

ANALYSIS OF GAPS AND CONFLICTS  
in the Kyrgyz Republic Regulatory Framework  
with an Overview of the Global and Regional Best  
Practices  
(Output 2)

MAY 2022

BISHKEK CITY, KYRGYZ REPUBLIC

CONTRACT NO. CS-QCBS-3-1-1

## Table of Content

INTRODUCTION.....	6
About this document .....	6
Context for the analysis.....	7
Domestic context.....	7
International context.....	7
Legal basis and principles of building the enabling regulatory environment for a developed, competitive digital economy in the Kyrgyz Republic .....	10
Analysis methodology.....	12
Key findings, by the analysis areas .....	13
References .....	20
Section 1. Legal basis for digital governance .....	21
Content.....	21
Current regulation (existing legislation): .....	21
Brief description of the identified shortcomings and international practice benchmarks ...	22
Comments .....	24
Section 3. Digital governance objects .....	29
Content.....	29
Current regulation (existing legislation): .....	29
Brief description of the identified shortcomings and international practice benchmarks ...	30
Comments .....	34
Content.....	38
Current regulation (existing legislation): .....	39
Brief description of the identified shortcomings and international practice benchmarks ...	41
Comments .....	41
Section 5. Grounds for the emergence, change, and termination of legal relations in the digital environment.....	44
Content.....	44
Current regulation (existing legislation): .....	44
Brief description of the identified shortcomings and international practice benchmarks ...	45
Comments .....	46
Section 6. Information legal relations .....	51
Content.....	51
Current regulation (existing legislation): .....	51
Brief description of the identified shortcomings and international practice benchmarks ...	51
Comments .....	55
Section 7. Personal data .....	61
Content.....	61

Current regulation (existing legislation): .....	61
Brief description of the identified shortcomings and international practice benchmarks ...	61
Comments .....	68
Section 8. Big Data .....	76
Content .....	76
Current regulation (existing legislation): .....	76
Brief description of the identified shortcomings and international practice benchmarks ...	76
Comments .....	79
Section 9. National spatial data infrastructure .....	81
Content .....	81
Current regulation (existing legislation): .....	81
Brief description of the identified shortcomings and international practice benchmarks ....	82
Comments.....	84
Section 10. Electronic message, record and document.....	86
Content .....	86
Current regulation (existing legislation): .....	86
Brief description of the identified shortcomings and international practice benchmarks ....	86
Comments.....	89
Section 11. Digital identification .....	97
Content .....	97
Current regulation (existing legislation): .....	97
Brief description of the identified shortcomings and international practice benchmarks ...	98
Comments.....	100
Section 12. Digital services .....	102
Content .....	102
Current regulation (existing legislation): .....	102
Brief description of the identified shortcomings.....	102
Comments.....	106
Section 13. State and municipal digital services .....	107
Content .....	107
Current regulation: .....	107
Brief description of the identified shortcomings.....	107
Comments.....	109
Section 14. Digital Health and Well-Being .....	110
Content .....	110
Current regulation (existing legislation): .....	110
Brief description of the identified shortcomings and international practice benchmarks ..	111
Comments.....	112

Section 15. Digital governance technological infrastructure .....	115
Content .....	115
Current regulation (existing legislation): .....	115
Brief description of the identified shortcomings and international practice benchmarks ..	115
Section 16. Telecommunications networks and resources .....	119
Current regulation (main regulations of current legislation):.....	119
Brief description of the identified shortcomings and international practice benchmarks ..	119
Comments.....	122
International experience .....	123
Conclusions and recommendations .....	123
Section 17. Inter-operator cooperation, network neutrality .....	125
Current regulation (existing legislation): .....	125
Brief description of the identified shortcomings and international practice benchmarks ..	125
Comments.....	126
International experience .....	127
Conclusions and recommendations .....	127
Section 19. PPP in the context of digital transformation .....	128
Content .....	128
Current regulation (existing legislation): .....	128
Brief description of the identified shortcomings and international practice benchmarks ..	128
Comments.....	132
Based on the reviewed international practice, analyzed legislation and PPP development in the Kyrgyz Republic, the following problems have been identified: .....	132
Thus, as a matter of priority, it is necessary to bring into conformity all laws and regulations governing PPP, as imperfect legal regulation of PPP will prevent full-fledged initiation of the PPP projects by foreign investors. ....	132
In most cases, investors prefer to work in countries where it is sufficient to rely on general legislation rather than sector-specific regulations for project implementation, such as transport or education, because interests of the increasingly more stakeholders are affected by the general legislation and there is less chance that problems would emerge as a result of changing laws.	132
Section 20. Related changes in the CC.....	136
Content .....	136
Current regulation (existing legislation): .....	136
Brief description of the identified shortcomings and international practice benchmarks ..	136
Comments.....	138
Section 23. Related changes in the Law "On Civil Service" .....	143
Current regulation (existing legislation): .....	143
Brief description of the identified shortcomings and international practice benchmarks ..	143
Comments.....	144
Section 24. Cloud technologies.....	148

Content.....	148
<b>Current regulation (existing legislation):</b> .....	148
<b>Brief description of the identified shortcomings and international practice benchmarks..</b>	148
<b>Comments.....</b>	152
Section 25. Technical requirements for data processing centers (DPC).....	153
Content .....	153
<b>Current regulation (existing legislation):</b> .....	153
<b>Brief description of the identified shortcomings and international practice benchmarks..</b>	153
<b>Comments.....</b>	155
Section 30. Cybersecurity .....	158
Content:.....	158
Current regulation (existing legislation) .....	158
Brief description of the identified shortcomings and international practice benchmarks .	158
Comments .....	165
Section 31. Experimental legal regimes (regulatory sandboxes) .....	172
Content.....	172
Current regulation (existing legislation): .....	172
Brief description of the identified shortcomings and international practice benchmarks .	172
Comments .....	173
Section 33. Tax regulation .....	178
Content.....	178
Current regulation (existing legislation): .....	178
Summary of the identified deficiencies and benchmarks from the global practice .....	178
Comments .....	181
Section 34. Customs regulation .....	186
Content.....	186
Brief description of the identified shortcomings and international practice benchmarks .	187
Comments .....	192

## INTRODUCTION

### About this document

The Civil Initiative of Internet Policy (hereinafter - the Consultant) is engaged in the Digital CASA-Kyrgyz Republic project (hereinafter - the Project) providing consulting services to support the development of an enabling environment for the digital economy in the Kyrgyz Republic.

The World Bank-funded Digital CASA-Kyrgyz Republic Project at the Ministry of Digital Development of the Kyrgyz Republic contracted the Consultant to “conduct a detailed review of the effective regulatory framework and draft the necessary regulations to create an enabling environment for the digital economy.”

In March 2022, the Contract No. CS-QCBS-3-1-1 was awarded to the Consultant. This report is submitted in fulfillment of the Consultant's services and represents Deliverable 2 under Phase 1 of the Project.

The Consultant delivers services under the multi-component, multi-year national Digital CASA-Kyrgyz Republic Project, covering the development of regional communications infrastructure, regional data centers, digital platforms and intelligent solutions, and the creation of an enabling environment for the digital economy. The Project development goal at the country level is to expand access to more affordable Internet, attract private investment in the ICT sector, and improve the country's capacity to provide digital public services in the Kyrgyz Republic by promoting the development of a regional integrated digital infrastructure and enabling environment.

The enabling environment component of the Project seeks to strengthen and harmonize laws, regulations, institutional and human resource capacity at the regional and national levels. It is also designed to develop the various partnerships needed to take full advantage of rapidly evolving digital technologies, infrastructure and platforms, improve market competitiveness, foster innovation and create jobs. It will also support digital leadership, skills and capacity development, and strategic communications.

This component includes three subcomponents: 3.1. Legal, regulatory, and institutional framework for the digital economy, 3.2. Regional partnerships for skills, jobs, and innovation in the digital economy, and 3.3. Digital leadership and strategic communications. The Consultant's services are part of sub-component 3.1. Legal, regulatory and institutional frameworks for the digital economy, aimed at supporting the creation of enabling regulatory environment for the digital economy through an in-depth gap analysis of the legislation and regulation.

As a result, the Project should create a framework for the implementation and sustainable development of digital infrastructure, the development of digital platforms and cloud technologies and digital services, in compliance with the Project goals and indicators, with prioritizing the public-private partnership mechanisms and cybersecurity.

In accordance with the Terms of Reference, the Consultant's services include:

- in-depth description of the legal and regulatory gaps and shortcomings;
- classification of identified issues on the impact on a specific activity (e.g., higher operating costs are an obstacle, lower capitalization, prevention of new services or markets, risk of market instability);
- description of international and regional best practices aimed at addressing the issues raised.

The analysis findings are systematized in this report so that they can be used to develop the Kyrgyz Republic regulatory framework. For these purposes, the analysis materials are arranged according to the structure of the regulatory framework proposed under Deliverable 1.

## Context for the analysis

### Domestic context

Since 2016, the Kyrgyz Republic has been focusing on the introduction of e-governance and country digitalization. In accordance with the Kyrgyz Republic's Constitution stating that the development of society and the state is based on scientific research, modern technology and innovation, the President and Jogorku Kenesh (Parliament) are consistently pursuing a policy of innovative development in the digital economy. In 2017, the E-Governance and Electronic Signature Laws of the Kyrgyz Republic were adopted, amendments were made to the laws of the Kyrgyz Republic "On Personal Information", "On the State and Municipal Services", "On Access to Information Under the Jurisdiction of State Bodies and Local Self-Government Bodies". In 2018, the Kyrgyz Republic Government decided to launch the "Tunduk" system, which is one of the key elements of e-governance. In this regard, a number of bylaws were adopted to implement the "Tunduk" system, and its operator was identified.

The tasks of the country digitalization and accelerated development based on digital technology are set out in a number of strategic documents:

- The National Development Strategy of the Kyrgyz Republic for 2018-2040 and "Taza Koom"<sup>1</sup> as the National Digital Transformation Program;
- The Digital Transformation Concept "Digital Kyrgyzstan" - 2019-2023;
- The main activities of the Kyrgyz Republic Government;
- Development Program of the Kyrgyz Republic for the period 2018-2022 "Unity. Trust. Creation"<sup>2</sup> (approved by Resolution of Jogorku Kenesh of the Kyrgyz Republic, dated 20 April 2018, No. 2377-VI);
- The Kyrgyz Republic National Development Program to 2026<sup>3</sup>.

However, in the med-term, the digitalization process was affected by a number of objective trends caused by both the two-year COVID-19 epidemic and the political upheavals in the Kyrgyz Republic of the second half of 2020. The initial surge in the digital technology use associated with the large scale transition of government agencies to remote operation has slowed down in the second half of the year, and then stopped completely. Coming back to the offline operation, the state agencies returned to paper-based document flow, as a matter of habit, but also due to the lower levels of traceability and accountability.

In such context, the instability of digitalization processes is noted in the Kyrgyz Republic, caused by both objective and subjective factors.

### International context

There is a long-standing international effort to develop regulatory approaches that can increase the sustainability of the development processes based on digital technologies. The results of this effort are reflected in a number of reports and reviews of international organizations and expert platforms,

---

<sup>1</sup> "Taza Koom" has never been approved as the National Digital Transformation Program (although there were several discussions of, versions of the program itself). In 2019, the Kyrgyz Republic Security Council approved the Digital Transformation Concept "Digital Kyrgyzstan" - 2019-2023 (instead of "Taza Koom")

<sup>2</sup> There are no public reports in open sources on the results of this program implementation.

<sup>3</sup> It is indicated that this Program was developed as part of the National Development Strategy of the Kyrgyz Republic to 2040, while maintaining continuity based on the country's long-term person-centered strategic development goals with a focus on the fundamental obligation to "Leave no one behind" of the Sustainable Development Goals. There are no publicly available reports on the implementation of this program

many of which use the rating system, that is, comparative analysis of different countries using various numerical metrics (coefficients).

The International Telecommunication Union studies show that even small improvements in the regulatory environment result in measurable progress and improvement under a number of economic indicators. The summarized data for 145 countries for the period of 2008-2019 show that optimizing and modernizing the regulatory environment increases investment in the fixed and mobile infrastructure. For example, a 10% improvement in the ICT Regulatory Tracker index (discussed in more detail below) leads on average to a 7% increase in investments, while halving the bureaucratic costs increases investment by 17%. Certain regulatory measures, such as mobile number portability, lead to meaningful improvements in coverage, penetration, and affordability for mobile users (ITU, 2021b).

Almost all periodically updated indices that aim at composite measurements of digital development tend to include components that measure various parameters of the digital development regulatory framework. The general indices that have a separate regulatory component include the Network Readiness Index, the ICT Regulatory Tracker and G5 Benchmark indices of the International Telecommunication Union, and the OECD Going Digital index.

**Network Readiness Index** measures readiness of the digital regulatory environment in five areas - general ICT regulatory environment, adaptability of the legal framework to the advanced technologies, e-commerce and confidential data protection legislation. For this index component, the latest assessment for 2021 ranked the Kyrgyz Republic only 110th out of 130 world economies included in the index, with the lowest score given to the adaptability of the legal framework to the advanced technologies (Portulans Institute, 2021).

As technologies advance, indices are emerging that cover exclusively the digital space regulation. The **ICT Regulatory Tracker** of the International Telecommunication Union (ITU, 2020) is the starting point for many of them, and a building block of many numerical indices and country assessments. It is a comparative tool to help determine the status of regulation across four regulatory environment clusters - regulatory authority, mandate, regulatory regime, and ICT competition protection. Including more than 50 indicators, the index states the presence or absence of certain regulation elements and does not aim to assess the quality of regulation.<sup>4</sup> The country assessment of the Kyrgyz Republic for 2020 (77.5 points out of 100 possible) shows regulatory gaps in such elements as requirements for operators to publish the information required to connect to networks, the cost of connection services, the availability of number portability for fixed and mobile communication users, the possibility of using VoIP by individuals.

In 2021, the International Telecommunications Union prepared a pilot **G5 Benchmark** index of 70 regulatory and rulemaking indicators (ITU, 2021a). The index is arranged around five levels and generations of digital technologies regulation (G1-G2-G3-G4-G5), with the ultimate goal of G5 representing the latest and most advanced generation of regulatory approaches and practices. The assessment methodology has four components with all of them having a regulatory basis. The very first country assessment of the Kyrgyz Republic for 2021 (45 points out of possible one hundred points) revealed the following gaps based on the G5 methodology:

**1) national collaborative governance, or the level of collaboration among regulators and other government institutions.** For this component, it is noted that Kyrgyzstan has no mechanisms for cooperation with the national CERT, an independent data protection authority, ministries or energy and environmental regulatory agencies (e-waste).

---

<sup>4</sup> The supporting document to the Tracker in practical regulatory terms is the International Telecommunication Union's Digital Regulation Handbook (ITU and The World Bank, 2020). The handbook provides a detailed overview of the following key topics: regulatory governance and regulatory independence, competition, access, consumer interests, data protection, trust, spectrum management, emerging technologies, technical regulation, and emergency communications.

2) **policy design principles** - stakeholder participation, involvement, transparency of decisions and processes. In case of Kyrgyzstan, there is no legal opportunity for affected parties to request a revision or appeal of the adopted rules to the relevant administrative body (across all sectors). The principle of technological neutrality of regulation is applied selectively in the country.

3) **digital development toolkit** - availability of national digital development strategies with sectoral requirements and alignment with the Sustainable Development Goals. Here, the country assessment of Kyrgyzstan revealed gaps in multiple areas.

- For certain thematic priorities, there is lack of legal acts regulating online child protection, smart city concepts, signed or ratified agreements on cybersecurity (Budapest Convention on Cybersecurity), regulation of cross-border data flows in relation to confidentiality, and on emergency communications (Tampere Convention).

- For the infrastructure component, there is no official registry or map of the whole telecommunications/ICT infrastructure; no procedures for cross-sector infrastructure sharing or rules, agreements, initiatives to promote joint fiber-optic network deployment.

- Besides, broadband is not seen as part of a unified access service, and the broadband action plans do not include specific measures to provide broadband services for the needs of socially disadvantaged individuals.

- The digital strategy is not focused on sustainable development goals, no documents have been identified to support the transition to sustainable consumption and production, no e-waste regulations have been developed and implemented, no global youth employment strategy has been developed and implemented, and the International Labor Organization Global Jobs Pact is not implemented.

4) **digital economy agenda** - availability of strategic documents on harmonization, innovation, digital transformation based on the breakthrough technologies, taxation and codes of conduct for market participants. The country assessment notes the lack of holistic policies on ICT/digital innovation, regulation of digital markets, artificial intelligence, special tax regimes for the telecommunications and digital sector or Internet services, and voluntary or mandatory codes of conduct.

The OECD **Going Digital** Index (OECD, 2020a) covers seven interrelated areas of regulation - 1) Access; 2) Efficient Use; 3) Innovation; 4) Employment; 5) Social Well-Being; 6) Trust; and 7) Market Openness. Each area consists of key priorities that represent the final regulation goals - for example, infrastructure investment, digital security, and market competitiveness.

The index developers assume that the sectoral division of legal acts for the purposes of regulating digital transformation has become less relevant, as each area affects the others, and may contain cross-cutting priorities - for example, digital skills, digital governance, and data. That is why it is necessary to consider all areas of the digital economy regulation in a unified and holistic way. The focus should be made on coordination and collaboration among all actors.

