Digital Code
of the Kyrgyz Republic

Concept

The Decree of the Kyrgyz Republic President "On Urgent Measures to Enhance the Implementation of Digital Technologies in Public Administration of the Kyrgyz Republic" dated 18 December 2020, provides for the development and submission to the Jogorku Kenesh (Parliament) of the Kyrgyz Republic of the draft Digital Code of the Kyrgyz Republic as a single document, which should build a unified public administration system in the field of digital technology and ensure application of uniform rules regulating social relations connected with use of digital technologies.

The Draft Digital Code of the Kyrgyz Republic (hereinafter - the Draft Code) is the result of a large-scale analysis of the Kyrgyz Republic legislation branches and study of the world's best practices on the digital environment. Adoption of the draft Code, which combines legal regulation and systematization of the entire technology legislation, will create a favorable regulatory and legal environment, which will lay the foundation for development of the digital economy in the Kyrgyz Republic. The results of successful implementation of this task will have a positive impact on economic growth rates, improve public and private sector service delivery, and lead to better investment climate.

Goal and objectives of the Code

The goal of the Code is to create a codified legal framework for relations in the digital economy.

The Code objectives include:

- updating the existing legal framework for relations in the use of information and communication technologies, eliminating the existing gaps and contradictions in it;

- removal of excessive legal barriers to the development of the digital economy;

- creation of conditions for long-term and effective legal regulation of relations, in which advanced digital technologies are used;

- ensuring fair and effective regulation of relations in the digital economy, protection of the rights and legitimate interests of the subjects of such relations;

- encouraging safe and responsible behavior of subjects of relations in the digital economy;

- implementing the world's best practices in regulation of the digital economy into the national legislation.

Subject matter and planned effects of codification

In the Kyrgyz Republic, there are more than a hundred legal acts of different levels, directly or indirectly regulating or relating to the areas of communications and telecommunications, digital governance, digital identity, open data, spatial data, cybersecurity, etc. However, these legal acts have a large number of serious shortcomings, which generally have negative impact on the process of digital transformation and implementation of the digital initiatives. Such shortcomings include: inconsistency of the system of normative legal acts, their fragmentation, existence of a great number of legal conflicts, the backwardness of digital law norms from the current needs of citizens and government bodies, the lack of sufficient legal conditions for quick and barrier-free testing and implementation of innovative digital solutions (digital assets, artificial intelligence, robotics, blockchain, big data, digital platforms and ecosystems, etc.) in the process of public administration, delivery of public and municipal services, and development of the country's digital economy in general, inconsistency of the national legislation with international standards in the field of implementation and use of digital technologies. The complete list of normative legal acts to be repealed or amended in the course of codification is given in the appendix to this Concept.

The adoption of a codified normative legal act will enable introducing a new legal regulation coordinated at once in several areas. Moreover, the draft Code will combine all the existing technological legislation into a single legal act, clearly structured, based on common principles, subjects, which will be easy to apply and keep up to date. At the same time, the draft Code should be flexible enough not to become obsolete before it is adopted.

Codification makes it possible to apply an ecosystem approach to regulation in modern conditions, when the necessary changes are considered immediately in relation to all elements of innovation ecosystems and are introduced, perhaps step by step, but in a coordinated manner in various directions.

In fact, this draft Code acts as a digital constitution, laying the foundations of digital governance, which then guide other branches of legislation. Therefore, the "digital law", like constitutional law, consists of two important elements: first, it is the basis of activity in the digital environment for all (similar to the foundations of the constitutional order); second, it is the rules for the creation and use of objects at the four levels of digital governance: (1) digital data, records and resources, (2) digital services, (3) digital technology systems, including data centers and telecommunications networks, (4) infrastructure to host them. Such rules should be common to all branches of legislation, and government agencies of the Kyrgyz Republic should be referring to them when regulating the digital economy.

An alternative to codification is the mass amendment of the existing legislation. Given the number of regulations governing the digital sphere in the Kyrgyz Republic, the planned large-scale digital transformation cannot be implemented, without revising a large number of normative legal acts, including not only amendments in the existing laws, but also development of new drafts normative legal acts.

The development of regulatory legal acts in various areas of law affecting the development of digital technologies and the digital economy (draft laws, regulatory legal acts at the level of the Cabinet of Ministers of the Kyrgyz Republic - regulations, requirements, instructions, methods ...) is a very long process with extremely low efficiency. Making many changes to existing laws, regulations, rules, instructions with the parallel development of new draft regulations will lead to an inevitable lag, a violation of systemic approaches in rulemaking (technology is developing much faster than the cycle of development, approval and adoption of one law).

Based on the analysis results, it was revealed that the current regulation is outdated and ineffective, and given the need to revise more than a hundred regulatory legal acts at various levels, including amending the existing legislative acts, developing new draft regulatory legal acts, it is impossible to carry out large-scale digital transformations and a digital breakthrough.

New areas are rapidly emerging where previous regulatory approaches do not work (platforms, artificial intelligence, taxation of various transactions in the context of digital transformation; a separate challenge is the use of artificial intelligence technologies in judicial decision-making). Regulated relations in connection with the use of new technologies are often so specific that they cannot be effectively applied to them by any of the regulatory mechanisms available to the country. New technologies are developing extremely quickly, while legal regulation is rather inert due to the complex mechanisms of adoption of regulatory acts, the law always looks to the "past", while technology is developing much faster. For this reason, the only possible way to develop regulation in the digital environment is to codify the rules in this area.

Input data for codification

The codification is based on an earlier analysis of the regulatory gaps in each section of the draft digital code and related legislative changes. The legal framework for digital governance was analyzed in accordance with the principles of best regulatory practices. The deficiencies identified were classified into four types - gaps, outdated regulations, barriers, and dysfunctional regulations.

Provisions of the following documents were used as best international regulatory practices in the digital economy.

1. The 2016 OECD Cancun Declaration on the Digital Economy as an Engine for Cooperation, Security and Growth, enshrining the digital economy as core principles:

- development of ideas of the free circulation of information;
- encouraging free digital creativity and innovation;
- development of digital services systems;
- development of the latest digital technologies, such as the Internet of Things, cloud computing, and digital data analytics

2. Report of the Chairman of the Global Symposium for Regulators (GSR) 2021 (under the International Telecommunication Union), which provides guidance based on best practices (2021), which describes practices:

- introduction of new, efficient and flexible mechanisms for financing digital infrastructure, access and use;
- prototyping regulatory schemes for the digital world after the COVID pandemic;
- guidance for realizing the potential of emerging technologies and business models.

