that design, develop or use such systems for the purpose of interacting with individuals – consumers shall be obliged to inform the latter of the fact of interaction with the AI system, except in cases where such interaction is obvious from the situation. Information on the application of AI systems within legal relations in the digital environment shall be publicly available information. This information shall be placed in an accessible and understandable form on the relevant system user's websites and the national ecosystem industry regulator's website.

2. Users of AI systems designed to recognize emotions or classify individuals based on biometric characteristics should inform individuals of the use of such systems on them.

3. The obligations under parts one and two of this Article shall not apply to the design, development and application of such functions of AI systems in respect of which such informing would prevent their lawful intended use for the purpose of ensuring:

1) defense capabilities;

2) national security;

3) public order in terms of detection, prevention, investigation and criminal prosecution.

4. The AI systems users who apply such systems for deepfakes should disclose information about the artificial origin or change of the materials.

5. The obligation provided for in part 4 of this Article shall not apply to cases of lawful use of such images or materials to protect the goods provided for in part 3 of this Article or to exercise the right to freedom of scientific, technical, artistic and other types of creativity, teaching and learning.

6. The application of the exceptions provided for in parts 3 and 5 of this Article shall be permitted only on condition that the necessary measures are taken to protect the human and civil rights and freedoms affected.

Chapter 24. Ensuring Continuity of Relations in the Digital Environment

Article 198. Validity of previously issued documents

1. In accordance with this Code, licenses for radio frequency resource shall be recognized by decisions on allocation of radio frequencies and shall be valid for the entire period specified therein. A license for a radio frequency resource shall be renewed, re-registered, cancelled in accordance with the rules established by this Code for renewal, amendment, termination of the right to use the radio frequency spectrum. Radio frequency resource licenses cannot be re-tendered.

2. In accordance with this Code, permits for frequency assignments shall be recognized by decisions on assignment of radio frequencies and shall be valid for the entire period specified therein. Frequency assignments shall be renewed, re-registered, and cancelled in accordance with the rules established by this Code for renewal, amendment, termination of the decision on radio frequency assignment. At the request of the frequency assignment owner and if there are grounds established by this Code, the telecommunications industry regulator shall be obliged to make a decision on general assignment.

3. In accordance with this Code, licenses for activities in the field of electric communication and in the field of data transmission shall be recognized as telecommunications operator licenses and shall be valid indefinitely. At the request of their holder, licenses for activities in the field of electric communications and in the field of data transmission may be re-registered into the telecommunications operator licenses without charging a fee.

4. In accordance with this Code, entries in digital registers shall be made based on previously issued documents without interrupting the validity of previously issued licenses, permits, decisions on allocation of the numbering resource and certificates, and no additional permits or payments shall be required for making entries in digital registers.

5. In accordance with this Code, electronic signature certificates shall be recognized as digital signature certificates and shall be valid until the expiration date specified therein.

6. The rules of this Code relating to digital identifiers shall apply to simple electronic signatures created before entry into force of this Code.

Article 199. Regulation of relations in the processing and transmission of information without the use of digital technologies

1. This Code shall not regulate transmission of messages that does not involve digital technologies, except for cases of licensing of relevant activity. Such transmission shall be performed based on contracts concluded in accordance with the procedure established by civil legislation.

2. Persons providing services for the transmission of messages without use of digital technologies shall be obliged to observe the secrecy of correspondence, postal, telegraphic and other messages.

3. If it is impossible to fulfill the obligation to notify the subjects of legal relations provided for by this Code using digital technologies due to the lack of relevant contact information, the subject shall be notified in person.

4. Information resources of state bodies or local government bodies presented in the form of non-digital records (state or municipal information resources) shall be subject to transformation into the state or municipal digital resources, respectively. Until digitalization of the state and municipal information resources is completed, the information contained in them is used on the same basis and with the same restrictions as the information contained in the state and municipal digital resources.

Article 200. Formation of the national ecosystem

The state information systems and state information resources owners (processors) shall be obliged to ensure inclusion of their information in the national ecosystem register in accordance with the procedure established by this Code.

President
of the Kyrgyz Republic