The key OECD scoping publication, **Vectors for Digital Transformation** (OECD, 2020b), highlights the rapidness, interconnectivity and complexity of the digital development processes, which makes standard regulatory approaches unacceptable. The specific features of technologies, business models, behavior of companies and consumers impose serious limitations on the traditional regulatory thinking. For example, digital scaling capabilities allow companies and platforms to grow globally with few employees, capital and physical presence - which may mean that such legal application criteria as size of capital or number of employees need to be revised. The complex structure and complexity of digital products encourage a shift toward convergent regulatory approaches that combine cross-industry authority and regulation functions. Digital business models can also function without reference to jurisdiction, reducing dependence on the principles of territoriality and sovereignty and forcing governments to strengthen regional, global and thematic collaboration for the purpose of interoperability and harmonization of policies. The digital activities can outpace the institutional development processes and regulatory frameworks - requiring proactive development of measures such as regulatory sandboxes.

In general, international studies of the digital regulation problems conclude that there is a need to apply a systematic approach to building an applicable legislation, which in case of the Kyrgyz Republic means the need for its codification, and the need to focus on the existing regulatory standards in the world to create a unified and barrier-free legal environment for activities in the global cyberspace.

## Legal basis and principles of building the enabling regulatory environment for a developed, competitive digital economy in the Kyrgyz Republic

**The fragmentation and heterogeneity** of the Kyrgyz Republic legislation, including the historically established normative legal acts (NLAs), are major obstacles to achieving the Project objectives. In this regard, the regulatory gaps analysis is functionally aimed at presenting the Kyrgyz Republic digital economy legislation as a unified **system**, which is an essential preparatory step for its **codification**. The functional approach makes it possible to assess the target provision of each current legal act in the system, to identify and describe the regulation gaps, including those caused by the development of the relations in the digital economy and the associated legislation lagging.

Regulation shortcomings identified in the course of regulatory analysis are not limited to gaps, because they can be caused by the actual inoperability of legal provisions or their inconsistency with the changed social relations in course of the digital economy development. Besides, quite working and applicable provisions may no longer meet the innovative development goals enshrined in the Kyrgyz Republic Constitution, laws and presidential acts, and therefore, should be considered as barriers. Filling the gaps and removing barriers - that is, the next phase of project implementation - should, first, be guided by best practices, if applicable to the Kyrgyz Republic and, second, take into account the basic legal regulation requirements, discussed below.

The Project work will be based on the **general legal principles** that include fundamental values such as respect for and protection of human rights; protection of personal data and the right to privacy; open and transparent regulation, ensuring a nondiscriminatory, inclusive approach based on the involvement and consideration of opinions in decision-making by all stakeholders; respect for the right to actively seek and impart information and to access it on fair terms. Basic **technical and regulatory principles**, including interoperability of policies and procedures, harmonization of regulatory frameworks with recognized world best practices, use of best practices from leaders in digital transformation; and support for market competition and innovation are also taken into account.

Effective regulation - combining international experience, best practices and an evidence-based framework - is a critical key to the Kyrgyz Republic's accelerated digital transformation. The basis of effective regulation is the **basic properties of law** as a regulator of human activity, which should be described in more details. The first of these is the **legal certainty** principle. Legal certainty is the clarity and precision of existing legal provisions, the stability of legal and reasonable judicial acts, the stability of legal relations formed on their basis, so that interested persons with a reasonable degree of probability could foresee the consequences of the court's application to them of existing legal prescriptions and accordingly, foresee the consequences of choosing one or another option of their behavior (Masalajiu, 2009). The legal certainty principle means that the rule should be clear and understandable to those whom it is addressed to. Any development of law, including that which implies or accepts the automation of certain areas of human activity, should increase legal certainty, rather than decrease it.

Legal provisions work because they increase trust, not decrease it. Therefore, the second (following the legal certainty principle) requirement for legal regulation is the **principle of trust** in the law and trust as an outcome of law. The law works when it is trusted, and an agreement is signed with

the assumption that it will be executed, and the public service is used in the expectation of obtaining an official result.

Introduction of modern legal tools, such as smart contracts, as well as the digitalization of public administration cannot diminish trust and should not deprive people of the opportunity to check the effect of a rule. One cannot completely trust the provisions that have been fully or partially automated. No hardware can be 100% reliable. There is a growing number of studies supporting the phenomenon of implicit trust in automated systems (Skitka et al., 1999; Parasuraman and Manzey, 2010). This is explained by one of the inherent cognitive distortions in human thinking, **the automation bias**. This distortion causes overlooking by the individual of factors and elements that are not explicitly indicated by the automated system. For example, of two equal choices, the system randomly selected one, resulting in the possibility to discriminate the second and all subsequent choices. Studies also show that people tend to take the wrong action when advised by an automated system, even if the recommendation contradicts the experience and other reliable data available to the individual. For example, many people turn into a one-way street in the wrong direction following the navigator's prompting - even though they see the forbidding signs.

The three listed basic properties of law as a social regulator (promoting legal certainty, increasing trust in the law, eliminating the automation distortion) act as the main metrics (or, in other words, application criteria) both in the analysis of regulatory gaps and in the subsequent development of proposals to eliminate the identified shortcoming in the legislation during codification. The fourth basic property refers not so much to the result as to the legal regulation process: it is the need for **participation (representation)** in the development of approaches to legal regulation in the digital economy - this has already been mentioned above on the international approaches. As mentioned below in consideration of best practices for developing a conceptual framework for analysis, the digital discrimination is one of the most significant risks to the emerging digital society. Therefore, the broadest possible involvement of all stakeholders in the project discussion, the aggregation and consideration of their interests is a basic requirement for both the project implementation and the application of its results.

## Analysis methodology

Based on the above discussed legal basis and principles, the following methodology was used in the regulatory gap analysis. The analysis was based on **the structure** proposed in the previous stage of work. As background information for the analysis for each section of the legislation and related changes in legislation, a **list of NLAs has been compiled**. In addition to being the analysis subjects, the acts included in the list were also considered from the perspective of subsequent codification: taking into account which of their provisions require incorporation into the code text, which should be amended, and which should be replaced by the code's provisions or abolished altogether.

Considering that according to the ToR for the Consultant's services, the analysis subject is broader than the planned regulation subject of the digital regulatory framework, the analysis also included areas of legislation in which significant changes are expected after adoption of the certain legal acts. The purpose of including these areas in the analysis is also related to the need to systematize legislation and address its fragmentation. At the same time, the analysis is focused on the main directions of the legal regulation development in the digital economy and therefore does not include those legal acts where technical amendments are possible (in particular, in the registration legislation), or which development should be the subject of separate activity (for example, financial legislation).

Results of the regulatory gap analysis are outlined in a brief (table) and a more complete form (in the form of comments). A tabular summary of the shortcomings identified in the legislation is the ground for the next stages of work, in particular, to create a roadmap for amendments to the legislation and subsequently discuss on a specially created digital platform. Each identified shortcoming in the table is assigned a **unique number**, which is needed to track the work on the identified shortcoming in the next steps of work. The ideal Project outcome is to eliminate all the identified shortcomings. However, this methodology of the regulatory gap analysis allows its repeated application, enabling to assess the Project performance, while amendments to the current legislation is being prepared, adopted and enforced, and also when other related legislative amendments are adopted and take effect.

Based on the legal basis and principles, and the international context described above, the identified shortcomings have been classified. The classification includes four categories (classes) of normative provisions of the current Kyrgyz Republic legislation:

- **(G) Gap** - a shortcoming refers to the gap category if, in accordance with the applicable legal basis and principles, regulation is required, but the relevant provisions are missing in the Kyrgyz Republic legislation;
- **(O) Obsolete provision** - a provision falls into the category of obsolete provisions if it is valid and applicable, but inconsistent with the applicable legal basis and principles described above, and as such it should be replaced or canceled;
- **(B) Barrier** - a provision prevents one's interests from being exercised, while such interests themselves may be considered legitimate, and the purpose of establishing an obstacle in a normative legal act is inconsistent with the applicable legal basis and principles described above, and as such the provision establishing the barrier should be replaced or canceled;
- **(N) Non-functioning provision** - a provision of a law or bylaw does not actually apply, based on the existing practice or expert evaluations.

The analysis compares each identified shortcoming with the applicable **foreign best practices** consistent with the applicable legal basis and principles described above. Wherever possible, the analysis described the experience of several countries or international organizations that are relevant to the issue under consideration and somehow consistent with the applicable legal basis and principles. While the best international practices described in the analysis are not necessarily a solution to the regulatory shortcoming to which they relate, the information about them may help to develop a solution to address the shortcoming when working on then text of the regulatory acts.

## Key findings, by the analysis areas

In accordance with the terms of reference for the Consultant's services, the analysis was conducted, in particular, with respect to the following regulation areas:

- Data and digital/ICT technologies (distribution and access to information in the form of open data, electronic document management, personal data processing and protection, use of information resources and systems, including the distributed cloud document management, artificial intelligence, blockchain technology, data centers and their data transmission channels, digital information protection, Internet services, mobile applications, electronic payments, electronic identification, public key infrastructure and digital signatures);
- Telecommunications (licensing and technical regulation issues including digital and telecommunications infrastructure, spectrum licensing, management and monitoring, addressing and numbering resource management, network interconnectivity, access to key facilities and “open access” policies, cross-infrastructure “dig once” regulation, network neutrality, converged voice data regulation, antimonopoly regulation);
- Cybersecurity (cybersecurity issues, use of digital evidence, criminalization and investigation of cybercrimes, protection of critical infrastructure);
- Public-private partnership (implementation of PPP models in the ICT sector);
- Civil sector (issues of signing and executing digital transactions and connection agreements, securing rights to digital assets, conducting transactions with such assets, electronic payments);
- The banking sector and financial technologies (issues of electronic money, payment systems, electronic payment solutions, electronic money transfer, implementation of financial technologies in the concerned agencies (KR Ministry of Finance, KR Chamber of Accounts, KR National Bank);
- Taxes (issues of digital accounting and other reporting, digital labeling of goods, interaction of taxpayers with the tax authorities through the electronic document management);
- Customs sector (issues of customs clearance and control using the digital means, customs control of intellectual property);
- Public administration and public service delivery (e-governance, digital government portals, cloud technologies regulation, digital delivery of public and municipal services, electronic document management, interconnectivity platform, competency development, improving digital skills of public servants).

For the purpose of subsequent use in the development of the Kyrgyz Republic’s regulatory frameworks, the analysis materials are arranged in accordance with the structure of work proposed under Output 1.

**The digital governance legal framework** was analyzed in accordance with the following industry principles derived from best regulatory practices in this area:

- Digital transformation of processes;
- Platform-independence and focus on mobile devices;
- Vendor-independence and data portability;
- User-centric approach and the user's right to informational self-determination;
- Digitalization at all stages of the formation and delivery of a public service or business process;
- Government as a platform;
- Making management decisions based on digital data;
- Use of open data;
- Use of open standards and free software;
- Technological neutrality and openness to innovation and “disruptive” technologies
- Presumption of public availability of information

The main conclusion from the analysis was that the Kyrgyz legislation lacks a description of structure of legislative and other normative legal acts containing provisions on the digital economy

regulation, and does not contain rules for resolving discrepancies among various acts regulating relations in the digital environment. The digital laws of the Kyrgyz Republic are adopted without consideration of each other, which causes many legal conflicts. The codification and the unified system of digital governance in the Kyrgyz Republic devised in accordance with it allows to eliminate such conflicts.

Besides, the structure of digital governance bodies is in fact dysfunctional. No digital governance subjects, other than the state, are presented in it, there is no delineation of authority for the digital information protection. Also, the e-governance principles envisaged in the current legislation are outdated, reflecting the logic of previous stages of public administration reform, which is why they should be updated in accordance with the above principles and regulatory framework.

The regulatory gap analysis did not include a centralized analysis of the terminology used in the legislation. The used terms were analyzed for some areas of regulation in accordance with their context, while the compilation of a full-fledged **glossary** for the digital economy regulation is an integral part to the legislation codification in this area.

The above principles should be taken into account in codification of legislation regarding the **digital governance objects and subjects**. Currently, the legislation does not provide conditions for digital governance, that is, data driven governance. Data from the government information systems are not used in decision-making and analytics either in the public or in the private sectors. The data formats and data exchange interfaces are different and incompatible in different bodies, which prevents building of an interoperable decision-making system.

The multi-level model of regulation of relations depending on their object (infrastructure, applications, data, services) enshrined in Article 18 of the E-Governance Law of KR applies only to the public sector and, moreover, is not reflected in other legal acts of the KR, including those adopted later. At the same time, the multi-layered nature of relations in the digital economy is the fact that cannot be ignored in the relations regulation in this area. The KR legislation does not set any legal regime for distributed information systems, and there are no conditions for the transition from electronic document management to the record-based management in the information systems, including distributed ones necessary in the digital economy.

Lack of provisions allowing exclusive digital interaction prevent the full transition to digital interaction, as the government agencies require paper documents. There are no standards for electronic document management or circulation of digital records. There are still outstanding issues of electronic document exchange with non-state organizations and individuals, and entire industries are cut off from the electronic document flow or other digital interaction.

The introduction of digital national currency is not yet regulated, although the issuing and circulation of such currency would save the National Bank the cost of printing real currency, and its adoption would facilitate the digital payments market development. It is necessary to make package amendments in the tax, civil, and banking legislation for the full implementation of digital financial assets and cryptocurrencies, and for supervision and administration, amendments are needed in the administrative and criminal legislation, thus creating a legal system for the regulation of different currency types in the Kyrgyz Republic market.

In the current legislation, there is no system of the main actors (subjects) of digital governance, which does not allow to build a system of relations in the digital environment specifically as a system. At the same time, the status of each of these subjects should be regulated as part of regulation of the relevant type of activity in the digital economy. In the digital economy, the emerging new actors, such as the digital platforms or ecosystems owners, remain invisible for the industry and antimonopoly laws, which fail to hold concentration of significant market power in their hands and, as a result, cannot address

the economic inequality. First of all, the effective digital governance requires regulation of such new entities' activity on a cross-industry basis.

The regulation of **relations in the digital environment, including the grounds for their emergence** should also be based on the principles of presumption of public access to information, equality of participants in relations in the digital environment and technological neutrality. Kyrgyzstan's legislation in this area needs to unify the different sources of information in the form of “old” (mass media) and “new” (social media, messenger channels, etc.) media, which requires revision and codification of the activities of various media based on the general principles of freedom of speech, legality and fairness in the information distribution. In terms of the basic requirements for legal regulation in the digital economy, an important conclusion of the analysis is that the Kyrgyz Republic legislation lacks a legal regime of trusted services (such as guaranteed delivery or time marking), which hinders the development of relationships in the digital economy and increase the trust in it.

The problem is that the legislation, primarily Article 12 of the E-Governance Law of the KR treats, considers the publicly available information as a legal regime of information, opposing the confidential information. This approach is outdated, since it does not create conditions for securing a balance between the public interest in the use of information (expressed, in particular, in freedom of speech) and the rights of information holders to restrict access to it, if they have the appropriate authority granted by law. The regime of access to information is poorly structured and not systematized, which leads to significant overlaps and inconsistencies among the different secrets regimes, significantly complicating the use of relevant information, including such use, which does not infringe upon the rights of persons to whom a particular secret relates.

Information from the state bodies and local governments systems is not actually placed on the websites of state bodies and local governments on the Internet in form of open data, since in the legislation, there are no procedures (practical guidelines) for the open data publication. The law does not provide a legal basis for the use of free software products and open API (Application Programming Interface) either.

The KR legislation lacks basic information protection and **cybersecurity** provisions. The specialized law that should contain such provisions - on electronic governance - contains only provisions to protect the right of access to information and to protect the rights of the information holder. These rights are important elements of cybersecurity, but neither information protection nor cybersecurity can be limited to the rights of key actors in the digital environment. Therefore, the basic provisions on cybersecurity, in particular on standardization and technical regulation in this area should be enshrined in a law.

The situation with the **personal data** protection is primarily complicated by outdated legislation - more than 10 years have passed since adoption of the Law “On Personal Information”. During this period, there have been global technological changes and new information and communication technologies are being introduced. Not only has the approach to collecting personal information, but also the public attitudes to this issue have changed.

One of these global changes in international standards for the personal data protection was the definition of new rights granted to citizens to manage their personal data in their processing, including those based on the mathematical algorithms, artificial intelligence; the obligation of personal data holders to notify the authority and citizens about leaks of personal data. Another shortcoming of the current law regarding the personal information is the requirement to the form of consent to process personal data - in writing (offline) or in electronic form (online), signed with an electronic signature.

The current law does not recognize the expression of a person's will by electronic means or devices. The law does not establish all of the internationally recognized legal grounds for dealing with personal data (e.g., availability of a contract), the exceptions to obtaining consent for lawful data processing are not clear, for example, for schools that are not state bodies that have an exception for obtaining consent when performing their functions.

In the general context of modern approaches to the protection of citizens' rights to privacy, there should be the right to receive information about unauthorized access by third parties to their personal data, the right to assert their disagreement, regardless of place of residence to receive competent protection, including from the authorized body. These provisions are also missing in the Kyrgyz legislation, as well as penalties for offenses and crimes with personal data, therefore, it is necessary to make amendments to the Code on offenses and the Criminal Code.

The determining factors in this case should be not so much the penalties for violations, but rather the restoration of the violated rights of subjects and compensation of the harm caused to them by illegal actions. The regime of cross-border data flows is also a challenge in Kyrgyzstan's integration in the Eurasian Economic Union, whose digital agenda includes the creation of the EEU common market and circulation (free movement) of citizens' personal data. The powers and competence of the authorized state body for the personal data protection are still not clearly defined.