3. The Digital Regulation Handbook (2020) prepared by the International Telecommunication Union in collaboration with the World Bank, is a guide for regulators on appropriate digital regulation standards and assessment of their application, how to regulate responsibilities for collecting, storing, processing and distributing data, and their protection.

4. The World Bank's Data, Digitalization and Governance report on the economies of the Europe and Central Asia region, which provides policy recommendations on how to use the data revolution to improve public administration in countries of the region:

- implementation of mechanisms to encourage the introduction and adaptation of data collection, processing and storage systems within the civil service;;
- scaling up the impact of the data revolution by expanding the digitalization of government activities and ensuring inter-agency coordination of decentralized data collection, processing and storage systems of various institutions;
- encouraging the development of platforms that hold governments accountable to citizens on issues such as the government's overall approach to data use;
- revising the principle of building a "Chinese wall" between citizens and the government through experiments involving direct feedback between the two;
- increased coverage and use of broadband Internet access, especially in Central Asian countries.

5. Report of the Commissioner for Human Rights of the Council of Europe "The Rule of Law on the Internet and in the rest digital world", containing the following recommendations and principles:

- universality of human rights and their equal observance "online" and "offline";
- protection of individuals in the automated processing of personal data as the cornerstone of the rule of law in Internet and in the rest digital environment;
- states should fully comply with their international obligations in the field of human rights, acting (or inactive) in the fight against cybercrime, both in determining the relevant crimes (their elements, related circumstances that exclude and extenuate responsibility), and in the conduct of criminal investigations, execution of sentences, or in the implementation of mutual legal assistance and extradition;
- states should stop delegating to impose restrictions that violate the state's human rights obligations to private companies that control Internet and the rest digital environment;

- states should ensure that any restrictions on access to Internet content that affect users under their jurisdiction are based on the clear and predictable legal rules.

Among the documents that are of a sectoral (specialized) nature and contain best regulatory practices in certain areas of the digital economy, in particular, were used in the Code development:

- General Data Protection Regulation (GDPR);
- World Bank World Development Report 2021 "Data for a Better Life";
- UN Convention on the Use of Electronic Communications in International Contracts (New York, 2005);
- UNCITRAL Model Law on Electronic Commerce (1996);
- UNCITRAL Model Law on Electronic Signatures (2001);
- UNCITRAL Model Law on Electronic Transferable Records (2017);
- Common guidelines for the implementation of digital health of the World Economic Forum and the EDISON Alliance;
- Eight Guiding Principles for the Digital Transformation of the Health Sector (PAHO/EIH/IS/21-0004).

Subject of the Code

The Code's subjects of regulation should be public relations in the digital environment (cyberspace), which are understood as public relations in the processing and exchange of digital data. The concepts of "digital environment" and "cyberspace" should be seen as identical, since they describe two sides of the same phenomenon, namely, the presence of a special sphere of social relations that develop independently of territorial boundaries according to general rules, which form digital environment as a kind of new space (cyberspace).

In regulation of relations in cyberspace, use of the traditional approach, related to the operation of the law in space, reduces rather than increases legal certainty. The limitation of the law scope to the territorial boundaries of the state, even taking into account the conflict norms, does not allow to fully protect the interests of citizens of such a state in transnational ecosystems (usually functioning under the law of one of the world superpowers), and attempts to apply the law extraterritorially only increase the number of conflicts between the legal norms of different legal systems.

As a consequence, the Code subject matter was based the main principle of the law on the scope of persons, combined with the principle of participation of all interested parties, is laid down. The Code is intended to be applied organically by subject on a voluntary basis when such subjects participate in different kinds of digital communities (social media, forums, marketplaces, professional communities and communities of interest) and form the rules of such communities, guided by provisions of the Code. The enforcement of the Code - allowed in exceptional cases - will in fact be applied when not only the Code provisions, but also the relevant provisions of the rules of the digital community have been violated. This approach lays down special requirements for the norms enshrined in the Code, because they should meet the interests not only and not so much of the Kyrgyz state as the digital environment as a global, universal phenomenon.

Relations included in the Code subject matter are not completely homogeneous and should be differentiated on four levels.

At the data level, the relationships associated with the digital data processing, the creation and use of digital records (including in the form of documents) and digital resources are regulated. The objectives of regulation at this level are to ensure the completeness, relevance and accessibility (or inaccessibility, that is, confidentiality) of digital data.

At the service level, the relationships associated with the creation and use of digital services and applications, the building of digital ecosystems, and participation in them are regulated. The objectives of regulation at this level are to ensure the quality of digital services and applications and to protect the rights of their users.

At the systems level, the relationships associated with the creation of digital technology systems, such as data centers and telecommunications networks, as well as the provision of services using them, are regulated. The objectives of regulation at this level are the safety and continuity of digital technology systems, as well as connectivity and interoperability, including for the purpose of transferring data between them.

At the level of infrastructure, the relations concerning the access of owners of digital technological systems to land, buildings, structures, constructions and other similar objects are regulated. The objective of regulation at this level is to ensure non-discriminatory access to facilities that cannot be considered digital economy objects, but without access, to which the development of digital economy infrastructure is impossible.

The Code Method

The Code should resolve the issue of its own method of regulation for the branch of digital law it creates. In its most general form, it can be stated as an access method. Digital legislation may restrict access to objects (e.g., by restricting access to personal data) or, conversely, provide non-discriminatory access to them (e.g., to communication networks or government information resources). The ratio of accessibility/inaccessibility provides the necessary balance between the interests of the objects owners and the interests of the society interested in using such objects for its own development.

The Code should provide for the establishment of:

- the absolute right to the object (data right, which is analogous to the ownership right), which implies that the object owner can manage access to the object, which creates conditions for investment in the digital environment;

- limitations of absolute rights (access rights) established, as in the case of property rights, in the interests of community and development of the digital environment as a whole

Since the Code is based on the principle of technological neutrality, it does not prescribe specific technologies, but only establishes the parameters, under which a particular technology may be available (for example, when bringing unmanned vehicles to market) or unavailable (when establishing a trade secret regime).

Principles of Regulation of Relations in the Digital Environment

The fundamental principles of regulating relations in the digital environment should be enshrined in the Code in order to determine the content and areas of legal regulation. Such principles should serve as guiding ideas for subsequent improvement of the legislation. Public relations in the digital environment are developing rapidly, so legal regulation cannot cover all possible situations. As a basic framework for the subjects of relations in the digital environment and for regulators, the code should establish the principles, some of which define the foundation for legal regulation, while the other part acts as description of the target state that social relations in the digital environment should reach. The general legal principles used to regulate relationships in the digital environment include the principles of fairness, certainty, and participation. The target principles for the regulation of relations in the digital environment include the principle of technological neutrality, the principle of content neutrality, the principles of digital sustainability, openness and accountability. Those principles that relate to specific areas of relations in

the digital environment (for example, telecommunications or public services) should be disclosed in the Special Part of the Code.