In the Kyrgyz Republic there is no legislation regulating the use of **big data and artificial intelligence technologies**. Another critical type of data for the digital economy - **spatial data** - is based on the outdated Law of the Kyrgyz Republic "On Geodesy and Cartography", which does not meet the current needs to provide legal regulation of spatial data and does not contain sufficient conditions for creation and development of the national infrastructure. The current normative legal acts of the Kyrgyz Republic do not regulate the collection, storage, processing, distribution, protection, and use of spatial data and metadata; there is no legal regulation of spatial data standardization.

Problems **with the identity management** in the Kyrgyz Republic are due to the fact that the infrastructure of electronic signatures or other more advanced ways of identity management is not fully deployed, and the applicable standards are commercial and developed by the Russian Federation and the Republic of Kazakhstan, which puts the Kyrgyz Republic domestic market in a dependent position. In accordance with international requirements, it is necessary to introduce the requirements, rules and standards for generation of electronic signatures at the national level, with adoption of uniform requirements for electronic signature certificates at the Eurasian Economic Union level.

Currently, the judiciary authorities do not recognize digital evidence in court proceedings for lack of competence and understanding of the digital legislation. There is no procedure for storing electronic documents, records (information) in digital form, or legislation on digital (electronic) archives. The legislation regulating the use of an ID-card - a citizen's passport does not allow the wide use of this tool, there are no opportunities to use other means, such as tokens, codes, identification by SMS, video identification.

Legislative opportunities for digital identification are significantly limited to the public administration - the provision of public services and voter participation in elections and referendums. For example, there is no provision for digital identification in e-commerce interactions. Legislative regulation of biometric identification is limited to the areas of migration and electoral legal relations, and the legislation regulating the legal status of the Unified Identification System does not assume the possibility of its wide use directly for identification purposes, and does not assume the connection of commercial banks and other organizations to it. All these shortcomings are particularly evident in light of the active work in various international platforms, primarily UNCITRAL, to determine the identity management principles and mechanisms, and, therefore, the results of work of international expert

groups in these platforms should be taken into account when codifying the Kyrgyz legislation in the field of identity management.

Analysis of the **digital services** legal regulation was based on the principles of digital security, healthy competition between digital services within the digital platforms, freedom of transition of users between digital services, freedom of disposal by users of their data, and guarantees of transparency of information about the service. From this point of view, it is necessary to fix the requirements that currently do not exist in the legislation, allowing to ensure fair competition in the information field, and to provide guarantees of users' personal data protection.

Similarly, legislation on the **public and municipal services** should implement the currently missing principles of proactive provision of the public and municipal services, electronic application, priority of the “registry” model, predominantly or exclusively digital interaction between the body when providing a service and the recipient, “proactive” offer of an opportunity to receive a particular service even prior to the occurrence of a legal event.

Besides, the KR legislation currently does not explicitly prohibit the provision of state and municipal services by processing biometric data, therefore, it is necessary to enshrine guarantees for the right to refuse to provide their biometric information without losing the opportunity to receive the public and municipal services in electronic form.

In the area of **digital health and well-being** services, the fundamental principles of e-health system development are not enshrined, and some gaps were identified in terms of the medical personal data security, for example:

- there is no procedure for issuing and obtaining informed voluntary consent and consent to processing of the patient’s personal data on the basis of conclusive actions when receiving health services using telemedicine technologies;
- the procedure and cases of transfer of personal medical data to a third party are not defined;
- some issues of processing personal medical data in medical information systems are not regulated.

Among other identified gaps in this area, one can point out that the procedure for co-payment is not defined for receiving health services using the telemedicine technologies with the participation of private companies in public-private partnerships, and the procedure is not regulated for using remote monitoring devices of health and physiological parameters of home use and hospital-replacement technologies, and the procedure is not provided for using a simple electronic signature by the patient when receiving medical services.

There are no self-standing (separate) legal acts on the **digital governance technological infrastructure** in the Kyrgyz Republic, which is why the relevant regulatory and non-regulatory legal acts were analyzed on the creation and operation of certain types and even infrastructure facilities (including strategic planning documents). The E-Governance Law of the Kyrgyz Republic provides for the regulation of state data centers only. The legislation has no provisions of the data center standardization. The technical regulation legislation does not provide sufficient mechanisms for the adoption of international standards at the national level.

These gaps in the legislation should be eliminated by stating in the legal framework the basis for creation and operation of the digital management technological infrastructure in the Kyrgyz Republic, based on the principles of non-discriminatory access to infrastructure; alienability of the electronic interaction infrastructure from its developers, suppliers and operating organizations; certainty of the procedure for using electronic interaction infrastructure; mutual compatibility of the information systems

of the electronic interaction infrastructure; stability and continuity of the characteristics of the electronic interaction infrastructure; maximum use of market opportunities; security of personal data and restricted information.

The legal norms regulating the creation of **telecommunications networks**, their operation and the use of telecommunications resources are included in various sectoral legislation and are often not harmonized with each other. Therefore, it is necessary to systematically align the norms on the telecommunications networks and resources with the sectoral (special) legislation, possibly deleting them from other legal acts, to avoid unnecessary duplication and over-regulation. In the KR Law on Telecommunication and Postal Services, it is necessary to exclude provisions relating to postal services due to the existence of the sectoral (special) law of the KR “On Postal Services”.

The principle of comprehensive support for the provision of high-quality traditional and innovative telecommunication and postal services, enshrined in the law, is not specified or implemented in practice in any way. In particular, the law does not contain provisions to facilitate the use of radio spectrum for the advanced services delivery and the development of new technologies (“Internet of things”, artificial intelligence systems, etc.). The terminology of this law should be brought in line with the International Telecommunication Union glossary.

The law also contains a non-working provision on compensation for losses incurred by telecommunications operators due to suspension of their activities, which requires regulation of the procedure for appropriate compensation from the state budget. The provision that construction and other organizations should observe the telecommunications operators’ requirements for the location of their equipment does not work either, because there is no developer’s liability for failure to comply with this norm. The provisions on contributions for the telecommunication sector development and additional taxation of telecommunications services do not work or contain significant barriers, and the methodology for calculating the annual fee for the use of nominal and (or) radio frequency spectrum bands is not aimed at encouraging network expansion and reducing the financial burden on the communications operator.

Article 30 of the KR Law On Telecommunication and Postal Services on **interconnection** is mainly addressed to “dominant” operators”, contains ambiguous terminology and does not allow the development of inter-operator relations based on equal agreements between operators, departing from the logic of building the telephone (fixed) communication networks.

The global trend in the regulation of interconnection relations is based on the principles of technological neutrality in interconnection traffic, abandonment of strict requirements for the construction of hierarchical fixed-line networks, and reduction of interconnection tariffs: “operators should earn on their customers, not on their competitors”. Interconnection rules in the Kyrgyz Republic also retain the obsolete logic of requirements to network functioning on the basis of circuit switching rather than packet routing. In addition, the current communications legislation does not contain provisions on the elimination (or significant reduction) of interconnection tariffs, primarily in cross-border inter-operator cooperation within the integration associations with the participation of the Kyrgyz Republic (EEU, CIS, etc.) - the issue of reducing (to a minimum level) the interconnect rate and cancellation of international roaming.

In the KR legislation, the issues related to the regulation of **communication** services, the rights and obligations of users (subscribers) and operators (suppliers) of telecommunications services are generally addressed at a fairly satisfactory level, without those features and uncertainty of regulation, which have recently become characteristic of the telecommunications legislation of several CIS countries. However, there are still open (requiring normative clarification) issues not only about the scope of powers and responsibilities of telecommunications operators, but also about who exactly and by what criteria can or should be classified as an operator. This brings the problem of legal regulation of telecommunications services back to more fundamental issues - the principles of licensing and authorization activities in the field of telecommunications, the stimulation of development and consumption of new value-added services, and the procedure of interaction between the telecommunications networks of licensed operators and equipment of the OTT service owners. It should

also be noted that the current KR legislation does not include provisions for a truly independent status of the telecommunications regulator.

International experience (including in CIS countries) demonstrates the desirability and **need for an independent status of the telecommunications regulator**. The independence of the telecommunications regulator is a critical factor in increasing mutual trust and fruitful interaction between the government and non-government organizations in the field of digital transformation.

The analysis also covered those sectors and acts of legislation, which may require changes due to codification of the Kyrgyz Republic digital legislation. Thus, a number of shortcomings of the existing regulation were identified in **public-private partnership (PPP)**. The Law of the Kyrgyz Republic “On the Public-Private Partnership” does not allow inclusion in other laws of the provisions, in which the PPP is the regulation subject.

The existing law lacks mechanisms to ensure competition and create equal and fair conditions for all participants in the tender process, and as a result, violates the principles of public-private partnership (transparency of activity, fairness, fair distribution of risks) in the selection of the tender winner. In contrast, although the law mentions the possibility of awarding a public-private partnership project through direct negotiations, there is no direct negotiation procedure itself.

The specifics of information technology development and the ever-growing volume of database elements cannot be the subject of a public-private partnership agreement financed from the state budget (in absence of state budget funds), because continuous improvement and modernization of information systems are necessary, which is better achieved by long-term support of private investment rather than by the state. Therefore, it may be appropriate to develop a separate law for public-private partnerships in the digital sphere.

Kyrgyzstan’s **Civil Code** does not mention the smart contract, nor does it define the civil law regime of digital rights and virtual assets and the related concepts, which requires appropriate amendments. Legislation regulating the professional retraining and professional development of civil servants does not contain requirements for training in digital skills and competencies. It does not establish performance indicators, or provide for online training and certification, or any scope to create digital teams in departments.

The **tax legislation** does not establish the basic principles, specific tasks and critical priorities of tax policy under transition to the digital economy. There are no basic concepts defined, and with regard to the already introduced “digital tax”, the criteria relating to the taxation subjects and objects are not clearly defined.

In terms of **customs legislation**, we have to conclude that the potential of electronic advance notification is not fully utilized, that there is duplication of the state controls at the border, that there is a need to simplify and optimize control over the delivery of goods, and that technologies for simplified and accelerated operations for certain categories of goods need to be developed. The KR legislation does not directly regulate the use of cloud technologies, and does not establish the relevant concepts.

Based on the analysis results, it is also important to note that there is no law on “**regulatory sandboxes**” in the Kyrgyz Republic. This prohibits using the “regulatory sandbox” mechanism in testing new legal relations, support for innovation in the digital sphere, and there are no mechanisms of partnership, state support for the technological start-ups.

## References

1. Digital Pathways (2020) *Digital Economy Kit: Harnessing digital technologies for inclusive growth Version 2*.
2. GSMA (2021) *GSMA Mobile Connectivity Index*. Available at: <https://www.mobileconnectivityindex.com/> (Accessed: May 7, 2022).
3. ITU (2020) *ITU | ICT Regulatory Tracker*. Available at: <https://app.gen5.digital/tracker/metrics> (Accessed: May 7, 2022).
4. ITU (2021a) *Benchmark of fifth-generation collaborative regulation*.
5. ITU (2021b) *The impact of policies, regulation, and institutions on ICT sector performance*.
6. ITU and The World Bank (2020) *Digital Regulation Handbook International Telecommunication Union*. Geneva.
7. OECD (2020a) *Going Digital integrated policy framework*. Paris. Available at: <https://doi.org/10.1787/dc930adc-en> (Accessed: May 4, 2022).
8. OECD (2020b) “Vectors of digital transformation,” *OECD Digital Economy Papers*, No. 273. Available at: <https://doi.org/10.1787/5ade2bba-en> (Accessed: May 5, 2022).
9. Portulans Institute (2021) *Network Readiness Index 2021 Kyrgyzstan*. Available at: <https://networkreadinessindex.org/country/kyrgyzstan/> (Accessed: May 7, 2022).
10. UNCDF (2021) *The Inclusive Digital Economy Scorecard - UN Capital Development Fund (UNCDF)*. Available at: <https://ides.uncdf.org/about-the-scorecard> (Accessed: May 7, 2022).
11. UNDP (2021a) *UNDP Digital Strategy 2022-2025*.
12. UNDP (2021b) *UNDP Whole-of-Society Digital Transformation Digital Readiness Assessment Methodology*.
13. USAID (2020) *Digital Ecosystem Framework*.
14. World Bank (2020) *Digital Government Readiness Assessment (DGRA) Toolkit V.31 Guidelines for Task Teams*.
15. World Bank and DE4A (2020) *Digital Economy for Africa Country Diagnostic Tool and Guidelines for Task Teams Version 2.0*.
16. UNCTAD (2021). *DIGITAL ECONOMY REPORT. Cross-border data flows and development: For whom the data flow*.
17. Masalajiu R. The Principle of Legal Certainty in the Science and Practice of the ECtHR and its Impact on the Availability of Justice at the Stage of Review Proceedings in Civil and Arbitration Proceedings // *Arbitration and Civil Procedure*. 2009. No. 7.
18. LINDA J. SKITKA, KATHLEEN L. MOSIER, MARK BURDICK. Does automation bias decision-making? *International Journal of Human-Computer Studies*, Volume 51, Issue 5, 1999, Pages 991-1006, ISSN 1071-5819, <https://doi.org/10.1006/ijhc.1999.0252>
19. Parasuraman R, Manzey DH. Complacency and Bias in Human Use of Automation: An Attentional Integration. *Human Factors*. 2010; 52(3): 381-410. doi:10.1177/0018720810376055

## Section 1. Legal basis for digital governance

### Content

- the structure (considering the current digital agenda)
- the relationship between legal acts
- relations regulated
- digital governance principles
- digital governance bodies; participation of all stakeholders in governance

### Current regulation (existing legislation):

1. E-Governance Law of the Kyrgyz Republic
2. Electronic Signature Law of the Kyrgyz Republic
3. Innovation Activities Law of the Kyrgyz Republic
4. Virtual Assets Law of the Kyrgyz Republic
5. E-Commerce Law of the Kyrgyz Republic
6. Law of the Kyrgyz Republic “On Telecommunications and Postal Service”
7. Law of the Kyrgyz Republic “On Access to Information Held by State Bodies and Local Self-Governments of the Kyrgyz Republic.”
8. Public Procurement Law of the Kyrgyz Republic
9. Law of the Kyrgyz Republic “On Personal Information”
10. Law of the Kyrgyz Republic “On Biometric Registration of Citizens of the Kyrgyz Republic”
11. Law of the Kyrgyz Republic “On National Security Agencies of the Kyrgyz Republic”
12. Decree of the Kyrgyz Republic President “On the National Development Program of the Kyrgyz Republic to 2026” dated October 12, 2021, PD No.435
13. Decree of the Kyrgyz Republic President "On Further Measures of Digital Transformation of the Kyrgyz Republic," dated July 21, 2021, UP No.305
14. Decree of the Kyrgyz Republic President "On Urgent Measures to Enhance the Implementation of Digital Technologies in Public Administration of the Kyrgyz Republic," dated December 17, 2020, PD No. 64
15. Resolution of the Kyrgyz Republic Cabinet of Ministers "On Approval of the Action Plan of the Kyrgyz Republic Cabinet of Ministers to implement the National Development Program of the Kyrgyz Republic to 2026" dated December 25, 2021, No. 352
16. Resolution of the Kyrgyz Republic Cabinet of Ministers “On the creation of the state institution "Project Office" dated August 16, 2021, No. 137
17. Resolution of the Government of the Kyrgyz Republic “On Approval of the Rules for Use of the State Portal of Electronic Services” dated October 7, 2019, No. 525
18. Resolution of the Kyrgyz Republic Government "On Approval of the Requirements for the Protection of Information contained in the Databases of State Information Systems," dated November 21, 2017, No. 762
19. Resolution of the Kyrgyz Republic Government "On Approval of the Regulations of the State Electronic Payment System," dated October 7, 2019, No. 709
20. [Resolution of the Kyrgyz Republic Government “On Approval of the Requirements for Interaction of the Information Systems in the Tunduk Interagency Electronic Interaction System”](#), dated April 11, 2018, No. 200
21. [Resolution of the Kyrgyz Republic Government “On Implementation of the Pilot Project “State as a Platform” to Introduce the Innovative Ways of Providing Public and Municipal Services”](#), dated February 25, 2020, No. 113
22. [Resolution of the Kyrgyz Republic Government “On Certain Issues Related to the Use of e-Signature”](#), dated December 31, 2019, No. 742
23. [Resolution of the Kyrgyz Republic Government “On Approval of the Regulation on the State System of Electronic Communications and the Rules for its Use”](#) dated December 31, 2019, No. 745

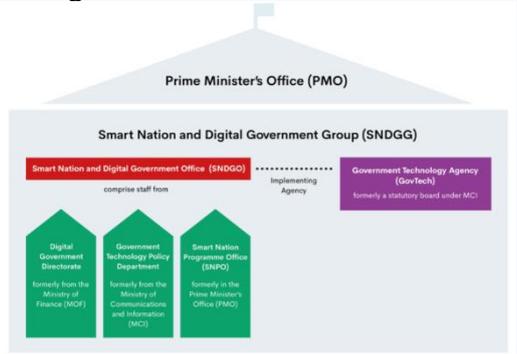
24. Resolution of the Kyrgyz Republic Government “On Approval of the Regulations on the Automated Information System “State Electronic Document Management System” dated October 30, 2020, No. 526
25. Resolution of the Kyrgyz Republic Government “On the Model Instructions for Paperwork in the Kyrgyz Republic” dated March 3, 2020, No. 120
26. Resolution of the Kyrgyz Republic Government “On Some Issues Related to the State Information Systems” dated December 31, 2019, No. 744
27. Resolution of the Kyrgyz Republic Government “On Approval of the Requirements for the State Data Processing Centers and Communication Channels Connecting Them” dated December 31, 2019, No. 747
28. Resolution of the Kyrgyz Republic Government “On Certain Issues of E-Governance in the Kyrgyz Republic” dated December 31, 2019, No. 748
29. [Resolution of the Kyrgyz Republic Government “On Some Issues Related to the e-Governance State Infrastructure” dated December 5, 2019, No. 661](#)
30. [Resolution of the Kyrgyz Republic Government “On Certain Issues Related to Basic State Information Resources” dated February 6, 2020 No. 66](#)
31. Order of the Kyrgyz Republic Cabinet of Ministers dated July 2, 2021, No. 74-r
32. Order of the Kyrgyz Republic Cabinet of Ministers dated January 12, 2022, No. 2-r
33. The digital transformation concept “Digital Kyrgyzstan 2019-2023”

#### Brief description of the identified shortcomings and international practice benchmarks

No.	Shortcomings	Type <sup>5</sup>	Best practices
1.1	The legislation lacks a description of the structure of legislative and other normative legal acts containing provisions to regulate the digital economy and does not contain rules for resolving conflicts among various acts regulating relations in the digital space	G	The project for the codification of digital area legislation in the Kyrgyz Republic is unique and has no analogs in the world practice. At the same time, such codification is, in many respects, a forced measure caused by the fact that the Kyrgyz Republic's digital laws are adopted without consideration of each other, which causes many legal conflicts. Codification and the unified digital governance system in the Kyrgyz Republic developed in alignment with it, allow removing these conflicts.
1.2	In fact, the digital governance bodies' structure is non-functional. Besides, it does not represent the digital governance subjects other than the state. In the Kyrgyz Republic, the transition to e-governance in is coordinated by: 1) the E-Governance and ICT Development Council under the Kyrgyz Republic Government (hereinafter referred to as the Council), which is a supreme body for coordinating the	N	In the US, the e-Government working group includes about 90 government employees representing about 50 government agencies. The activities of the working group are normatively fixed in E-Government Strategy. The e-Government working group identified key federal problems that can be solved by the e-government and e-business concepts. In Singapore, the digital governance bodies report directly to the Prime

<sup>5</sup> The following types of regulatory deficiencies are listed in the table:

- (G) regulatory gap (regulation is required but is missing)
- (O) obsolete provision (the existing provision needs change)
- (N) non-functioning provision (the existing provision is non-functioning for the reasons described)
- (B) this provision is an unreasonable barrier to the implementation of activities

	<p>transition to e-governance in the Kyrgyz Republic;</p> <p>2) The Interdepartmental Commission for the Coordination of Informatization (hereinafter referred to as the Commission), which ensures interdepartmental coordination of departmental projects for the transition to e-governance in the executive authorities of the Kyrgyz Republic, local self-governments, state and municipal enterprises and institutions, including in the process of implementation and provision electronic public and municipal services.</p> <p>However, these advisory bodies did not meet for the last four years and did not carry out their activities under the Kyrgyz Republic legislation.</p> <p>For example, the law stipulates that the Council agrees on the e-governance NLAs, while in practice, in recent years, NLAs have been adopted in accordance with the legislation and regulations of the government without the consent of the Council.</p> <p>According to the Kyrgyz Republic President's Decree "On Further Measure of Digital Transformation of the Kyrgyz Republic" dated July 21, 2021, PD No. 305, the Supervisory Board for Digitalization under the Kyrgyz Republic President was established; however, it also functions fragmentarily and does not reflect the general picture of digital development as a whole.</p>	<p>Minister (head of the state) and are divided into the Smart Nation Office and e-Government Office (a coordinating body including representatives from the Ministry of Finance, Ministry of Communications and Information, Prime Minister's Office) and the Government Technology Policy Department (the executive body that implements the government digital transformation policy). Direct coordination of digital transformation plans and their implementation is the most effective form of digital transformation management.</p> 
<p><b>1.3</b></p>	<p>Lack of delimitation of powers for the digital information protection (Example: the SCNS (the State Committee for National Security) is the main body for protection of the state secrets, including confidential information, but it is the SAPDP (the State Agency for the Personal Data Protection) that is the body for the PD protection, which should be implemented, but this is the point where there is a data protection problem, because due to its specifics the SCNS implements the necessary measures to protect the state secrets, but not PD).</p>	<p><b>B</b></p> <p>This situation is specific to the structure of the KR state bodies, given the history of their creation and development</p>

	Conclusion: it is necessary to strictly delineate the powers relating to the protection of certain types of information, or to assign these powers to a single digital governance body.		
<b>1.4</b>	The e-governance principles provided for in the current legislation are outdated. In fact, e-government is the very first initial stage of maturity, and it is necessary to move towards digital governance, which (like the digital economy) is characterized by the massive use of data when operations are automated, and decisions are made based on data.	<b>O</b>	Countries that are going through the digital transformation and building the digital economy are adopting a fully "digital" and "smart" government, rather than electronic. The key difference between e-governance and digital governance is the shift from providing online public services to a data-driven approach. User-centered digital services require horizontal integration and interaction between different government agencies. The digital government initiatives often also involve changes in the organization of governance. Following the same path of digital development as all the countries that have declared digital economy as a paradigm for their own development requires a legal framework for digital governance as data-driven governance. A simple "upgrade" of already outdated e-government approaches will not work; innovative regulatory measures and an ecosystem approach are needed.

### Comments

To build an information society and consolidate the efforts of the government agencies, businesses and civil society to accelerate the country's digital transformation and socioeconomic development, as the most critical task, the government agencies and LSG bodies adopted the digital transformation concept "Digital Kyrgyzstan 2019-2023". As part of the Roadmap of the above Concept, the state authorities are implementing various activities and projects aimed at building the digital infrastructure, improving human capacity, and re-engineering the state interaction and governance processes.

However, the Kyrgyz legislation does not describe the structure of legislative and other normative legal acts containing the digital economy regulation provisions, and does not contain rules for resolving conflicts between the various acts regulating relations in the digital environment. The Kyrgyz Republic digital laws are adopted without consideration of each other, which causes many legal conflicts. The codification and the unified system of digital governance in the Kyrgyz Republic being built in accordance with it allow for removing these conflicts.

In accordance with the E-Governance Law of the Kyrgyz Republic, e-governance is regulated by the Kyrgyz Republic Government. The transition to e-governance in the Kyrgyz Republic is coordinated:

1) The E-Governance and ICT Development Council under the Kyrgyz Republic Government (hereinafter, referred to as the Council), which is a supreme body for coordinating the transition to e-governance in the Kyrgyz Republic;

2) The Interdepartmental Commission for the Coordination of Informatization (hereinafter referred to as the Commission), which ensures interdepartmental coordination of departmental projects for the transition to e-governance in the executive authorities of the Kyrgyz Republic, local self-governments, state and municipal enterprises and institutions, including in the process of implementation and provision electronic public and municipal services.

However, these advisory bodies did not meet for the last 4 years and did not carry out their activities under the Kyrgyz Republic legislation. For example, the law stipulates that the Council agrees on the e-governance NLAs, while in practice, in recent years, NLAs have been adopted in accordance with the legislation and regulations of the government without the consent of the Council.

According to the Kyrgyz Republic President's Decree "On Further Measure of Digital Transformation of the Kyrgyz Republic" dated July 21, 2021, PD No. 305, the Supervisory Board for Digitalization under the Kyrgyz Republic President was established; however, it also functions fragmentarily and does not reflect the general picture of digital development as a whole.

The international experience also suggests the need to revise the structure of digital transformation governance bodies. In the United States, the federal information systems serve as the e-government, which is how the government interacts with citizens, non-governmental organizations, and communities.

The US e-government foundations were laid by the formation and operation of the portal [www.data.gov](http://www.data.gov). The feature of this portal is that it is formed and developed only through the administrative impact on civil servants. For example, in 2009, at the policy level, all government bodies were ordered to publish information of at least some value. There are quite a lot of useful applications for users on this portal.

In the US, the e-Government working group includes about 90 government employees representing about 50 government agencies. The activities of the working group are normatively fixed in E-Government Strategy. The e-Government working group identified key federal problems that can be solved by the e-government and e-business concepts. A review of the working group activities showed that the main obstacle to the creation of citizen-centered e-government is the redundancy and duplication of functions and activities in various government bodies.

For example, in 2010, it was found that 22 of the 30 functions are performed in ministries and agencies, and each ministry performs an average of 19 different functions. This situation leads to the development of a large number of duplicate reports, for the creation of which it is necessary to visit dozens and hundreds of Web pages and contact hundreds of call centers in order to get the requested service.

Current U.S. e-government operations use the following fundamental principles:

- the goal is citizens, not bureaucracy;
- a concrete result of e-government action should be there;
- innovativeness in development.

E-government is necessary for the activities of state authorities because the first users of information technology are civil servants themselves.

The main reasons that inhibit the information technology promotion in public administration are the following:

- (1) self-evaluation and self-reflection without regard to civic needs are essential to government agencies;
- 2) officials mostly use the information technology as typewriters and calculators, but not for management decision-making;
- 3) government officials believe that information technology is a threat to their command position, so it is not worth investing funds in the development of information and communication technology;
- 4) most government agencies do not organize the joint functioning of their information flows.

Currently, the US government supports project activities to organize joint activities of all government agencies while using a wide variety of formats: e-procurement format, e-grant format, e-regulation format, and electronic signature format.

Thus, for the United States, the e-government format involves requesting requirements for its own activities. It performs functions for external users and does not perform internal management functions.

In **European countries**, the following factors and conditions define the information society:

- national information infrastructure;
- integrated economy;
- demand for information resources;
- free competition.

Initially, invaluable positive experience in the information support of management processes has been accumulated in the United States; therefore, we will analyze the information support processes in the United States in terms of the possibilities of applying this experience in the Kyrgyz Republic. Internet resources were formed initially and used in the defense department (the Pentagon) - it was the first ARPAnet. Further, the "California Miracle" ("Silicon Valley") was a consequence of the "Washington Consensus" (the American development model).

This development model was aimed at:

- lowering the role of the state in economic development (withdrawal of the state from the regulatory processes);
- use of the tax incentives and tax holidays system for firms participating in this project;
- all-around growth of processes of real (not monopolistic) competition.

As a result of successful real privatization processes, private business and entrepreneurship gained access to defense programs, forcing them to actively explore and apply the information processes to their own businesses. And this was already the first step toward laying the foundation for a serious revolutionary information transformation.

The lack of a regulatory framework for the use of information resources and technologies for information services to the population could have led to an information crisis in the United States, but this did not happen, as the Congress and the President revised the basic legislation in this context, thereby legislating the participation of state authorities in the country informatization processes. The United States at that time occupied a leading position among all world powers in all the criteria for using the Internet space (data transfer speed, number of ICTs, number of network users). Therefore, it was in this country that a genuinely functioning "E-Government" was created, which immediately led to a high level of relations between the state and the population, thereby increasing the efficiency of the entire public administration system.

But the use of "e-Government" has not become a goal in itself, it has provided a large number of effective tools for administrative and government reform, which currently include the following:

- federal public key infrastructure (FPKI);
- system access authorization (ACES);
- government-wide system of federal forms (Fed Forms);
- GILS - search for information resources on all government agencies;
- federal government procurement system (FedBizOpps).

In European countries, the "Technology for the Formation and Development of the Information Society" project was developed as the Fifth Framework Program for Information Research.

The first year of project activities was deemed unsatisfactory. The European Commission came up with a new program called "E-Europe", the goal of which was to form a united interstate information-type society.

The key tasks of the "E-Europe" included the following:

- formation of infrastructural information and communication space;
- free entrance to this space for all interested users;
- regulatory and legal support for information projects: "Multimedia Communication", "E-Commerce", "Transaction Protection";
- effective functioning of e-government in its various forms;
- increasing the professionalism, education and qualifications of all citizens;
- formation and maintenance of the European Union global network.

The key goals of software products in Western countries are to take the lead in the economic, social and spiritual spheres. The Kyrgyz legislators predict economic growth (and economic leadership in the long term) through sustainable and effective public administration. This is the difference between approaches: in Western countries, an individual with his/her requests, needs and interests is placed at the center of development programs, and the goal is socioeconomic development to increase the material well-being of the population; and Kyrgyz software products are focused on the state interests, and only indirectly - on the personal needs of citizens.

With the coincidence in priority areas (law, personnel, infrastructure) in Europe and in Kyrgyzstan, the European concepts are built on the formation of a respectful and trusting attitude of citizens to the information technologies in public life, to the e-government in a variety of formats, to small and medium-sized businesses; while the Kyrgyz concept is based on strong state institutions and not on human resource capacity. We also note that in European countries, e-commerce and e-governments are integrated into a single online technology, which is the basis for entering the digital economy and information society. On the other hand, Kyrgyzstan is trying to digitalize key sectors of the economy and public life.

The third path in the development of digital transformation is **Singapore**, which has set the task of forming a Smart Nation. In Singapore, the digital governance bodies report directly to the Prime Minister (head of the state) and are divided into the Smart Nation Office and e-Government Office (a coordinating body including representatives from the Ministry of Finance, Ministry of Communications and Information, Prime Minister's Office) and the Government Technology Policy Department (the executive body that implements the government digital transformation policy). Direct coordination of digital transformation plans and their implementation is the most effective form of digital transformation management.

Particular attention should be paid to the delimitation of powers in the field of digital security. At present, the main body under Article 15 of the Law of the Kyrgyz Republic "On National Security Bodies of the Kyrgyz Republic" is the State National Security Committee of the Kyrgyz Republic, but the powers are not clearly defined. At the same time, it should be understood that the preservation of state secrets is undoubtedly the prerogative of the national security bodies. However, the information security issues in terms of the digital information control functions within the digital economy could be performed by an authorized state body in charge of digital governance. It should have the necessary administrative powers and mechanisms to influence the information owners and could also act to protect the data owners. Besides, there is a threat when market participants with private ownership try to interact with public participants, since there are significant differences in the security levels of information systems. This entails certain administrative delays, even in cases where the private sector security levels exceed the public sector information systems security levels. Due to the rapid development of common threats to the digital information security, both external and internal, the development of fraudulent schemes, as well as the accelerated development of global practices to ensure the security of information systems, the existing instructive provisions should be constantly reviewed to bring them in line with international information security practices. There also needs to be a flexible mechanism that allows the direct effect of such standards and rules in national legislation without additional legalization measures. A separate step in uniform security should be the platform for private and public sector collaboration to develop uniform digital data security practices.

In this context, an important role will be played by the authorized state body in the field of personal data, which, among other things, should be empowered with the functions of monitoring the information systems security in terms of personal data, a kind of independent arbiter to determine and establish the internal rules for market participants, and sufficient powers and administrative resources.

As applicable international experience in this area, we can refer to the United States, where the administrative and organizational support of information security is aimed at coordinating all actions to protect information and implement the unified state policy of information security; and the experience of developed European countries, which also pay close attention to the comprehensive provision under the national policy of protection of civil society from the information threats arising in the modern global information society.

In concluding consideration of the general issues of the digital governance regulation in the Kyrgyz Republic, it should be noted that it relies on the currently outdated principles enshrined in the E-Governance Law of Kyrgyz Republic. In fact, e-government is the very initial stage of maturity, and we should move towards digital governance, which (like the digital economy) is characterized by the massive use of data, when decisions are made based on data in interaction with consumers of a particular service.

Digital governance should establish the following vectors/principles/logic for building the management processes:

- focus on the needs and demands of citizens, resulting in the use of tools and methods of process changes, depending on the life situations of citizens;
- management decision-making based on the analysis of up-to-date and reliable data (data-driven government);
- formation of a modern change management system that ensures the implementation of strategic priorities based on the needs of society;
- creation of a modern HR management system, formation of professional teams in the civil service;
- formation of a culture of behavior of civil servants that meets the changing challenges of the public administration system;
- a transparent system of public administration based on a process approach;
- cross-cutting interdepartmental digitalization;
- synchronization of the state information systems in terms of functionality and data integration based on unified regulatory rules;
- optimization of costs for the state apparatus through the centralization of auxiliary processes.

The principles of digital governance should be:

- digital services by default (not the conversion of offline services into digital format, but the “birth” of digital services);
- Platform independence and focus on mobile devices;
- User-centered service design;
- Digital from start to finish;
- Government as a platform;
- implementation of a data-driven strategy;
- promoting the use of open data;
- use of open standards and open-source software;
- openness to innovation and “disruptive” technologies.

Countries that are going through the digital transformation and building the digital economy are adopting a fully "digital" and "smart" government, rather than an electronic one. The key difference between e-governance and digital governance is the shift from providing online public services to a data-driven approach. User-centered digital services require horizontal integration and interaction between different government agencies. The digital government initiatives often also involve changes in the organization of governance.

To follow the same path of digital development as all the countries that have declared the construction of a digital economy as a paradigm for their own development, it is necessary to develop a legal framework for digital governance as data-driven governance. A simple "upgrade" of already outdated e-government approaches will not work; innovative regulatory measures and an ecosystem approach are needed.