Terminology of the Code

Due to the fact that with the adoption of the Code, a new branch of legislation will actually be created that regulates the use of modern digital technologies in the conditions of a developing digital economy, the set of concepts used by the Code (the terminology of the Code) is of particular importance. On the one hand, a careful development of terminology, including concepts not used in the Code itself but necessary to create a logical link between the terms used in the Code, is necessary for the proper understanding and application of the Code. On the other hand, if this approach is implemented, the volume of the glossary (the "Terms and Definitions" chapter) will constitute a significant part of the Code, and there will be more than a hundred terms in it. To resolve this problem, which is mainly of a legal and technical nature, the terminology of the Code will be annexed to the Code. At the same time, given the importance of keeping the terminology up to date, this task should be assigned by the Code to the authorized state body that implements the state policy in the digital environment.

Structure of the Code

Structurally, the draft Digital Code consists of a General Part and a Special Part. The general part of the Code contains the basic normative provisions, which are characterized by a high degree of generalization, stability and lay down the legal basis for the use (application) of the Special Part norms. Provisions of the General Part of the Code lay foundations of the digital law as a new branch of legislation and define the elements of those social relations that are regulated by the Code. The General Part includes two sections that address the issues of the legal foundations of public administration in the digital environment and the elements of legal relations in the digital environment: objects and subjects of legal relations in the digital environment, grounds for the emergence, change and termination of legal relations in the digital environment, exercise of rights and performance of duties in the digital environment.

The Special Part includes the following sections devoted to the regulation of the following objects:

- digital data (personal data; big data, including its use by artificial intelligence and robotics technologies; spatial data);

- digital services (including state and municipal services, digital health services);

- trusted services (including identity services and systems, digital signature services and digital documents);

- digital technological systems, including issues of public-private partnerships in this area and issues of placing digital infrastructure facilities on lands, structures, buildings and facilities;

- telecommunications objects (primarily, telecommunications networks), including the placement of telecommunications networks and their elements on lands, structures, buildings and constructions.

Content of sections and chapters of the Code

Given the planned structure of the Code, the normative provisions on the main regulation issues should be distributed in the following way.

The first chapter of the Code should enshrine the most general provisions, in particular define the subject and method of regulation, the underlying principles of regulation, address the relationship of the Code and other sources of regulation in the digital environment. The issues of the subject, method, and principles of regulation (including the absence of territorial boundaries in the digital environment) were discussed above in this Concept.

The Code should take precedence in regulating relations in the digital environment insofar as the legislation uses the method of digital law, that is, it regulates the establishment or restriction of access to digital data, records, services, systems or infrastructure to house them. Norms of other laws and normative legal acts adopted in accordance with them, defining the rules of establishing or limiting access to digital data, services, systems or infrastructure for their placement, cannot contradict the Code provisions. Although changes to the Code should be made according to the general procedure established by the legislation on normative legal acts, the specifics of regulation in the digital environment should be taken into account, which requires broad participation of the expert community in the discussion and examination of amendments to the Code. At the same time, the results of examination and discussion should be binding, that is, amendments to the Code cannot contradict the position expressed in the course of their examination and discussion. Otherwise, the mechanism of organic application of the Code, when its provisions are implemented by the participants of relations mainly on a voluntary basis, will be violated. By-laws on legal regulation in the digital environment can only be adopted in cases expressly provided for by the Code.

The second chapter of the Code requires defining the goals and activities of state regulation in the digital environment, listing the powers of state bodies to regulate in the digital environment, as well as establishing requirements for the status and structure of authorized state bodies. Substantial limitation of cases of subordinate normative legal regulation imposes restriction on the activities of the authorized state body that carries out public policy in the digital environment. Nevertheless, the powers of such a body should include the development and implementation of programs and plans for the transition to digital governance in the Kyrgyz Republic, monitoring implementation of the Code, other laws of the Kyrgyz Republic, acts of the President and the Cabinet of Ministers of the Kyrgyz Republic regulating relations in the digital environment.

The Code should provide basis for the creation of a system of independent industry regulators, at least in the area of personal data, telecommunications and data exchange for the purpose of providing state and municipal services. Such regulators should function, in accordance with international best practices, based on the principles of independence, accountability, sufficiency of authority, financial, human and technical support. At the same time, the specific structure of bodies engaged in regulation, control and supervision in the digital environment should be established by the Cabinet of Ministers, which provides the necessary flexibility in the evolving digital economy and stability of the Code provisions. The Code should provide a framework for delineation of functions of public policy implementation, coordination and control in the digital environment.

The second section of the Code contains four chapters devoted to the basic elements of legal relations in the digital environment: objects, subjects, grounds for the emergence, change and termination, as well as the actual implementation of such legal relations by exercising the rights and obligations of their participants.

The third chapter of the Code should fix the legal regime of objects of relations in the digital environment, which include:

1) digital data, digital records (including in the form of digital documents) and digital resources;

2) digital services and applications, digital ecosystems;

3) digital technological systems, including data processing centers and telecommunication networks, as well as services provided with their use;

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

This chapter is intended to provide a unified legal regime of objects at different levels of digital governance, so that including data formats and data exchange interfaces in different bodies are compatible with each other, to create a legal basis for building an interoperable decision-making system in the field of digital governance. The provisions of this chapter should create conditions for the necessary transition in the digital economy from electronic document management to management based on records in digital resources, including the distributed ones; to form a legal framework for standardization in the field of electronic document management and circulation of digital records. Since the Code objectives include, on the one hand, to ensure the speedy transition to digital governance as the most effective phase of public administration, and on the other hand, to ensure sustainability of the existing regulatory system, the draft norms relating to the obsolete objects, such as information resources on non-digital media, electronic documents beyond the digital resources, analogue telecommunication networks and services, although they should provide certainty about their use, should be aimed at encouraging their modernization or abandonment. Information systems should no longer be regulated by the Code (because of the regulation of digital technology systems).

For items such as digital records and digital resources, the Code requires that digital rights be established. Digital rights are established as an implementation of a digital law method and provide protection for investments in digital rights objects and the possibility of circulation of such objects. Digital rights are established independently of property rights and exclusive rights, although their exercise should comply with the restrictions established by law. Digital rights may be held jointly by more than one person. The Code provisions in this part should aim to maintain a balance between the interests of digital rights holders and data principals, i.e., those, whom the records relate to.