## Section 3. Digital governance objects

### Content

The legal regime of the following digital governance objects:

- electronic messages
- records
- documents
- information resources
- information systems, including distributed (blockchain)
- technological systems (data centers)
- telecommunication networks
- applications
- digital services, including public and municipal services

### Current regulation (existing legislation):

1. Law of the Kyrgyz Republic “On e-Government”
2. Electronic Signature Law of the Kyrgyz Republic
3. Innovation Activities Law of the Kyrgyz Republic
4. Virtual Assets Law of the Kyrgyz Republic
5. E-Commerce Law of the Kyrgyz Republic
6. Law of the Kyrgyz Republic “On Telecommunications and Postal Service”
7. Law of the Kyrgyz Republic "On Access to Information Held by State Bodies and Local Self-Governments of the Kyrgyz Republic.”
8. Public Procurement Law of the Kyrgyz Republic
9. Law of the Kyrgyz Republic “On Personal Information”
10. Law of the Kyrgyz Republic “On Biometric Registration of Citizens of the Kyrgyz Republic”
11. Law of the Kyrgyz Republic “On National Security Agencies of the Kyrgyz Republic”
12. Decree of the Kyrgyz Republic Degree “On the National Development Program of the Kyrgyz Republic to 2026” dated October 12, 2021, UP No.435
13. Decree of the Kyrgyz Republic President “On Further Measures of Digital Transformation of the Kyrgyz Republic”, dated July 21, 2021, UP No.305
14. Decree of the Kyrgyz Republic President “On Urgent Measures to Enhance the Implementation of Digital Technologies in Public Administration of the Kyrgyz Republic”, dated December 17, 2020, UP No. 64
15. Resolution of the Kyrgyz Republic Cabinet of Ministers “On Approval of the Action Plan of the Kyrgyz Republic Cabinet of Ministers to Implement the National Development Program of the Kyrgyz Republic to 2026” dated December 25, 2021, No. 352
16. Resolution of the Kyrgyz Republic Cabinet of Ministers “On the creation of the state institution “Project Office” dated August 16, 2021, No. 137
17. Resolution of the Government of the Kyrgyz Republic “On Approval of the Rules for Use of the State Portal of Electronic Services” dated October 7, 2019, No. 525
18. Resolution of the Kyrgyz Republic Government “On Approval of the Requirements for the Protection of Information contained in the Databases of State Information Systems”, dated November 21, 2017, No. 762
19. Resolution of the Kyrgyz Republic Government “On Approval of the Regulations of the State Electronic Payment System”, dated October 7, 2019, No. 709
20. [Resolution of the Kyrgyz Republic Government “On Approval of the Requirements for the Interaction of the Information Systems in the Tunduk Interagency Electronic Interaction System, dated April 11, 2018, No. 200](#)

21. [Resolution of the Kyrgyz Republic Government “On Implementation of the Pilot Project “State as a Platform” to Introduce the Innovative Ways of Providing Public and Municipal Services”, dated February 25, 2020, No. 113](#)
22. [Resolution of the Kyrgyz Republic Government “On Certain Issues Related to the Use of e-Signature”, dated December 31, 2019, No. 742](#)
23. [Resolution of the Kyrgyz Republic Government “On Approval of the Regulation on the State System of Electronic Communications and the Rules for its Use” dated December 31, 2019, No. 745](#)
24. Resolution of the Kyrgyz Republic Government “On Approval of the Regulations on the Automated Information System “State Electronic Document Management System” dated October 30, 2020, No. 526
25. Resolution of the Kyrgyz Republic Government “On the Model Instructions for Paperwork in the Kyrgyz Republic” dated March 3, 2020, No. 120
26. Resolution of the Kyrgyz Republic Government “On Some Issues Related to the State Information Systems” dated December 31, 2019, No. 744
27. Resolution of the Kyrgyz Republic Government “On Approval of the Requirements for the State Data Processing Centers and Communication Channels Connecting Them” dated December 31, 2019, No. 747
28. Resolution of the Kyrgyz Republic Government “On Certain Issues of E-Governance in the Kyrgyz Republic” dated December 31, 2019, No. 748
29. [Resolution of the Kyrgyz Republic Government “On Some Issues Related to the e-Governance State Infrastructure” dated December 5, 2019, No. 661](#)
30. [Resolution of the Kyrgyz Republic Government](#) “On Certain Issues Related to Basic State Information Resources” dated February 6, 2020 No. 66
31. Order of the Kyrgyz Republic Cabinet of Ministers dated July 2, 2021, No. 74-r
32. Order of the Kyrgyz Republic Cabinet of Ministers dated January 12, 2022, No. 2-r
33. The digital transformation concept “Digital Kyrgyzstan 2019-2023”

#### Brief description of the identified shortcomings and international practice benchmarks

No.	Description of the shortcoming	Type <sup>6</sup>	Best practice
3.1	The existing legislation does not create conditions for digital governance, that is, the data-driven governance. Data from the government information systems are not used for decision-making and analytics in either the public or private sectors. Each agency works with its own data set, not in coordination with other agencies - different methods of data formation are used, with a different understanding of the data composition, and these data are not fundamentally reconciled with each other. Most of the GIS is document-based: as a rule, the systems store documents in Word format or scanned manually signed pdf documents, and not the data to which	N	The World Bank's Data for a Better Life Report (2021) notes that as the amount of shared and reused data (especially personal data) increases, the potential public benefits of the improved public policy and service delivery may increase rapidly, but the risks of data abuse will also increase. These potential benefits depend on a factor such as data distribution or exchange between the parties. However, in order for parties to voluntarily engage in this process, they should trust the systems, rules, and institutions that govern the security of such exchanges. How can people be assured that their data will be protected and that they will get

<sup>6</sup> The following types of regulatory deficiencies are listed in the table:

- (G) regulatory gap (regulation is required but is missing)
- (O) obsolete provision (the existing provision should be changed)
- (N) non-working provision (the existing provision is non-working for the reasons described)
- (B) this provision is an unreasonable barrier to the implementation of activities

	these documents are linked - it is almost impossible to work with such data.		their share of the value that data can create? The growth of such fears suggests the need for a new social contract regarding data, i.e., an agreement among all those involved in the creation, sharing, and reuse of data that fosters confidence that they will not be harmed and will receive a fair share of the value that the data will create
<b>3.2</b>	The multi-level model of the regulation of the relations depending on their object (infrastructure, applications, data, services) enshrined in Article 18 of the E-Governance Law of KR applies only to the public sector and, moreover, is not reflected in other KR legislative acts, including those adopted later. The multi-layered nature of relations within the digital economy is a fact that cannot be ignored in the regulation of the relations in this area.	<b>N</b>	This problem is specific to the KR legislation and is caused by the fact that other legal acts have not been harmonized with the E-Government Law of the KR
<b>3.3</b>	There is no legal regime for distributed information systems in the KR legislation.	<b>O</b>	In general, the existing legal regulation of the information systems creation and operation can be considered as established. An information system is a basic concept used in various branches of law, and the scope of this concept is not controversial. At the same time, the concept and classification of types of information systems require further development to reflect the development of relations in this area, primarily the emergence of so-called distributed registries and the active creation of information systems in public-private partnerships.
<b>3.4</b>	The Kyrgyz Republic does not provide for the transition from electronic document management to the records-based management in the information systems, which is necessary for a digital economy. Besides, the legislation does not create conditions for using records in information systems for legally significant purposes either.	<b>G</b>	First, it is necessary to distinguish between the information and data, the regulation of which is related to the content of the information. Further, a qualified form of information should be recognized as a record, that is, information stored and transmitted in electronic or another form, suitable for storage, processing, and transmission, including in the information systems, through telecommunications networks, and the Internet. It is necessary to introduce the "record" concept into the basic information law so that it can be applied to different legal relations, including civil legal relations, in which new information

		<p>technologies appear. Here, it is also necessary to draw on the experience of foreign countries, primarily the United States, in the transfer of information in certain areas into the electronic records form (rather than documents), for example, in the health care. This has dramatically increased the availability and connectivity of the accumulated information by lowering the requirements for its details. The definition of records is associated with the need to regulate the processing (storage, transfer) of specific units of information, including the establishment of procedures to restrict access to information whose distribution is prohibited, the adoption of measures to ensure the proper protection of information. The new concept of "record" is the most appropriate for use in a digital environment.</p> <p>Moreover, the introduction of the "record" concept will change the approach to defining the "document" concept, necessary firstly to maintain the continuity of regulation with the rules of circulation of documents on paper and secondly, to create conditions for the circulation of electronic documents along with documents on paper without loss of legal force of either type of document.</p>
<p><b>3.5</b></p>	<p>There are no provisions enabling the exclusive digital interaction, which does not allow a full transition to digital interaction since government agencies require paper documents.</p> <p>There are no standards for the electronic document flow or circulation of digital records.</p> <p>The issues of electronic document flow with non-governmental organizations and individuals who could send e-mails to state bodies and receive answers have not been resolved, and entire industries are cut off from the electronic document flow and cannot fully participate in the exchange of electronic correspondence.</p> <p>Existing provisions are aimed only at regulating the electronic document flow in the public sector, while there are no</p>	<p><b>G</b></p> <p>Standardization in the field of EDMS can significantly help to establish interdepartmental and inter-corporate interaction, especially if the state authorities insist on the compliance of the software to be procured to such standards. Functional requirements for the electronic document management systems (in our terminology - electronic document management systems) are developed mainly in the interests of state authorities. Such requirements serve as a benchmark (and sometimes as a mandatory requirement) in procurement, which allows for maintaining a unified technical policy in the public sector and creating the necessary conditions for interagency cooperation. Simply put, the use of these kinds of requirements is an opportunity for the state to solve a number of serious</p>

<p>standards that would enshrine the possibility of interaction between private information systems on the document management with public ones.</p>	<p>problems at the expense of EDMS vendors, thereby saving a lot of money. Overseas, requirements for electronic document management systems began to appear in the early 1990s. Now standards of this kind exist in the United States, England, Germany, Austria, Norway, Holland, Australia, and many other countries. In 2007–2008, the requirements for the third generation EDMS began to appear, starting with the 3rd edition of the well-known American standard DoD 5015.2. The most notable event was the release in February 2008 of the European MoReq2 requirements developed by order of the European Commission (the European Union government). Currently, based on MoReq2, Slovenia and the Czech Republic developed their own national standards, and Ukraine is developing a similar standard under the MOREQ-UA project.</p> <p>International experience shows that the use of EDS pays off when dealing with sensitive electronic documents. The use of EDS for less important documents (including internal correspondence, which is exchanged within the secure corporate EDMS) is considered unjustified. The use of EDS when working with documents of permanent and long-term (more than 7-10 years) is currently not recommended, since the technology to ensure the long-term verifiability of EDS has not yet been finalized.</p> <p>Experience also shows that in order to automate mass mailings of notices and other similar documents, it is necessary, if possible, to abandon the use of original signatures and stamps on such documents. In this regard, the EU experience is interesting, where the relevant European directives prohibit national governments from requiring personal signatures on electronic invoices and bills.</p> <p>The authenticity and integrity of documents are promoted by adherence to the relevant standards and the "good business practice" rules. It is now possible to find foreign standards for almost all aspects of electronic document management.</p>
--	---

			<p>Today, there are two main methods of electronic document storage (which can also be used in combination). The first method involves storing documents on removable media, preferably single-entry WORM media (CD, DVD, etc.). With the second method, online documents are stored in electronic document management systems or electronic archives (EA). In this case, integrity and authenticity protection is provided by means of EDMS/EA.</p> <p>In other countries, there is a lot of experience in state regulation to ensure the quality and compatibility of software and hardware purchased by government agencies both for internal use and to solve problems within the "e-government" program. Especially noteworthy are the standards of functional requirements for EDMS (in the US this is DoD 5015.2, in Europe - MoReq2).</p>
<p><b>3.6</b></p>	<p>The Electronic Governance Law Kyrgyz Republic stipulates that the creation, development and operation of state e-governance infrastructure shall be subject to the requirements envisaged by the <a href="#">Public Procurement Law of the Kyrgyz Republic</a>, which creates difficulties in the procurement of information systems. As a result of this, suppliers may implement information systems that do not fully meet the requirements. The legislation does not provide for any procedure for the development and commissioning of non-state information systems at all.</p>	<p><b>B</b></p>	<p>The problem of correlation between the information legislation and the public procurement legislation has generally been resolved in the Russian Federation, where public and municipal information systems are created and put into operation following appropriate procedure (a by-law approved by the government). Besides, there is a coordination mechanism for the creation of state information systems at the relevant ministry.</p>

### Comments

To build an information society and consolidate efforts of the government agencies, business and civil society aimed at accelerating the digital transformation and socioeconomic development of the country, as the most important task, the government agencies and LSG bodies adopted the digital transformation concept "Digital Kyrgyzstan 2019-2023". According to the Concept roadmap, the state authorities are implementing various activities and projects aimed at building digital infrastructure, improving human capacity, and re-engineering the government interaction and management processes.

The main gap in the current Kyrgyz Republic on digital governance objects is that it does not create proper conditions for digital governance, that is, data-driven governance. Data are now a dead weight in state information systems. They are not used for decision-making and analytics in either the public or private sectors. Each agency works with its own data set, not in coordination with other agencies - different methods of data formation are used, with a different understanding of the data composition, and these data are not fundamentally reconciled with each other. Most of the GIS is document-based: as a rule, the systems store documents in Word format or scanned manually signed pdf

documents, and not the data to which these documents are linked - it is almost impossible to work with such data.

The World Bank's Data for a Better Life Report (2021) notes that as the amount of shared and reused data (especially personal data) increases, the potential public benefits of the improved public policy and service delivery may increase rapidly, but the risks of data abuse will also increase. These potential benefits depend on a factor such as data distribution or exchange between the parties. However, in order for parties to voluntarily engage in this process, they should trust the systems, rules, and institutions that govern the security of such exchanges.

How can people be assured that their data will be protected and that they will get their share of the value that data can create? The growth of such fears suggests the need for a new social contract regarding data, i.e., an agreement among all those involved in the creation, sharing, and reuse of data that fosters confidence that they will not be harmed and will receive a fair share of the value that the data will create. Legal systems and public administration, in general, can be regarded as tools for shaping, facilitating implementation, and monitoring compliance with social contracts. It is not easy to convince parties to adhere to the social contract rules, and the solution depends on whether there is a fair distribution of the benefits associated with the use of the data; in other words, everyone has something to gain. In this process, the lower-income countries too often get into a disadvantaged situation because they often lack the infrastructure and skills needed to collect data and turn them into value, the institutional and regulatory systems needed to build trust in the data collection and processing system, or the scope of activities and organizational structures that ensure equitable participation in the operation and management of the global data markets. The sophisticated data management system allows countries to fully enjoy the social and economic value of the public and private data and use their synergies. This requires building trust in the reliability of the data collection, processing and storage system, along with ensuring fair distribution of benefits.

Robust regulatory frameworks that include both safeguards and enforcement tools can help maintain trust in data transactions. The security mechanisms increase confidence in data transactions because they prevent or limit the damage caused by data abuse. Information security is the most important prerequisite for trust in systems for data collection, processing and storing. To achieve an appropriate level of information security, it is necessary to form a legal framework that obliges data holders and processors to implement the technical data protection systems. To date, only a small minority of low- and middle-income countries have adequate legal frameworks for information security. Kenya, with its new Data Protection Law, gives a good example of a comprehensive information security law that stands out against this background.

Creating a proper legal framework for data protection is also of paramount importance. These frameworks should clearly distinguish between personal data (personally identifiable data) and non-personal data (data containing no personally identifiable information). Among the middle-income countries with relatively well-developed personal data protection mechanisms, Mauritius stands out. In fact, it was the first Sub-Saharan African country to ratify the "Convention 108+" (the European Council Convention for Protection of Individuals in the Automatic Processing of Personal Data). The implementation tools facilitate data access and reuse within and across different stakeholder groups to ensure that the full socioeconomic value of the data is gained. There are marked differences between public and private data in the nature and scope of data-sharing provisions. Much work has been done globally to ensure the secure disclosure of public data through open data policies (they encourage the advance publication of public data) and laws governing access to information (they give citizens a legally enforceable right to request the information disclosure). However, for an open data policy to have a real impact, it should be based on a single data privacy protocol coupled with interoperable technical standards, machine-readable formats, and open licenses that facilitate subsequent data reuse. All the above are missing in the Kyrgyz Republic legislation.

Digital interaction, that is, interaction in digital form using the electronic documents and records, enables simplifying the procedure for official interaction between state bodies, local governments, their structural divisions and officials, and facilitates recording the incoming and outgoing correspondence and monitoring the performance discipline.

The electronic document management is currently based on the Automated Information System “State Electronic Document Management System”, which was created in accordance with the KR Government Resolution “On Approval of the Regulations on the Automated Information System “State Electronic Document Management System” dated October 30, 2020, No. 526.

The E-Government Law of the Kyrgyz Republic provides for electronic documents in the interaction of the e-governance participants, which is provided for in Article 1 of the Law, and was directly legalized in articles of the above-mentioned law. Article 16 of the same law establishes the cases and procedures for the electronic documents exchange.

Among other things, electronic documents should have appropriate features, which are provided by signing the document with an electronic signature in accordance with the Electronic Signature Law of the Kyrgyz Republic. According to the above Law, the electronic information signed with the appropriate electronic signature is recognized as an electronic document, equivalent to a paper document signed with a handwritten signature, except for cases when laws or other regulatory legal acts prohibit drawing up such a document in electronic form. It is also established that an electronic document signed with an electronic signature cannot be considered invalid only on the grounds that the signature in the electronic document is not handwritten.

Activation of the process of introducing the electronic document management was provided for in the Digital Transformation Concept “Digital Kyrgyzstan 2019-2023”, and the need to introduce electronic document management was reflected in the Roadmap for implementation of the Digital Transformation Concept “Digital Kyrgyzstan 2019-2023”, approved by Order of the Kyrgyz Republic Government dated February 15, 2019, No. 20-r.

Activities of the “Roadmap” for the implementation of electronic document management should have been completed in December 2020, and in December 2021 the electronic document management system should have been introduced in the judiciary bodies.

However, the active implementation of the system began only as part of measures to counter the spread of COVID-19 in the Kyrgyz Republic when many government agencies started working remotely, and a state of emergency was declared in Bishkek and Osh cities.

Meanwhile, the introduction and dissemination of electronic document management in the context of COVID-19 was not supported both at the state agencies level and at the managerial level. The state bodies still prefer paper document management.

Due to the social and political upheaval of October 2020 and the subsequent changes in the structure of the executive branch, and optimization of state enterprises, the process of implementing electronic document management stopped. However, prior to the active phase of the transition to electronic document management, efforts were taken to update the documentation in the area of document management. Thus, a new Model Instruction on Office Administration in the Kyrgyz Republic was developed and approved by Resolution of the Kyrgyz Republic Government dated March 3, 2020, No. 120.

At the same time, despite the measures taken, the government agencies, after going offline, began to return to the paper document management because they are more used to it, as well as the low degree of traceability and control by the responsible persons. This situation required a regulatory correction: Decree of the Kyrgyz Republic President "On Urgent Measures to Enhance the Introduction of Digital Technologies in Public Administration of the Kyrgyz Republic" dated December 17, 2020, UP No. 64 established the need for the widespread introduction of electronic document management in state agencies.

The main problem in the implementation of electronic document management and rejection of paper is still the high bureaucratization of state bodies and the low level of understanding by government authorities of the benefits of electronic document management for them.

Thus, the introduction of electronic document management has stopped because of the "human factor", including the habitual paperwork. Bringing the information relations legal regulation into the system requires differentiation of regulation depending on the information processing form and methods. Information as a subject of the legal relations participants' activity may have a variety of forms.

First, it is necessary to distinguish between the information and data, the regulation of which is related to the content of the information. Further, a qualified form of information should be recognized as a record, that is, information stored and transmitted in electronic or another form, which is suitable for storage, processing, and transmission, including in the information systems, through telecommunications networks, and the Internet.

It is necessary to introduce the "record" concept into the basic information law so that it can be applied to different legal relations, including civil legal relations, in which new information technologies appear. Here, it is also necessary to draw on the experience of foreign countries, primarily the United States, in the transfer of information in certain areas into the electronic records form (rather than documents), for example, in the health care. This has dramatically increased the availability and connectivity of the accumulated information by lowering the requirements for its details. The definition of records is associated with the need to regulate the processing (storage, transfer) of specific units of information, including the establishment of procedures to restrict access to information with prohibited distribution and the adoption of measures to ensure the proper protection of information. The new concept of "record" is the most appropriate for use in a digital environment.

Moreover, the introduction of the "record" concept will change the approach to defining the "document" concept, which is necessary, first, to maintain the continuity of regulation with the rules of circulation of documents on paper, and second, to create conditions for the circulation of electronic documents along with documents on paper without loss of legal force of either type of documents.

A document is a record that contains details that allow it to be identified. The document regulation should be associated with the definition of requirements for document requisites and other circumstances determining its legal value and document processing, including storage. The document as a qualified record may have legal value in various legal relations, including expressing the content of transactions and other willful or powerful acts.

One of the main problems in transition is now becoming the archive legislation, which provides for the storage of documents that are suitable for paper documents storage. There is no procedure for storing electronic documents and electronic information.

In general, the existing legal regulation of the information systems creation and operation can be considered as established. An information system is a basic concept used in various branches of law, and the scope of this concept is not controversial. At the same time, the concept and classification of types of information systems require further development in order to reflect the development of relations in this area, primarily the emergence of so-called distributed registries, as well as the active creation of information systems in public-private partnerships.

Legislation should define the legal regime for such type of information system as a distributed information system and its operator. These changes are necessary to regulate relations connected with the circulation of digital rights arising from the adoption of the Virtual Assets Law of the Kyrgyz Republic Law.

It is proposed that the operator of the distributed information system (the information system in which the creation, processing, including storage of information contained therein is performed using or by means of hardware belonging to users of such a system) is a person who independently or jointly with other persons established the procedure for processing the information contained therein using the hardware of users of such information system. Besides, to reflect the essence of the distributed information systems, it is necessary to define the distributed information system node operator as a participant of the information system, who is not the entire information system operator but provides the identity of information in this information system through the algorithms specified in it.

In addition to the state information system, the legislation should also define the joint (public-private, municipal-private) information systems created and operated on the basis of agreements between the state or municipal bodies and private individuals. Such systems will enable public functions on the infrastructure shared with private entities, thus reducing the cost of the information infrastructure development.

To streamline relations in the use of information systems, it is necessary to fix the presumption of reliability of the information contained in the state information systems and the obligation of the

system operators to ensure such reliability. Special acts may establish procedures for eliminating discrepancies between the information contained in different state information systems.

The E-Governance Law stipulates that the information systems, data centers, and other elements are included in the state e-governance infrastructure:

1) with regard to elements commissioned prior to the entry into force of this law - on the basis of an act of the Kyrgyz Republic Government;

2) with regard to elements that are commissioned in accordance with this law - on the basis of an act of the Kyrgyz Republic Government.

This method of inclusion of elements into the state e-governance infrastructure is ineffective and bureaucratic. Each inclusion involves many stages of approval by government agencies.

It is necessary to approve the requirements for inclusion in the state e-governance infrastructure, which will be stipulated in the e-governance infrastructure Registry, where after meeting certain parameters, they will be included in the state e-governance infrastructure.

Besides, the law stipulates that the creation, development, and operation of the state e-governance infrastructure shall be subject to requirements envisaged by the [Public Procurement Law of the Kyrgyz Republic](#), which creates difficulties in the procurement of information systems. As a result, suppliers may introduce information systems that do not fully meet the requirements.

Thus, the government agencies face big problems:

- if the developer is a foreign supplier who may not know the e-governance structure and may create an information system that cannot be upgraded;
- the developer creates systems based on paid licenses, and the state body will not be able to pay fees for lack of budget;
- the developer does not transfer the source codes to the state body, as this was not envisaged by the contract;
- ToR is drawn up incorrectly, as the state body does not understand the technical part. The result is a system that is difficult to operate and maintain.

Therefore, to avoid such problems, it is necessary to establish that for the creation and operation of the state information systems, direct agreements should be signed with state-owned enterprises that have experience in developing the information systems. It should be noted that the problem of correlation between the information legislation and public procurement legislation has generally been resolved in the Russian Federation, where public and municipal information systems are created and put into operation following the appropriate procedure (a by-law approved by the government). Besides, there is a coordination mechanism for the creation of state information systems at the relevant ministry.

## Section 4. Digital governance subjects

### Content

#### Digital governance subjects

- operators of technological systems
- information system operators
- telecommunications operators
- service providers
- digital platforms and ecosystems
- outsourcers (processors)
- information resource owners
- data principals (persons to whom the data relate - personal data subjects, industrial data sources, etc.)
- data and service users (professional users and end users)

#### Current regulation (existing legislation):

1. E-Governance Law of the Kyrgyz Republic
2. Electronic Signature Law of the Kyrgyz Republic
3. Innovation Activities Law of the Kyrgyz Republic
4. Virtual Assets Law of the Kyrgyz Republic
5. E-Commerce Law of the Kyrgyz Republic
6. Law of the Kyrgyz Republic “On Telecommunications and Postal Service”
7. Law of the Kyrgyz Republic “On Access to Information Held by State Bodies and Local Self-Governments of the Kyrgyz Republic.”
8. Public Procurement Law of the Kyrgyz Republic
9. Law of the Kyrgyz Republic “On Personal Information”
10. Law of the Kyrgyz Republic “On Biometric Registration of Citizens of the Kyrgyz Republic”
11. Law of the Kyrgyz Republic “On National Security Agencies of the Kyrgyz Republic”
12. Decree of the Kyrgyz Republic President “On the National Development Program of the Kyrgyz Republic to 2026” dated October 12, 2021, UP No.435
13. Decree of the Kyrgyz Republic President “On Further Measures of Digital Transformation of the Kyrgyz Republic”, dated July 21, 2021, UP No.305
14. Decree of the Kyrgyz Republic President “On Urgent Measures to Enhance the Implementation of Digital Technologies in Public Administration of the Kyrgyz Republic”, dated December 17, 2020, UP No. 64
15. Resolution of the Kyrgyz Republic Cabinet of Ministers “On Approval of the Action Plan of the Kyrgyz Republic Cabinet of Ministers to Implement the National Development Program of the Kyrgyz Republic to 2026” dated December 25, 2021, No. 352
16. Resolution of the Kyrgyz Republic Cabinet of Ministers “On the creation of the state institution "Project Office" dated August 16, 2021, No. 137
17. Resolution of the Government of the Kyrgyz Republic “On Approval of the Rules for Use of the State Portal of Electronic Services” dated October 7, 2019, No. 525
18. Resolution of the Kyrgyz Republic Government “On Approval of the Requirements for the Protection of Information contained in the Databases of State Information Systems”, dated November 21, 2017, No. 762
19. Resolution of the Kyrgyz Republic Government “On Approval of the Regulations of the State Electronic Payment System”, dated October 7, 2019, No. 709
20. [Resolution of the Kyrgyz Republic Government “On Approval of the Requirements for the Interaction of the Information Systems in the Tunduk Interagency Electronic Interaction System, dated April 11, 2018, No. 200](#)
21. [Resolution of the Kyrgyz Republic Government “On Implementation of the Pilot Project “State as a Platform” to Introduce the Innovative Ways of Providing Public and Municipal Services”, dated February 25, 2020, No. 113](#)
22. [Resolution of the Kyrgyz Republic Government “On Certain Issues Related to the Use of e-Signature”, dated December 31, 2019, No. 742](#)
23. [Resolution of the Kyrgyz Republic Government “On Approval of the Regulation on the State System of Electronic Communications and the Rules for its Use” dated December 31, 2019, No. 745](#)
24. Resolution of the Kyrgyz Republic Government “On Approval of the Regulations on the Automated Information System “State Electronic Document Management System” dated October 30, 2020, No. 526
25. Resolution of the Kyrgyz Republic Government “On the Model Instructions for Paperwork in the Kyrgyz Republic” dated March 3, 2020, No. 120
26. Resolution of the Kyrgyz Republic Government “On Some Issues Related to the State Information Systems” dated December 31, 2019, No. 744

27. Resolution of the Kyrgyz Republic Government "On Approval of the Requirements for the State Data Processing Centers and Communication Channels Connecting Them" dated December 31, 2019, No. 747
28. Resolution of the Kyrgyz Republic Government "On Certain Issues of E-Governance in the Kyrgyz Republic" dated December 31, 2019, No. 748
29. [Resolution of the Kyrgyz Republic Government "On Some Issues Related to the e-Governance State Infrastructure" dated December 5, 2019, No. 661](#)
30. [Resolution of the Kyrgyz Republic Government](#) "On Certain Issues Related to Basic State Information Resources" dated February 6, 2020 No. 66
31. Order of the Kyrgyz Republic Cabinet of Ministers dated July 2, 2021, No. 74-r
32. Order of the Kyrgyz Republic Cabinet of Ministers dated January 12, 2022, No. 2-r
33. The digital transformation concept "Digital Kyrgyzstan 2019-2023"

## Brief description of the identified shortcomings and international practice benchmarks

No.	Description of the shortcoming	Type <sup>7</sup>	Best practice
4.1	In the current legislation, there is no system of key digital governance actors (subjects), which does not allow building relations in the digital environment as a system. At the same time, the status of each of these actors should be defined as part of the regulation of the relevant type of activity in the digital economy.	G	This gap is caused by the non-systematic development of the digital economy legislation in the KR, in particular, the adoption of the E-Commerce Law of the Kyrgyz Republic without consideration of provisions of the already existing E-Governance Law of the KR. To prevent such conflicts in future, codification of the digital governance legislation is required.
4.2	In the digital economy, the emerging new actors, such as the digital platforms or ecosystems owners, remain invisible to the sector and antimonopoly laws, which fail to prevent significant market power in the hands of these actors and, as a result, cannot address economic inequality. First of all, effective digital governance requires regulation of such new entities' activity on a cross-industry basis.	G	Currently, the system of regulation of digital economy actors' activity is developed as part of the EU Digital Single Market strategy and should be included in two basic EU acts - on the digital market and digital services. These acts imply comprehensive regulation of digital platforms in the EU.

### Comments

The KR legislation requires a serious upgrade in terms of regulating the activities of fundamentally new subjects - so-called "champions of the digital economy" or digital platforms. To follow the same path of digital development as all the countries that have declared the digital economy as their development paradigm, it is necessary to develop a legal framework for digital governance - as a data driven governance. A simple "upgrade" of the outdated e-governance approaches will not work; innovative regulatory measures and an ecosystem approach are needed. Here, it is worth paying attention, first of all, to the European experience. For years, digital market regulation has been a key priority in Europe. In 2015, the European Commission committed the EC to create a single digital market, and that commitment resulted in a variety of initiatives and regulatory amendments affecting the digital goods and services providers and users. Even among the EU member states, standards for digital regulation have varied - and continue to vary – with many issues left to the local governments' consent. And in 2016, the UK voted to leave the EU, which will lead to further divergence in digital regulation across Europe.

In the course of the ongoing evolution of the European digital regulation, the digital compliance process has become a much higher priority for any organization providing or consuming digital goods and services in Europe. As digital technologies evolve, it becomes increasingly difficult for organizations to ensure compliance continuously. In December 2020, the European Commission published two major proposed bills aimed at implementing the EU's digital strategy. Together, the Digital Services Act (DSA) and the Digital Markets Act (DMA) are designed to create a more secure digital space and create equal conditions for stimulating innovation and growth both in the EU and around the world.

The DSA, as one-half of this legislative package, focuses on regulating the digital service providers, or "intermediaries." It aims to address the dominance of "very large" platforms (covering

<sup>7</sup> The following types of regulatory deficiencies are listed in the table:

- (G) regulatory gap (regulation is required but is missing)
- (O) obsolete provision (the existing provision should be changed)
- (N) non-working provision (the existing provision is non-working for the reasons described)
- (B) this provision is an unreasonable barrier to the implementation of activities

more than 10% of 450 million consumers in Europe) and companies' responsibility for the third-party content. The DSA violations may entail single-time fines of up to 6% of the annual global turnover or recurring fines of no more than 5% of the average daily turnover. It is important to note that the DSA will apply to any provider offering its services to users in the EU. Intermediaries regulated by the DSA will have different obligations depending on their role, size and impact on the online ecosystem. Digital platforms will be responsible for the elimination of the illegal content, fulfilling transparency obligations, and additional verification. The DSA seeks to complement and develop the EU E-Commerce Directive, while harmonizing the regulation across the EU and clarifying issues such as responsibility for the third-party content.

Once in force, the DSA and DMS will be effective throughout the EU and therefore will not require national implementation by each member state.

The second part of the above EU legislative duo is the Digital Markets Act (DMA). The DMA will target “gatekeepers”- the core platforms that act as a gateway between business users and customers. The proposed rules express concerns about the “entrenched and strong” position of such platforms, which as the EU believes, lead to unfair practices and lack of competition, resulting in higher prices, lower quality and less innovation in the digital economy.

A base platform provider will be considered a “gatekeeper” if it:

- has a significant impact on the EU internal market (currently, the annual turnover of the EEA exceeds 6.5 billion Euros over three years or the fair market value of the company or its parent company is 65 billion Euros);
- manages one or more important customer gateways (there are currently more than 45 million end users in the EU and more than 10,000 active business users per year); and
- uses, or is expected to hold a strong and lasting position in its activities.

While the DMA draft sets these thresholds assuming that a supplier is a gatekeeper, it also allows the European Commission to assign the gatekeeper status based on other assessments.

Among other things, gatekeepers:

- should comply with the new data exchange rules;
- should allow their own software and applications to be removed from the hardware and allow business users to sign contracts with end users outside of the gatekeeper platform;
- will be prohibited from promoting their own products over other business users.

The DMA comes at a time when several EU member states are discussing or have already adopted new regulations, also aimed at regulating gatekeepers or "big digital companies" more generally, in order to ensure that the relevant markets remain open and competitive (for example, the German UPSCAM regulation, which came into force in January 2021). Given that the DMA claims to be the only tool providing such regulation throughout the EU, it remains to be seen how its relationship with these national regimes will ultimately be established.

After Brexit, the UK will not observe the DSA or the DMA. But the UK is also seeking to change the way digital markets are regulated, which likely means trying to achieve the same goal as the EU in terms of regulating the "big technological" companies.

A number of key UK regulators (the Competition and Markets Authority (CMA), the Information Commissioner's Office, the Financial Supervision Office and Ofcom) joined their efforts to advise on the UK strategy for regulating the digital markets. They jointly represent the British Digital Task Force, which has published its first advisory document.

The regulatory regime proposed by the Digital Task Force includes a legally binding code of conduct (with different rules for different types of companies), competition protection measures (including such protection measures as mobility and personal data interoperability) and enhanced merger rules, all to be overseen by the new Digital Markets Unit (DMU) based at the CMA. The UK government established the DMU in April 2021 and committed to hold consultations on the competition encouraging regime later in 2021, to be able to regulate large global digital technology providers by 2022.