The fourth chapter of the Code is designed to fix the basics of the legal status of the subjects of digital governance, which include citizens and legal entities, the Kyrgyz Republic and other states, state agencies, local governments, officials. They all have the inalienable right to be digital stakeholders, as well as other rights and responsibilities under the Code and rules of the digital communities. Sustainable legal connection of subjects within the digital environment, forming such a digital environment, in the draft code is understood as digital citizenship. The Code should also describe the main legal statuses (roles) in which the subjects of relations in the digital environment may be. Depending on their activities in the digital environment, subjects may act as owners of digital records, digital resources, digital technological systems or ecosystems, digital service providers, data principals, users, processors, or in other roles provided for by the Code, rules of digital communities or contracts of subjects of relationships in the digital environment. It should be noted that this chapter creates a legal framework to regulate the activities of new digital governance subjects, such as owners of digital ecosystems, preventing them from violating the interests of other participants in the digital economy.

The fifth chapter of the Code should be devoted to the emergence, change, and termination of legal relations in the digital environment. The Code should enshrine rules to maintain a balance of interests between the parties to the relationship when using modern digital tools, such as smart contracts, digital signatures, stamps and other trusted services, as well as when making decisions automatically. It is advisable to enshrine in the Code a mechanism similar to the eIDAS Regulation in the European Union or the UNCITRAL IdM Model Law, which allows using the results of using foreign services as grounds for the emergence, change, and termination of legal relations in the digital environment. Besides, this chapter should define features of the emergence, change, termination of digital rights and rights of the data principal.

The sixth chapter of the Code should establish the order of implementation of the basic legal regimes of access to digital data and their distribution, including in the form of open data. In addition, the basic requirements for access to government digital data are established. At the same time, we note that this chapter excludes the regulation of issues related to state secrets, which are regulated by the Law of the Kyrgyz Republic “On Protection of State Secrets of the Kyrgyz Republic”.

Provisions of this chapter create conditions for the unification, based on the principle of content neutrality, of the legal regulation of different sources of information in the form of “old” (mass media) and “new” (social media, messenger channels, etc.) media; defines independent legal regimes for publicly available data and for the system of secrets; structures and systematizes regimes of access to information.

The chapter introduces the concept of digital sustainability and defines measures and levels of implementation. The goal of digital resilience measures is to effectively allocate the resources of relationship subjects in the digital environment, enabling them to overcome the negative consequences of incidents resulting in incomplete, unreliable, irrelevant digital records, inaccessibility or disruption of digital services or digital technology systems. Digital sustainability is a priority for digital governance, including the practical impossibility of complete protection against incidents in the digital environment. This chapter should also define the rules for protection of the rights of subjects of relations in the digital environment, including dispute resolution and liability.

The next three chapters of the Special Part (devoted to personal data; big data, including its use by artificial intelligence and robotics technologies; spatial data) form the section “Regulation of digital data processing”.

The seventh chapter of the Code, devoted to personal data, should be a revision of the Law of the Kyrgyz Republic “On Personal Information” in the course of codification. In preparing this chapter, special attention should be paid to international best practices, which are the General Data Protection Regulation (GDPR), the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, together with the protocol of amendments dated 10 October 2018, Organization for Economic Co-operation and Development (OECD) guidance on protecting privacy and cross-border flows of personal data.

In accordance with provisions of these documents, the Code should be updated, and the norms expanded to enshrine:

- principles and grounds for processing personal data;
- categories of personal data;
- rights of the subject of personal data and corresponding obligations of the operator;
- features of personal data processing in certain areas, in particular in automatic decision-making;
- procedure for cross-border transfer of personal data in a digital environment;
- features of control and supervision of personal data processing;
- status of an independent regulator in the field of personal data.

As part of the codification, the requirements for the form of consent to processing of personal data, which reduce transaction costs in the context of digital interaction, should be revised; the number of grounds for the processing of personal data has been expanded in the law; the rights to receive information about unauthorized access of third parties to personal data are secured; mechanisms for restoring the violated rights of subjects and restoring the harm caused to them by illegal actions are fixed; established consistent regulation of cross-border data transmission.

The eighth chapter of the Code should establish regulation of the circulation of data and artificial intelligence systems based on the approaches listed below.

In relation to data (including for the purposes of developing big data technologies):

- Openness of government digital data - projected and default. Exceptions may only be provided by law, and only when they are proportionate and necessary for defense, national security, justice, law enforcement, health or morals, the reputation or rights of others, or the prevention of disclosure of confidential information;

- non-discrimination in providing access to public digital resources. At the same time, small and medium-sized businesses should be given more favorable conditions;

- taking measures necessary and sufficient for the protection of state digital data intended for re-use, taking into account the new goals of processing. The possibility for the data owner to condition its provision, inter alia, on its anonymization, pseudonymization and/or working with it exclusively in a secure processing environment;

- prohibition on establishing data localization requirements. Exceptions may be provided only by law and only when they are proportionate and necessary to ensure defense, national security, justice, or the maintenance of law and order;

- inadmissibility of abuse by data owners and data processing service providers of their dominant position in any market, including through the imposition of unfair contractual terms on counterparties or through the use of technical means;

- encouraging self-regulation that promotes data portability. A general rule on the right of any business entities to portability of any kind of data is not proposed at this stage. At the same time, the industry is being encouraged to adopt codes of conduct that encourage service providers to (1) improve the interoperability of their data processing systems and (2) allow their users, including professional users, to seamlessly transfer data to another service provider's systems.

Regarding artificial intelligence systems:

- A ban on the establishment of mandatory requirements for activities related to the development and use of non-hazardous AI systems. The use of AI in any activity or product may not be the basis for imposing mandatory requirements on such activity or product, unless such use increases the risk of harm to someone's rights or legally protected interests;

- Introduction of a safety and risk management system for activities related to the development and application of high-risk AI systems based on the promotion of self-regulation and the introduction of a small number of directly applicable rules referring to internationally recognized industry practices and standards to be applied, unless otherwise subsequently provided for by law or by-law;

- mandatory preliminary assessment of the impact of AI systems and their application on the safety and rights of citizens, the environment, and public and national security and the adoption of necessary and proportionate organizational and technical risk management measures;

- mandatory requirements for the safety, reliability, transparency and explainability of such systems and the activities, in which such systems are applied, including projected compliance with the law;

- mandatory requirements to ensure real human control over the use of such systems, including:

1) establishing accountability (the obligation to record the work of high-risk AI systems), appointing personally disciplinary responsibility for significant adverse consequences of their work,

(2) Anticipating and monitoring the long-term effects of their use on public and state security, as well as on human rights, democracy, and the rule of law.

- mandatory data handling requirements for the design and use of such systems, including requirements for the quality of training, validation, and control samples, including to avoid unlawful discrimination of citizens, against whom such systems may be used;

- obligation to confirm the compliance of such systems and related processes with mandatory requirements in one of the following ways, selected depending on the results of the preliminary safety impact assessment of the system:

1) adoption and publication of the declaration,

2) joining the code of ethics of an industry self-regulatory association, which ensures periodic audit of its members' compliance with the requirements of its code,

3) certification of quality management systems of supplier and operator of AI system by a national, foreign or private body with international recognized reputation (TÜV SÜD, etc.) for compliance with international (for example, ISO 9001) or regional standard.

- no need for a separate experimental legal regime for AI (AI sandbox), provided that the low-intensity approach to regulation described above is maintained.

- introduction of a mandatory requirement to disclose information regarding the use of AI systems, the results of whose activities are intended for human perception and may entail legal or other significant consequences for him or another person.

The ninth chapter of the Code should be devoted to the processing of spatial data as the most important type of data needed to develop the digital economy. The Code should provide a legal basis for the functioning of the national spatial data infrastructure and the spatial data portal; establish rules for access to spatial data and spatial metadata. It is planned to use legislation of the Republic of Korea as a best practice in developing relevant provisions of the Code.

Provisions of the Code, as well as the by-laws adopted in accordance with the Code, should be primarily aimed at:

- revision of the conceptual apparatus of the current regulatory legal acts in the field of geodetic and cartographic activities;
- implementation of principles for the creation and development of a national spatial data infrastructure, such as openness and reuse of digital spatial data;
- determination of the organizational structure of the national spatial data infrastructure;
- establishment and consolidation of powers and responsibilities of the process participants in the creation and functioning of the national spatial data infrastructure;
- approval in a prescribed manner of the regulations for interaction (including interdepartmental interaction) and formats for the exchange of spatial data between developers, copyright holders and users of the national infrastructure of spatial data;
- approval of standards for the creation and use of national spatial data infrastructure in accordance with established procedure;
- establishing and enforcing digital rights in the creation and use of national spatial data infrastructure data;
- addressing the protection of national spatial data infrastructure;
- establishment of liability for violation of legislation in the sphere of national spatial data infrastructure.

The next section of the Code is devoted to digital services and includes three chapters: on general issues of regulation of digital services, features of digital state and municipal services, and features of digital health services.

The tenth chapter of the Code should enshrine general provisions for the regulation of digital services in cyberspace, including the principles of creation and use of digital services, the definition of rules for the regulation of digital services. The benchmark for legislation in this area is the Digital Services Act, which is in the final stages of development in the EU and which should be the core of the electronic commerce legislation. Lawmakers' efforts in this area reflect the increasing integration of a large number of digital services within a single digital ecosystem, threatening discriminatory practices by digital ecosystem owners and service providers.

The provisions of the Digital Services Code are intended to set a clear and enforceable standard for regulation in this area, including the following elements:

- security of the digital environment for users;

- healthy competition between digital services within digital ecosystems;

- transparency of the conditions of consumer access to the digital ecosystem services, not allowing the arbitrariness of the ecosystem owner;

- freedom of users transition and data transfer between digital services and ecosystems; service

- freedom for users to dispose of their data processed as part of the digital service and digital ecosystem;

- preventing the imposition of services by ecosystems and creation of discriminatory conditions;

- prevention of restriction of consumer choice;

- guarantee of openness of data on services.

The eleventh chapter of the Code should fix the features of regulation of state and municipal digital services, designed to ensure the process of digital transformation of public administration. The chapter should consolidate the principles of providing state and municipal services in digital form, such as proactivity and priority of the digital form of interaction, and create conditions for coordination in the digital transformation of public administration (between the bodies responsible for digital transformation, economic development bodies, bodies providing public administration).

The rules for the creation and use of state and municipal services enshrined in this chapter of the Code should reflect the model of digital government architecture developed in the preparation of chapters of the Code on Digital Government Infrastructure and related bylaws.

The twelfth chapter of the Code should fix the specifics of the regulation of digital health and wellness services. As best practice, when developing this chapter of the Code, the principles of the digital transformation of public health of the WHO Regional Office – The Pan American Health Organization can be taken as a basis, which includes the following:

- principle of the unity of the electronic health system;
- principle of interoperability (compatibility) of digital medical systems;
- principles of inclusion and free access to e-health;
- principles of personal data security;
- principle of continuous improvement of the e-health system architecture.

In addition, this chapter of the Code should lay the foundation for digital health sustainability in the Kyrgyz Republic, which requires creating conditions for the effective application of other institutions laid out in the Code (such as trusted services and personal data protection) in the field of digital health and well-being, taking into account the specifics of this sphere.

This chapter of the Code should lay the foundation for the legal regime of health digital resources that form the digital medical record. The digital medical record will have to contain a structured volume of general personal, clinical, biometric, social, economic, financial, insurance, and other data about the patient, documenting the medical services rendered. The main goals of introducing a digital medical record are to ensure the consistency, continuity and quality of diagnosis, treatment, as well as timely prevention and other measures to ensure the health of a particular person by documenting and storing relevant medical information and providing it to the patient by authorized healthcare workers in a timely manner.

Since the digital medical record cannot improve the efficiency of health care by itself, along with the introduction of the digital medical record as a basic product, the conditions for digital interaction between laboratories, pharmacies, sanitary and epidemiological services and other specialized health organizations should be created for the sustainable development of e-health. In particular, to ensure access to information in the field of drug circulation and to improve transparency, conditions should be created for the functioning of a digital resource for drugs and medical devices, covering all aspects of drug circulation, from registration to sale and disposal. In this area, it will also be necessary to harmonize the provisions of the Code with the provisions of international treaties of the Kyrgyz Republic.

The following basic requirements should be implemented in establishing the specifics of the application of the Code's artificial intelligence and big data provisions in the field of digital health:

- specific standards and regulations should be created or implemented to encourage the responsible use of artificial intelligence in digital health and wellness;

- introduction of AI technologies should be accompanied by scientific, practical and educational activities aimed, among other things, at debunking myths and demonstrating the practical application of AI in health care;

- it is necessary to ensure an inclusive approach to artificial intelligence in health care that involves health professionals, patients, and the public, transparency about initiatives and case studies.