The Digital Task Force mode targets the digital companies with the "strategic market status" (SMS), which will be determined by the evidence-based assessment. This reflects the EU strategy (as described above) targeting those companies deemed to have the entrenched market power. But unlike

the EU approach, the UK Digital Task Force suggests that such an SMS assessment should be applied to a company's specific activity, not to the company as a whole.

While the Digital Task Force envisions active operation and open and productive relationship with SMS companies, it goes further than the EU in its proposed sanctions. The Task Force recommends the United Kingdom stop the regime violations by imposing fines of up to 10% of global turnover, which is seen as an effective measure, but until it is implemented it is not yet possible to judge its effectiveness.

## Section 5. Grounds for the emergence, change, and termination of legal relations in the digital environment

### Content

- sources of information;
- smart contracts;
- results of digital services

### Current regulation (existing legislation):

1. E-Governance Law of the Kyrgyz Republic
2. Electronic Signature Law of the Kyrgyz Republic
3. Innovation Activities Law of the Kyrgyz Republic
4. Virtual Assets Law of the Kyrgyz Republic
5. E-Commerce Law of the Kyrgyz Republic
6. Law of the Kyrgyz Republic “On Telecommunications and Postal Service”
7. Law of the Kyrgyz Republic “On Access to Information Held by State Bodies and Local Self-Governments of the Kyrgyz Republic.”
8. Public Procurement Law of the Kyrgyz Republic
9. Law of the Kyrgyz Republic “On Personal Information”
10. Law of the Kyrgyz Republic “On Biometric Registration of Citizens of the Kyrgyz Republic”
11. Law of the Kyrgyz Republic “On National Security Agencies of the Kyrgyz Republic”
12. Decree of the Kyrgyz Republic President “On the National Development Program of the Kyrgyz Republic to 2026” dated October 12, 2021, UP No.435
13. Decree of the Kyrgyz Republic President “On Further Measures of Digital Transformation of the Kyrgyz Republic” dated July 21, 2021, UP No.305
14. Decree of the Kyrgyz Republic President “On Urgent Measures to Enhance the Implementation of Digital Technologies in Public Administration of the Kyrgyz Republic” dated December 17, 2020, UP No. 64
15. Resolution of the Kyrgyz Republic Cabinet of Ministers “On Approval of the Action Plan of the Kyrgyz Republic Cabinet of Ministers to Implement the National Development Program of the Kyrgyz Republic to 2026” dated December 25, 2021, No. 352
16. Resolution of the Kyrgyz Republic Cabinet of Ministers “On the creation of the state institution “Project Office” dated August 16, 2021, No. 137
17. Resolution of the Government of the Kyrgyz Republic “On Approval of the Rules for Use of the State Portal of Electronic Services” dated October 7, 2019, No. 525
18. Resolution of the Kyrgyz Republic Government “On Approval of the Requirements for the Protection of Information contained in the Databases of State Information Systems”, dated November 21, 2017, No. 762
19. Resolution of the Kyrgyz Republic Government “On Approval of the Regulations of the State Electronic Payment System” dated October 7, 2019, No. 709
20. [Resolution of the Kyrgyz Republic Government “On Approval of the Requirements for the Interaction of the Information Systems in the Tunduk Interagency Electronic Interaction System, dated April 11, 2018, No. 200](#)
21. [Resolution of the Kyrgyz Republic Government “On Implementation of the Pilot Project “State as a Platform” to Introduce the Innovative Ways of Providing Public and Municipal Services” dated February 25, 2020, No. 113](#)
22. [Resolution of the Kyrgyz Republic Government “On Certain Issues Related to the Use of e-Signature” dated December 31, 2019, No. 742](#)
23. [Resolution of the Kyrgyz Republic Government “On Approval of the Regulation on the State System of Electronic Communications and the Rules for its Use” dated December 31, 2019, No. 745](#)

24. Resolution of the Kyrgyz Republic Government “On Approval of the Regulations on the Automated Information System “State Electronic Document Management System” dated October 30, 2020, No. 526
25. Resolution of the Kyrgyz Republic Government “On the Model Instructions for Paperwork in the Kyrgyz Republic” dated March 3, 2020, No. 120
26. Resolution of the Kyrgyz Republic Government “On Some Issues Related to the State Information Systems” dated December 31, 2019, No. 744
27. Resolution of the Kyrgyz Republic Government “On Approval of the Requirements for the State Data Processing Centers and Communication Channels Connecting Them” dated December 31, 2019, No. 747
28. Resolution of the Kyrgyz Republic Government “On Certain Issues of E-Governance in the Kyrgyz Republic” dated December 31, 2019, No. 748
29. [Resolution of the Kyrgyz Republic Government “On Some Issues Related to the e-Governance State Infrastructure” dated December 5, 2019, No. 661](#)
30. [Resolution of the Kyrgyz Republic Government](#) “On Certain Issues Related to Basic State Information Resources” dated February 6, 2020 No. 66
31. Order of the Kyrgyz Republic Cabinet of Ministers dated July 2, 2021, No. 74-r
32. Order of the Kyrgyz Republic Cabinet of Ministers dated January 12, 2022, No. 2-r
33. The digital transformation concept “Digital Kyrgyzstan 2019-2023”

#### Brief description of the identified shortcomings and international practice benchmarks

No.	Description of the shortcoming	Type <sup>8</sup>	Best practice
5.1	The KR legislation needs to unify different sources of information in the form of “old” (mass media) and “new” (social media, messenger channels, etc.) media, which requires revision and codification of the activities of various media based on the general principles of freedom of speech, legality and fairness in the information distribution.	G	In the world, the information sources regulation is based on respect for freedom of speech and the need to limit the liability of information intermediaries, as is done, for example, in the US Communications Decency Act. This mechanism may be supplemented by notification as a means of rebutting the immunity of the information intermediary, when the intermediary who received the notification cannot claim that he was unaware of the illegal nature of the information distributed (or that it is fake or irrelevant)
5.2	The concept of “smart contracts” in the Virtual Assets Law and the E-Commerce Law of the Kyrgyz Republic contradict each other and limit its application due to the fact that the relevant amendments are not enshrined in the civil law, and the legal regime of a smart contract is regulated as ordinary computer SWs. It is necessary to enshrine smart contracts as the basis for the emergence, modification, termination of rights and obligations in the	N	The advanced legal systems of France, Germany, Switzerland, Belgium, Great Britain do not contain definition of a smart contract, however, blockchain technologies and smart contracts are used on the basis of traditional civil law, based on the general contract law, while Italy has legislated the smart contract concept and applies the civil law provisions directly to the regulation of legal relations arising from smart contracts.

<sup>8</sup> The following types of regulatory deficiencies are listed in the table:

- (G) regulatory gap (regulation is required but it is missing)
- (O) obsolete provision (the existing provision should be changed)
- (N) non-working provision (the existing provision is non-working for the reasons described)
- (B) this provision is an unreasonable barrier to the implementation of activities

	digital sphere, to provide a more detailed legal basis for their application.		
<b>5.3</b>	There is no legal regime for trusted services (such as guaranteed delivery or timestamp) in the KR legislation, which hinders the development of relationships in the digital economy.	<b>G</b>	The most recent best practice in the world is the UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services (TS). The law establishes a general rule on the legal recognition of TS, as well as establishes the obligations of the main participants in the relationship (TS providers, subscribers and users) and the responsibility of TS providers. The law sets the requirements for TS, which should be met to ensure their reliability, and contains provisions relating to certain types of TS: electronic signatures, electronic stamps, electronic archives, guaranteed message delivery services, website authentication services.

### Comments

The receipt of information (as a result of its distribution or access to it) is the main ground for the emergence, change, and termination of legal relations in the digital environment. The E-Governance Law of the KR already establishes that information is publicly available if access to it is not restricted by law or by the decision of the information owner. The law also prohibits distribution and publication of information aimed at propaganda of war, incitement of national, interregional, racial or religious hatred and enmity, as well as other information for which liability is stipulated by the Kyrgyz Republic Criminal Code, the Code of Offenses and the Code of Violations of the Kyrgyz Republic. First of all, this refers to the information whose dissemination, above all, violates the private interests of specific subjects and, therefore, is prosecuted by the state upon the will of the information holders and other persons who consider their rights as violated by the information dissemination.

Such information includes:

- information containing obscene language;
- personal data;
- information about a citizen's private life obtained through the civil law violation;
- information discrediting the honor, dignity and business reputation of citizens and the business reputation of organizations;
- unreliable data, the accuracy requirements for which are established by law (unreliable advertising, unreliable information about the product, etc.).

One of the significant problems of today's information society is the spread of fake news. The dissemination of such news can cause significant problems in the financial markets and lead to political and social upheaval. The fight against fake news (disinformation) requires other approaches to regulation than regulation of the restricted circulation of information. The latter requires comprehensive assessment and verification of facts to check the reliability of information, since the dissemination of false information is not directly prohibited by law and does not directly violate the rights and freedoms of specific subjects (otherwise, fake becomes the information restricted for dissemination).

Both traditional mechanisms (consideration of applications and deletion (blocking) of fake news and other mechanisms, for example, the creation of an information resource (website, application) for checking facts and denials, and implementing the media literacy programs can be used as tools to combat the dissemination of fake information, the use of new technologies (artificial intelligence) to identify fake information, changing the algorithm for generating a news feed, etc.

A significant part of the provisions regulating the infocommunication relations is addressed to the information sources. These can be Internet sites, the media, or any other organized and intended for the use of amounts of information. To regulate these relations, it is advisable to use a basic, root concept, which should be the concept of an information resource as a source of information.

Mass media and/or their certain issues (including newspapers, TV channels and other "traditional" media) should be recognized as varieties of information resources. The separation of an information resource as an independent object of regulation of information law will bring together the legal regulation of information dissemination in traditional media and in the new media, and unify approaches to determining the rights and obligations of the owners of the resources. In addition, the most important task of the information law should be to delineate the scope of responsibility of the information resource owner and the person who initiated the information dissemination. This task requires further improvement and specification of the legal status of the information intermediary, as well as the development of the concept of responsibility of the information resource for the information distributed.

The international practice in this area was established at the end of the 20th century and has proven its effectiveness. In the landmark case, *Cubby, Inc. v. CompuServe*, the court took the side of the "news board" and pointed out that while the person who published the defamatory material was, in principle, just as liable as the person who originally published the material, the news agencies, bookstores and libraries could not be held liable if they were unaware of the defamatory nature of the material. In addition, the court found that it had "roots in the First Amendment" - distributors could only be held liable if they knew the content of the publication. The court concluded that CompuServe had no more control over the content available through the firm than a library, bookstore, or newsstand, and dismissed the suit. Consequently, despite the unlawful nature of the distributed information, CompuServe acted within its subjective right, providing access to third parties' information, the content of which it had no control over. In the second case, *Stratton Oakmont v. Prodigy* - the court came to the exact opposite conclusion. The plaintiff pointed out that Prodigy's Terms of Service included a provision to remove offensive messages, so the firm should be aware of them. Besides, Prodigy uses the automatic software that scans all the message boards for offensive words and removes them if they are found. The court considered these facts distinguished the case from *Cubby v. CompuServe*.

An odd consequence of the decision in this case was that the provider that made a good-faith attempt to remove illegal content from its servers and thereby, took certain self-regulatory measures was subject to greater liability than the provider that self-removed from combating illegal content on its servers. Many providers have become fearful of the risk of unforeseen liability in this regard.

However, it is necessary to note certain logic in this court's decision: if in the *CompuServe* case, the information distributor's behavior did not differ depending on its content, in the *Stratton Oakmont* case, the assumption of the distributor's obligation to control the content - for improper performance of this obligation and the liability, was noticed.

The US lawmaker has drawn attention to the uncertainty created by the *Stratton Oakmont* decision and concluded that this uncertainty acts as a barrier to further Internet development. The consequence was the inclusion of Section 230 in the Communications Decency Act. While § 223(a) and § 223(d) of the Act, which imposed penalties for transmitting obscene or patently offensive material, increased liability for own content on the Internet, Section 230 went in the opposite direction and limited liability for the third-party content.

The central provision of Section 230 is §230(c)(1):

"No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."

In addition, Article 230(c)(2) contains the *Stratton Oakmont* case response:

"No provider or user of an interactive computer service shall be held liable on account of any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected."

That is, the US law maker was forced to specifically limit the liability of information intermediaries (to which the courts have already begun to hold them) because it felt that this would have a chilling effect on both the development of technology and freedom of speech.

But with the passage of the Communications Decency Act, it became apparent that a bias had occurred: A legal structure was needed that would still allow forcing information intermediaries to remove illegal content, even if they had not posted it and even in a situation where they could not be held liable for it. The US Digital Millennium Copyright Act made up for the missing element. Reproducing provisions of the Communications Decency Act about exemption from liability, this law provided for the possibility of sending a notice to the intermediary that he/it has something illegal on his/it server. And if the intermediary did not remove or block the illegal content in response to the notice, he/it could be held liable.

Thus, the Kyrgyz legislation, by enshrining the liability of the information intermediaries, will be in line with the global trend. Intermediaries do influence the dissemination of information, but at the same time they cannot control all the information that passes through them. And if you impose excessive burdens on them, it will only lead to a deterioration in the quality of information services, and not at all to greater control over information.

With technologies advancing, smart contracts become essential for the emergence, modification, and termination of legal relationships in the digital environment. Although this concept is already contained in the new KR legislation, the two laws that established it (on electronic commerce and on virtual assets) contradict each other, indicating a lack of understanding of the essence of this concept. Meanwhile, the term "smart contract" was first introduced by N. Szabo in 1994, who defined this phenomenon as a computerized transaction protocol that executes the terms of a contract, which is designed to satisfy common contractual conditions by the parties, minimize fraud losses, arbitration and enforcement costs, reduce the number of persons involved in the process of concluding and executing contracts. However, despite the fact that the concept of such automation of contractual relations appeared at the end of the last century, the launch of the Ethereum project in 2015, a blockchain-based platform specifically designed for the placement and execution of smart contracts, should be taken as the starting point for its actual implementation and promotion.

First of all, we note that there are two approaches to defining the concept of a "smart contract": technical and legal. Thus, in terms of functioning technology, a smart contract is a computer code designed to perform certain tasks subject to predetermined conditions. In most cases, this code is implemented in the blockchain - a type of distributed register, which is a decentralized database distributed among several network nodes, servers, users, etc. Therefore, the blockchain can be represented as a single chain of blocks of information on the confirmed transactions in relation to a certain digital asset, which are sequentially organized "through the use of cryptographic identifiers (hashes) created as a result of performing a complex mathematical calculation operation called mining, and then confirming this result by the majority of participants in the system (nodes)". The blocks within the blockchain are synchronized with each other by consensus, which means that the key principle of its operation is the partial duplication of information from each block to the next, so that a new block in the chain cannot be formed in contradiction to the previous one. Thus, the recorded information is kept unchanged, and each copy is updated with new information automatically. One of the advantages of a smart contract over a traditional contract is associated with the described principle of blockchain functioning - they minimize the risk of uncoordinated interference in their content, which guarantees greater protection of the property interests of the parties.

It is worth noting that blockchain is currently the most popular technology for the execution of smart contracts, in connection with which some researchers (e.g., Efimova LG and Sizemova O.B., Savelyev A.I.) indicate the execution of code in the blockchain as one of the semantic features of smart contracts. This is true in most cases, but given the impressive pace of scientific and technological progress, in the future it is conceivable that an alternative technology will be created for the automated performance of contract terms, recorded as a program code, which also ensures the impossibility of breach of obligation, so that the concept of defining a smart contract through blockchain or other distributed registry technology will lose its relevance. Thus, the opinion A.M. Vashkevich, pointing out

that the implementation of smart contracts is possible without a distributed registry, seems more adaptive.

The content of a smart contract is a set of conditions set out in a special programming language in the form of a code, which is subsequently "autonomously executed on multiple computers - blockchain nodes – beyond the control of the contract parties", and does not require the participation of the counterparty after its conclusion. Smart contracts can be used in various spheres of human activity (financial, real estate, administrative, intellectual property protection, etc.), but only digital assets can be disposed of through them, because "the transfer (provision) of the transaction is provided in the blockchain by linking it to a specific block of information in this system". Consequently, if the parties interact over the disposition of tangible assets, "it is necessary that the asset which is the contract subject be attached to the virtual unit operated by the software." As V. Buterin rightly notes, "the potential of smart contracts cannot be realized without cryptocurrencies." Therefore, we note that the issue of visibility of smart contracts by the Russian law directly depends on the definition of the legal status of cryptocurrency and, in the event of a complete ban on its use by civil subjects, further discussions about the legal qualification of this phenomenon lose their relevance.

To summarize, a smart contract from a technical point of view is "a piece of program code designed to perform certain tasks if a predetermined condition in the program is met." The technical side of the smart contract in the blockchain context is reflected in its definition as a type of coding, a way for the blockchain to function; as a piece of code that is implemented on a blockchain platform and is initiated by blockchain transactions, and organizes the entry of records into the database. In this sense, the smart contract can be organically built into the legal system as a program for the computer, because the smart contract is also an objective set of data and commands designed for the functioning of computers and other computer devices in order to obtain certain results. However, in this situation, a smart contract definition is limited to the framework of technological principles of its functioning, while the expression of will by the parties, aimed at the development of certain legal relations between them, is no longer covered by the smart contract concept. At the same time, the analysis of smart contracts is not limited to their consideration as a technical phenomenon: the scope of the smart contract concept to some extent covers the interaction between counterparties, because it, due to its specificity, can not be realized outside of the smart contract. In this regard, it is necessary to enshrine smart contracts as the basis for the emergence, change, termination of rights and obligations in the digital sphere to give a more detailed legal basis to its application.