The next section of the Code deals with the legal regulation of trusted services and includes chapters on identity services and systems, digital signature services, and digital documents. Together, the institutions laid down in the relevant chapters of the Code should ensure trust among participants in the digital environment and in the digital data they use.

The thirteenth chapter of the Code is devoted to digital identification and is intended to codify the scattered acts currently in force in the Kyrgyz Republic, including the law “On Electronic Signature” with regard to the use of a simple electronic signature. Digital identification, which allows for the interaction of stakeholders (state, business, individual) remotely, is one of the trends in the development of digitalization, while regulation in the field of digital identification involves creation of the necessary conditions for its application, including by increasing the flexibility in regulation, improving tools for protecting user rights, as well as establishing requirements for ensuring digital sustainability, primarily in terms of data protection and ensuring the uninterrupted operation of services and identification systems. New identification tools and technologies, such as biometric identification, identification by cell phone number, using digital cards or codes require a legal framework for their responsible and secure use.

The United Nations General Principles for Identification develop the capacity of identification systems to support development and the achievement of the UN Sustainable Development Goals, so they should be used in the development of this chapter of the Code. Robust identity systems can empower subjects and their access to digital data and digital services. They can also build the capacity of government agencies and the private sector.

The principles for regulating identification systems and services should be enshrined in the Code as follows.

The first group consists of principles related to inclusion and universal coverage and accessibility. Accordingly, the identification systems should strive for continuous universal coverage from birth to death, be non-discriminatory and accessible to all people. This group includes two subgroups of principles. The first subgroup includes the principles of universality (as an obligation of the state to provide legally valid identification to all residents from birth to death) and non-discrimination (as a requirement for the state to identify and mitigate legal, procedural and social barriers to the use of identification systems, with special attention to poor people and groups that may be at risk of exclusion for cultural, political or

other reasons). In addition, identification systems and identities should not be used as a tool for discrimination or infringement of rights. The second subgroup addresses barriers to access and use, as well as disparities in the availability of data and technology. The principles of accessibility (according to which cost should not be a barrier to access to identification services), reasonableness and proportionality (which requires considering the indirect costs associated with access to identification services - for example, cumbersome administrative procedures) are important here. The reduction of information asymmetries that can prevent individuals from accessing identity-related services or benefits is also important here. In particular, no one should be denied in receiving the identification or related services because they lack Internet connectivity or technical knowledge. Stakeholders should work together to ensure that both online and offline infrastructure can be expanded to provide access and connectivity, especially for those living in rural areas.

The second group of principles refers to the technical construction (design) of identification systems. Identification systems must be robust, context-sensitive, and interoperable. Responding to users and their long-term needs, they should only collect and use information that is necessary for the explicit purpose of the system. Open standards and supplier neutrality help ensure financial and operational efficiency and sustainability.

The third group of principles relates to governance: building trust by protecting the confidentiality of information and protecting the rights of users. Identification systems should be built on a legal and organizational basis of trust and accountability between government agencies, international organizations, private sector subjects, and individuals. Subjects should have confidence in the privacy and protection of their data, the ability to control and supervise their use, and guarantees of independent oversight and complaint resolution.

The use of identification systems in the Kyrgyz Republic should be independently monitored (for efficiency, transparency, non-discrimination, proper use, etc.) to ensure that all stakeholders properly use identification systems to achieve their goals, monitor and respond to potential violations in the field of use data, as well as received individual complaints regarding the processing of personal data. Disputes relating to the identification and use of personal data that have not been satisfyingly resolved by providers (for example, refusal to register a person or correct data, adverse determination of the legal status of a person) should be subject to rapid and inexpensive administrative or judicial review.

The fourteenth chapter of the Code is devoted to digital signatures and is intended to update the provisions enshrined in the Law of the Kyrgyz Republic "On Electronic Signature. The change of name from “electronic” to “digital” signatures reflects the separation of the regulation of digital (cryptographic) signatures proper and simple electronic signature, which within the framework of the Code is considered as an identifier.

Although the current Law “On Electronic Signature” is generally consistent with internationally accepted approaches to regulation, it has two significant drawbacks that hinder its widespread use. The first is a violation of the principle of technological neutrality in the implementation of the law, which limits competition in the market, and naturally leads to the second disadvantage, namely the practical impossibility of cross-border recognition of digital signatures due to the incompatibility of technologies used in the Kyrgyz Republic and abroad. In course of codification, these shortcomings should be eliminated, while taking into account the EU Electronic Identification and Authentication Services Regulation - eIDAS) dated 23 July 2014 and the UNCITRAL Model Law dated 23 July 2014 and the UNCITRAL on the use and cross-border recognition of identity management and trust services (IdM) as best practices.

In order to address these shortcomings of the current law and to create conditions for the widespread use of digital signatures, including in cross-border relations, the Code should establish mechanisms for harmonizing national regulation in this area with the approaches existing in other states. In addition to

developing already existing approaches to the recognition of foreign digital signatures, focus should be made on recognition in the Kyrgyz Republic of foreign and international standards in this area. In addition to providing an equivalent level of reliability, reliance on international standards will also create the conditions for the accelerated introduction of new digital signature technologies, such as cloud-based signatures, as well as a paradigm shift in signature formation - not with respect to documents, but with respect to digital records (with the formation of a digital document).

The fifteenth chapter of the Code should consolidate the rules and procedures necessary in the digital economy to ensure the trusted storage, use and other types of processing of digital records. In addition, it should reflect the necessary elements of backward compatibility to enable the transition from information systems and electronic document management to digital management based on digital data. This demands consolidation of requirements for trusted digital archive services and guaranteed message delivery. In addition, the Code provisions should encourage the transition to an exclusively digital interaction in all areas of digital governance, which in turn requires addressing issues with the formation, presentation and examination of digital evidence, ensuring the legal significance of digital copies of documents on paper, the conversion of digital documents.

The current trend towards digital interaction shows that services using the message “delivery” model are becoming less and less demanded, being organically replaced by cloud services. This is facilitated by the so-called “network effect,” which reduces the number of transactions between users when they move to a cloud-based interaction model. As a consequence, the idea of an "electronic message," that is, something that has been sent and delivered, is replaced by the idea of a “record,” that is, something that has been created and can be accessed for some time after creation. In such a system of coordinates, there is almost no room for electronic documents: electronic document flow turns into cloud storage, similar to how ICQ turned into Telegram. An electronic document is intended to exist autonomously, which usually requires attestation by an electronic signature. The cloud storage is a system of records which safety is ensured by means of the technological system, and the ability to use these records is determined by access levels, i.e. by the information system settings.

Despite the large number of different cloud services, both domestic and foreign, none of them solves the problem that is now the delivery of official messages, primarily postal. Data from a cloud service is difficult, almost impossible to use for the emergence, change, termination of legal relations, while any registered mail or even a paper bill can easily be used for this purpose. Existing solutions for legalizing data from the cloud are inconvenient and expensive crutches, such as electronic notarial acts or the services of electronic document management operators.

The purpose of the Code in this regard is to stimulate the emergence and use of document storage services, which organically, by design will create the possibility of using these documents for the emergence, modification, termination of legal relations. In fact, the only task to be solved in this regard is the recognition of documents from such a cloud storage facility as written evidence in courts (as well as in the activities of supervisory authorities).

Although the procedural codes already include written evidence of contracts, acts, certificates, business correspondence, and other documents made in digital, graphic or other form that allows to establish the reliability of the document, in practice, however, the court does not examine evidence in digital form: the parties can attach them on a digital medium, but the judges examine their respective paper printouts, and what cannot be printed, they send for examination. Similar practice existed in foreign countries, so in many of them there was a political decision to mostly electronic form of evidence and proof in the courts. In the United States, the Case Management / Electronic Case Files (CM/ ECF) filing system has been very successful, and in 2005, it was implemented in all federal courts in the country. Since that time, the obligation of the parties to file electronically via CM/ECF has also been established, while paper filing is made an exception in case of special need based on a special motion “for failure to comply with the

obligation to file electronically." It is important to note that this system is not an electronic document management system: it provides access to court documents online based on a centralized shared system. A similar approach applies in the United Kingdom, where only minor administrative offenses and criminal acts of low public danger punishable by imprisonment are considered online, as well as civil disputes with a claim value of up to 25 thousand pounds. This is provided by the Courts Electronic Filing system (CE-File), the CaseLines online portal for filing claims and evidence electronically, and Her Majesty's Online Court (HMOC).

This organization of case consideration and, above all, evidence handling, required an innovative approach to electronic archives that fundamentally rethinks archival practice, beginning with foundational principles. Such an archive should ensure the long-term preservation of electronic documents of all kinds, not just those created in several widely used formats. This ideology was enshrined in the strategic plan "Archives Inspire: Plans and Priorities for the UK National Archives 2015-2019," which relies on a document continuum model that treats documents as archival from their inception. The National Archives of Great Britain is an active participant in the discussion of new information systems, so that the problems of preservation of electronic documents begin to be thought about as early as possible. In Estonia, the problem of long-term document storage is beginning to be addressed at the departmental or organizational level. For this purpose, a special software Universal Archiving Module (UAM) was created, available on the website of the National Archive of Estonia, which is designed for the archivists of the organization and allows exporting data to the archive. The main functions of UAM meet all technical and archival requirements for the successful development of documents and their metadata for transfer from the organization to the state archive. UAM has been used in practice since 2010 to transfer documents to a digital archive. The National Archives is in constant contact with all ministries and helps them to complete the transfer (import) of documents through UAM. Thus, thanks to this software module, a single universal tool for transferring electronic documents from the field of operational management to the state archive was implemented.

The foreign practices described above provide guidance for provisions of the Digital Document Code. The trusted services created on the basis of digital documents should become a necessary intermediate link between organizations that create documents and digital records in their activities, the archival department, and government agencies that need access to documents in connection with the implementation of their functions, primarily for dispute resolution and state control (supervision).

The next section of the Code is devoted to digital technological systems, including issues of public-private partnership in this area and issues of placement of digital infrastructure facilities on lands, buildings, buildings and structures.

The sixteenth chapter of the Code establishes the legal regime for digital technology systems used for digital control. Since the legal regime of telecommunications networks is the subject of regulation by other chapters of the Code, this chapter should primarily address the operation of data centers, including those used to provide state and municipal digital services. The following principles are to be implemented in this chapter of the Code:

- non-discriminatory access to digital technology systems;
- independence of users from vendors, developers, and operating organizations;
- public certainty in the use of digital technology systems;
- interoperability of digital technology systems;
- stability and continuity of the characteristics of digital technological systems;
- market competition when using digital technology systems;
- reuse of digital technology systems;
- digital data security and the availability of digital services hosted within digital technology systems.

This chapter of the Digital Code should contain mechanisms to ensure that the Code's provisions are harmonized with relevant regulations governing the creation and use of digital technology systems, such as data centers, in various areas of the digital economy and public administration. To this end, the Code should establish the authority to establish requirements for certain types of digital technology systems or the procedure for establishing such requirements.

A separate issue requiring consolidation within the Code is the problem of access by the digital technology systems owners to land, structures, buildings and facilities in order to locate and operate elements of digital technology systems. This issue should be addressed by the Code separately for the two main types of digital technology systems - telecommunications networks and data centers. Priority should be given to contractual grounds for access, with establishment of the necessary mechanisms for determining fair contract terms and disputes resolution, including those relating to the enforcement of such contracts.

The seventeenth chapter of the Code should enshrine the features of public-private partnerships in the digital environment. These features result from the specifics of the objects of relations in the digital environment (primarily due to the fact that they are objects of digital rights, rather than property rights), specifics of the procedure for establishing public-private partnership relations, the order of use and monetization of public-private partnership objects in the digital environment.

Due to specific features of the life cycle of legal relations in the digital environment, the mechanism of public-private partnership here should fully comply with the principles of legal certainty, transparency and accountability. The mechanisms enshrined in the Code should stimulate full-fledged investment in research and development work on the subject of partnership, as well as technical support and continuous modernization of the object of public-private partnership. The full and effective use of facilities created in the course of public-private partnerships is possible only if all of these conditions are met.

The next section of the Code deals with telecommunications and includes chapters on the government telecommunications policy, telecommunications facilities, telecommunications providers and operators, and other telecommunications regulatory issues. This section should reflect the changes in telecommunications technologies that have occurred since adoption of the current legislation in this area, as well as the best regulatory practices in the field of telecommunications, involving a significant reduction in bureaucratic procedures and the transition from formal control to monitoring the observance of the rights and legitimate interests of users telecommunication services by the advanced monitoring systems.

The eighteenth chapter of the Code, “The State Telecommunications Policy,” should enshrine the industry regulatory framework. In particular, the Code should explicitly state the policy goals such as:

- creation of favorable competitive conditions for the provision of quality telecommunications services throughout the country;

- promoting the introduction and use of advanced telecommunications technologies;

- protection of the interests of telecommunications users and organizations engaged in telecommunications activities, and other public and state interests in the implementation of telecommunications activities.

- development of the national telecommunications infrastructure, its integration with international telecommunications networks, as well as the effective use of telecommunications resources and meeting the telecommunications needs of government agencies and law enforcement.

Among the foundations of the state communications policy it is necessary to identify and disclose measures to comply with constitutional principles in the field of telecommunications, as well as mechanisms for the implementation of constitutional rights such as right to information. This chapter should also enshrine the types of state regulation in the field of telecommunications, powers of the

telecommunications regulator, and address the relations of regulatory and other acts regulating telecommunications activities in the Kyrgyz Republic. It should be expressly stipulated that the Code regulates the telecommunications activities, taking into account their cross-border nature, based on decisions of international organizations, to which the Kyrgyz Republic is a party, and taking into account the provisions of internationally applicable standards and recommendations, including those adopted at the international level. Such standards and recommendations shall be applied taking into account the Code principles for regulating relations in the digital environment, and the provisions contradicting this Code shall not be applied.

The nineteenth chapter of the Code enshrines the legal regime of telecommunications facilities, which include:

- telecommunications networks as a type of digital technological systems, their elements representing technological and other equipment designed for telecommunications activities, as well as individual communication means;

- telecommunications services;

- land, buildings, structures in terms of access to them by owners of telecommunications networks;

- telecommunications resources (radio frequency resource, numbering and addressing resources) in terms of access to them by telecommunications operators.

This chapter shall define the rules for the operation of telecommunications facilities, as well as the rules for the allocation of telecommunications resources. Taking into account the practice of application of the current legislation, the Code should minimize the number of by-laws regulating these issues, which will also reduce the number of excessive administrative barriers established in relation to telecommunications market participants. The status of the State Commission on Radio Frequencies should also be secured.

The same chapter should establish mechanisms for the protection of telecommunications networks and mechanisms for non-discriminatory access to land, buildings, structures, and constructions in terms of access to them by owners of telecommunications networks. In order to encourage responsible behavior by owners of telecommunications networks and to implement the principle of legal certainty, priority in the use of such facilities should be given to telecommunications operators, that is, persons who have obtained the appropriate license.

The twentieth chapter of the Code should fix the status of telecommunications operators and telecommunications service providers who do not have the status of an operator, and define the rules for inter-operator interaction. Such a distinction of status is necessary to equalize the legal regulation of telecommunications operators in the traditional sense (telephone operators, Internet access operators) and providers of communication services (such as messengers or audiovisual services), which provide users with the same opportunities, but do not bear the burden imposed by law on licensed operators. The Code should define common responsibilities for all providers of telecommunications services, with the license acting as a right rather than an additional burden for those organizations that are interested in developing and operating their own telecommunications infrastructure.

This chapter of the Code should provide that licensing of telecommunications activities is carried out in order to regulate the use by telecommunications providers of the radio frequency spectrum, the numbering resource, their broadcasting activities, telecommunications activities in the border zone (including the use of telecommunications infrastructure when crossing the border of the Kyrgyz Republic), and to provide them with priority access to lands, buildings, structures, structures for the placement of elements of telecommunication networks. The Code should comprehensively fix all the main elements of the procedure for licensing telecommunications activities, in particular, define licensing requirements.

This chapter should also define the rules of inter-operator (inter-network) cooperation (including settlements), establish the specifics of telecommunications activities in the field of broadcasting, and establish the procedure for cross-border cooperation and settlements in the field of telecommunications.

The twenty-first chapter of the Code deals with the provision of telecommunications services. It should stipulate the types and procedure for delivery of telecommunications services, including the provision of telecommunications services in special conditions and in specific cases, define mechanisms for protecting the rights of telecommunications services users and the legal regime of digital records of users and the services provided to them. Provisions of this chapter should be of a framework nature and not provide for bylaws. Given the variety of technologies, on the basis of which telecommunications services are provided and their rapid development, the establishment of detailed procedures and rules for each type of service by normative legal acts makes no sense. In this regard, the rules of telecommunications services should be defined by their providers together with users, and the Code should establish basic requirements for such rules and mechanisms to protect the rights of users when these requirements are violated.

The twenty-second chapter of the Code should contain other provisions on the regulation of telecommunications activities, in particular, fix the powers of other state bodies (except for the telecommunications regulator) in relation to participants in telecommunications activities, establish rules for international cooperation in the field of telecommunications, rules for state control and supervision in the field of telecommunications.

Implementation of the Concept

This Concept shall be implemented in accordance with the Roadmap for drafting normative acts to create favorable conditions for the digital economy and involves, in addition to the development and adoption of the draft Digital Code of the Kyrgyz Republic, also amendments to other legislative acts of the Kyrgyz Republic and the adoption of regulations in cases stipulated by the Code. The list of normative legal acts necessary for implementation of the Code is given below.

Law on regulatory sandboxes	The procedure for creating the regulatory sandboxes for innovation in the Kyrgyz Republic was defined
Related amendments to the CC	Concepts such as digital transactions and smart contracts, digital/virtual assets, securing rights to digital/virtual assets, electronic payments are defined
Related changes to the Payment System Act/ or the Virtual Assets Act (adopted on 21 January 2022)	The legal regime of such objects is established and the main approaches such as digital currency, basic digital income, mobile banking services and providing access to the market of mobile operators; payments using smartphones and QR codes, market entry for operators of international payment systems are enshrined;
Regulation on the government cloud platform G-Cloud; (NLA at the level of the KR Cabinet of Ministers)	Regulation of cloud technology interaction with providers, service delivery, processes related to data processing, identification and authentication of access subjects and objects, restriction of the software environment, recording of security events, protection of the virtualization environment, protection of technical means, enabling efficient and secure use of cloud resources (e.g. networks, storage, applications and services), reducing costs associated with the creation and use of IT infrastructure, etc.

Technical requirements for data centers (NLA at the level of the KR Cabinet of Ministers)	National regulatory and technical approaches to telecom infrastructure of data centers were defined, harmonization with international standards for the levels of reliability of data center engineering infrastructure was carried out
Regulation (rules) on technical standards for fiber optic broadband infrastructure (NLA at the level of the KR Cabinet of Ministers)	Defined requirements for cross-border local and nationwide networks, 5G readiness, ultra-reliable low-latency communications, and multi-device connectivity (mMTC)
Regulations on the authorized body for communications/telecommunications (NLA at the level of the KR Cabinet of Ministers)	The status and powers of the (independent) national regulator of the communications industry have been enshrined
Amendments to tax legislation	Specific features of taxation of telecommunication services, e-commerce, digital platforms are defined

Appendix

List of normative legal acts to be repealed or amended in the course of codification