It should be noted that the Kyrgyz Republic legislation lacks the legal regime of trusted (certified) services (such as guaranteed delivery or time check), which hinders the development of relations in the digital economy. The most recent best practice in the world is the UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services (TS). The draft Model Law is the result of more than a century quarter of work by UNCITRAL to create a legal environment for electronic commerce development. The Model Law provisions develop the approaches laid down in the Model Law on Electronic Commerce (MLEC) and the Model Law on Electronic Signatures (MLES). The purpose of the MLEC and MLES was to provide validation to electronic documents. They aimed to remove legal barriers to the use of electronic agreements, and to abolish the "monopoly of paper documents."

Thus, according to Article 6 (1) of the MLEC, where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference. P.1 Art. 7 of the MLEC establishes that where the law requires a signature of a person, that requirement is met in relation to a data message if:

- (a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and
- (b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

These provisions did not establish criteria for assessing the compliance of the method with the requirements listed in them, and the guarantees of legal value of electronic information (validity of the

offer, acceptance, electronic evidence) could not be applied. Therefore, a special MLES was later developed, which clarified a number of significant issues.

After its adoption, the MLES became a benchmark for legislation on electronic signatures in various countries, in particular, its approaches are used in the Russian Federal Law "On e-Signature" dated 06.04.2011, No. 63-FZ and in the Electronic Signature Law of the Kyrgyz Republic Law. The basis of the MLES approach is to give special status to the information intermediary(s) - a trusted person who could technically certify, at the request of one or both parties, that the signature was actually made by the person named as the signer of the document.

The MLES approach is further developed and strengthened in the new draft Model Law, which describes not just the status of information intermediaries, but in general, the TS infrastructure (trusted third party service) and UID as an essential element of trust in the digital economy. UNCITRAL's work is consistent with the current regulatory practice in the European Union: Directive 1999/93/EC on electronic signatures and Directive 2000/31/EC on electronic commerce. The Electronic Signatures Directive is much like the MLES in its content, but their structure is different. Whereas the MLES focuses on problems of signature validity and the rights and obligations of the parties, the Directive sought primarily to create an organizational unit for working with electronic signatures, and to establish a framework for this unit to function.

In 2014, the structure of electronic signatures regulation in the European Union was changed, and instead of directives, the Regulation was adopted, covering other identification services and trusted services in addition to electronic signatures. The regulation, in turn, is one of the elements of the European Union's digital single market strategy. The Regulation aims at the free circulation in the internal market of products and TS complying with the Regulation requirements: there should be no restriction for the TS delivery in an EU member state by a TS supplier established in another member state.

Chapter 3 of the new Model Law is entirely devoted to trust services. This chapter establishes a general rule on the legal recognition of the TS, and sets the obligations of the main participants in the relationship (TS providers, subscribers and users) and the responsibilities of the TS providers. The Chapter defines the requirements for TS, which should be complied with to ensure their reliability, and contains provisions relating to certain types of TS: electronic signatures, electronic seals, electronic archives, guaranteed message delivery services, web site authentication services.

The general approaches in the draft Model Law allow to characterize it as an example of so-called "soft laws", that is, documents that are not normative in themselves, but by virtue of the elaboration of the approaches enshrined in them and the authority of the expert community that developed them become the basis for binding rules at various levels (from international treaties to national legislation). From this point of view, the Model Law is very important for Kyrgyzstan and the Eurasian Economic Union countries, as it sets a high regulation standard for identification and authentication, which are now being actively developed in the Kyrgyz legislation and the Eurasian Economic Union documents.

## Section 6. Information legal relations

### Content

- types of information
- information dissemination, provision
- access to information
- open data
- information protection and cybersecurity (authority to adopt the information protection requirements in certain areas of relations).

### Current regulation (existing legislation):

1. E-Governance Law of the Kyrgyz Republic
2. Law of the Kyrgyz Republic "On Access to Information Held by State Bodies and Local Self-Governments of the Kyrgyz Republic"
3. Law of the Kyrgyz Republic "On Protection of State Secrets of the Kyrgyz Republic"
4. Law of the Kyrgyz Republic "On Personal Information"
5. Law of the Kyrgyz Republic "On Commercial Secret"
6. Resolution of the Kyrgyz Republic Government "On Approval of the Requirements for the Protection of Information Contained in the Databases of State Information Systems" dated November 21, 2017, No. 762
7. Resolution of the Kyrgyz Republic Government "On Approval of the Requirements for the Security and Protection of Personal Data at Their Processing in Personal Data Information Systems, the Implementation of Which Provides the Established Levels of Protection of Personal Data" dated November 21 2017, No. 760

### Brief description of the identified shortcomings and international practice benchmarks

No.	Description of the shortcoming	Type <sup>9</sup>	Best practice
6.1	The KR legislation, primarily Article 12 of the E-Governance Law of the KR treats publicly available information as a legal regime of information, opposing the confidential information. This approach is outdated, since it does not create conditions for securing a balance between the public interest in the use of information (expressed, in particular, in freedom of speech) and the rights of information holders to restrict access to it, if they have the relevant power granted by law.	O	In other countries, the public availability of information is not so much an element of the legal regime of information itself, as a consequence of the exercise of the basic human right of access to information, stipulated by Article 19 of the Universal Declaration of Human Rights and Article 19 of the International Covenant on Civil and Political Rights (New York, December 16, 1966). For example, in the United States, as a general rule, all publicly available information, including personal data, may be used without restriction, except in cases specified in the law (the principle of "permitted by default, unless otherwise provided by law"). This is based on the First Amendment to the US Constitution to protect freedom of speech. The open nature of the Internet is emphasized in US Supreme Court decisions. Such an approach, on the

<sup>9</sup> The following types of regulatory deficiencies are listed in the table:

- (G) regulatory gap (regulation is required, but it is missing)
- (O) obsolete provision (the existing provision should be changed)
- (N) non-functioning provision (the existing provision is non-functioning for the reasons described)
- (B) this provision is an unreasonable barrier to the implementation of activities

			one hand, promotes the widest possible use of information in society, and, on the other hand, does not create conditions for violation of the information holders' rights, who may restrict access to information if they are legally entitled to do so.
<b>6.2</b>	<p>In the Kyrgyz legislation (in other legal acts, except for the e-governance law), the mode of access to information is poorly structured and not systematized, which leads to significant overlaps and inconsistencies between different secret regimes, which highly complicates the use of relevant information, including such use that cannot violate the rights of persons whom this or that secret belongs to.</p> <p>To unify the legal regimes of legally protected secrets in the current legislation, it is necessary, in accordance with the Constitution provisions, to limit their application only to the following types of data:</p> <p>data constituting state secrets;  data constituting trade secret;  data constituting professional or procedural secrets;  data on a citizen's private life.</p>	<b>B</b>	<p>The US and Europe developed a system of secrets arranged both by industry (banking secrets, communications secrets) and by subject matter (trade secrets, privacy secrets), with state secrets (state secrets) designated as a separate institution. These legal regimes have a significant history of development and are designed to protect the essential interests of those to whom they apply. The basis for establishing a secrecy regime in all cases is that the disclosure of information constituting a particular secret is capable of causing harm to the person to whom the secret relates ("the secret principal").</p>
<b>6.3</b>	<p>In fact, the provision of Article 9 of the E-Governance Law that the authorized body on the electronic governance performs (among other things) the following functions: "assisting the state and local self-government bodies in the transition to e-governance, including in the development and approval by them of regulations, standards, procedures for the delivery of electronic public and municipal services, creating tools for open and accountable governance, mechanisms for using the open data models based on advanced information technology, development of methods to assess the effectiveness of the implementation of initiatives in the field of openness and accountability, creating the open data portals".</p>	<b>G</b>	<p><b>UK:</b></p> <p>Approaches to legal regulation of unification of formats for presentation of information and information exchange technologies in the state information systems are regulated by the Open Standards Principles (2018), which contain the following criteria for the selection of standards, which should:</p> <ul style="list-style-type: none"> <li>– meet user needs,</li> <li>– give suppliers equal access to government contracts,</li> <li>– support flexibility and change,</li> <li>– support sustainable cost,</li> <li>– be transparent.</li> </ul> <p>The principles ensure that future technologies will be affordable, safe and innovative. They describe how the government will define and select open standards and how those standards can be implemented in open source and proprietary software. All government departments and agencies should use these principles.</p> <p>Open standards should meet the users' needs: government users or citizens may be users.</p>

		<p>The main purpose of open standards is to allow users:</p> <ul style="list-style-type: none"> <li>● share data with the software of own choice</li> <li>● improve data clarity and consistency</li> <li>● improve the interaction between departments</li> <li>● improve the interaction between the government and citizens.</li> </ul> <p>The selection process that the government uses to determine open intergovernmental standards for IT begins with identifying user needs.</p> <p>Open standards should give suppliers equal access to government contracts: European procurement law (Article 42 of Directive 2014/24/EC) requires that technical specifications give suppliers equal access to public contracts and do not create obstacles to the opening of public procurement for competition.</p> <p>Open standards should support flexibility and change: Government agencies should share relevant data with each other in order to provide effective services to citizens. Using open formats, units can:</p> <ul style="list-style-type: none"> <li>● standardize the data, which will reduce the likelihood of storing duplicate data.</li> <li>● integrate their IT systems to improve communication and efficiency for users (flexible IT will help make the existing and new systems compatible)</li> <li>● easily transfer data and information between the old and new systems</li> <li>● make data and application programming interfaces (APIs) accessible - this allows others to create alternative, innovative representations of the government data and get access government services.</li> </ul>
6.4	<p>Information from the information systems of state bodies and local governments is actually not placed on the Internet websites of state bodies and local governments in the form of open data due to the fact that the legislation does not set the procedures (practical recommendations) for publishing open data, including on the Open Data Portal, or the requirements for technological, software and linguistic means necessary for posting information by state bodies and local self-governments on the Internet in the open data format. Besides, the law does not provide a legal basis for the use of open source software</p>	<p><b>G</b></p> <p>The Moldovan legislation contains a special Law “On Reuse of the Public Sector Information”, which obliges the state authorities and institutions to publish on the Single Government Open Data Portal, all the information accumulated and collected by public authorities and institutions, in a format that allows for automatic processing of documents and metadata.</p> <p>To implement this law, the Resolution of the Republic of Moldova Government “On Approval of the Methodology of Publication of Open Government Data” was adopted, which describes:</p>

	products (Open Source) and open API (Application Programming Interface).		<ul style="list-style-type: none"> <li>- type of information to be opened and published,</li> <li>- procedure for its preparation and publication,</li> <li>- how to access this information,</li> <li>- use of API (application programming interfaces) and other issues related to interaction with the Single Portal of State Data of state bodies and institutions.</li> </ul>
6.5	The KR legislation does not include basic information protection and <b>cybersecurity</b> provisions. The specialized law that should contain such provisions - on electronic governance - contains only provisions to protect the right of access to information and to protect the information holders' rights. These rights are important elements of cybersecurity, but neither information protection nor cybersecurity can be reduced to the main actors' rights in the digital environment. In this regard, the basic provisions on cybersecurity, in particular on standardization and technical regulation in this area should be enshrined in the law.	<b>G</b>	<p>Today, the IT community, in addition to information protection, is increasingly talking about cyber resilience, the essence of which is to ensure the smooth and sustainable functioning of the information infrastructure in the face of ongoing cybersecurity risks. Thus, the main efforts should be focused on the design of systems taking into account the requirements for their cyber resilience. At the same time, one of the main and important areas of cyber resilience is the resilience of international Internet connections. As the digital economy develops, the financial and business sectors are increasingly using the technological capabilities of the Internet for international transactions and other types of international interaction. As a result, most international experts conclude that in the XXI century, there is an urgent need to move toward cyber resilience, which implies the ability to quickly recover from cyber incidents.</p> <p>Another trend in the global cybersecurity practice is the use of supply chain security approaches, which are aimed at securing the entire supply chain (of goods, services, works, etc.). Today, the supply chain is becoming transnational and global, and supply chain security is becoming increasingly important. The presence of a wide range of cybersecurity risks, including those related to human factors in one participant can cause difficulties for all other partners interconnected by the information and communication technologies.</p> <p>In addition to the above trends in cybersecurity, many countries have begun to pay special attention to the security of the critical information infrastructure (hereinafter - CII). In international practice, there are different approaches to regulating CII security. Based on the results of a comparative legal analysis of such methods, it is possible to distinguish two basic models</p>

			of the CII regulation, depending on the direct subject of regulation: the "object" (RF, Kazakhstan, Germany) and the "subject-activity" (EU except Germany, Georgia, Singapore, China, Japan).
--	--	--	--

### Comments

The information legal relations in Kyrgyzstan consist of relations on the information dissemination and obtaining access to it, including in the open data form. Such a relationship involves the categorization of information by type, and the information is protected.

The KR legislation, primarily Article 12 of the E-Governance Law of the KR treats publicly available information as a legal regime of information, opposing the confidential information. In other countries, the public availability of information is not so much an element of the legal regime of information itself, as a consequence of the exercise of the basic human right of access to information, stipulated by Article 19 of the Universal Declaration of Human Rights and Article 19 of the International Covenant on Civil and Political Rights (New York, December 16, 1966). For example, in the United States, as a general rule, all publicly available information, including personal data, may be used without restriction, except in cases specified in the law (the principle of "permitted by default, unless otherwise provided by law"). This is based on the First Amendment to the US Constitution to protect freedom of speech. The open nature of the Internet is emphasized in US Supreme Court decisions. Such an approach, on the one hand, promotes the widest possible use of information in society, and, on the other hand, does not create conditions for violation of the information holders' rights, who may restrict access to information if they are legally entitled to do so.

The e-Governance Law of the Kyrgyz Republic establishes that information, access to which is restricted by law or by the decision of the information owner, is considered confidential. The Kyrgyz Republic laws restrict access to information only in order to protect national security, public order, public health and morals, and to protect the rights and freedoms of individuals and legal entities. The restrictions imposed should be proportionate to the stated objectives. Confidential information includes data:

- 1) on a person's private life;
- 2) content of correspondence, telephone and other conversations, postal, telegraphic, electronic and other communications;
- 3) constituting trade secrets;
- 4) on materials of preliminary investigation, other information, access to which is restricted in accordance with procedural legislation;
- 5) constituting tax, banking, medical, lawyer, journalist secrets, adoption and insurance secrets, and other professional secrets;
- 6) other information in accordance with the Kyrgyz Republic laws.

In the Kyrgyz legislation (in other legal acts, except for the e-governance law), the mode of access to information is poorly structured and not systematized, which leads to significant overlaps and inconsistencies between different secret regimes, which highly complicates the use of relevant information, including such use that cannot violate the rights of persons whom this or that secret belongs to.

To unify the legal regimes of legally protected secrets in the current legislation, it is necessary, in accordance with the Constitution provisions, to limit their application only to the following types of data:

- data constituting state secrets;
- data constitutes a trade secret;
- data constituting professional or procedural secrets;
- data on a citizen's private life.

When building this legislative institution, it is necessary to be guided by the United States and Europe experience, where a system of secrets is arranged both by industry (banking secrets,

communications secrets) and by subject matter (trade secrets, privacy secrets), with state secrets (state secrets) designated as a separate institution. These legal regimes have a significant history of development and are designed to protect the essential interests of those to whom they apply. The basis for establishing a secrecy regime in all cases is that the disclosure of information constituting a particular secret is capable of causing harm to the person to whom the secret relates ("the secret principal"). As a general rule, for every legally protected secret, codification or special laws should define:

- a list of data to which access is restricted or the procedure for designating specific data as secret by authorized persons;
- a list of legal, organizational and technical measures taken to limit access to the data;
- an exhaustive list of grounds for liability for violation of the statutory restrictions on access to data.

Kyrgyzstan has the necessary conditions to actively move forward with the open data initiative. The current legal framework provides sufficient legal grounds for state bodies and local self-governments to place the information at their disposal in the open data form.

The regulatory framework covers:

- the open data concept and principles;
- procedure for restricting access to information;
- procedure for the dissemination and use of publicly available information;
- the obligation of state bodies and local self-government bodies, as well as organizations financed from the national and local budgets, to provide access to information under their jurisdiction;
- a list of categories of information that state and local self-government bodies are obliged to make publicly available on an annual basis and in an accessible form;
- frequency of posting information on the Internet in the open data form;
- right to protection in accordance with the established procedure in case of violation of rights of access to information, etc.

To provide a complete list of publicly accessible information on the activities of public authorities and local governments, in 2019, the Open Data Portal was launched, which consists of a set of software and hardware tools that ensure interaction between the Portal operator, open data providers and users in the publication and use of open data.

It should also be noted that there are gaps in the current KR legislation.

Thus, normative legal acts do not establish procedures for publishing data and requirements for technological, software and linguistic means required for the placement of information by state and local authorities on the Internet in the open data form. There are no legal grounds for the use of Open Source and open API (Application Programming Interface) - a software interface-application consisting of a specific set of technical protocols and methods by which programs can exchange information. Simply put, open APIs will allow to freely integrate the "parts" of one program into another or into a third-party site.

Today's open API is the door to the digital environment. The obligation for government agencies to use an open API when publishing open data will allow the developers to access databases. The open interface will enable third-party developers and other businesses to create data access tools and customer applications. This will allow not only to form new, but also to improve old services and products. Thus, putting interfaces in the public domain gives an impetus to innovation.

At present, the following provisions should be included in the legislation, on the procedure of open data publication of the Kyrgyz Republic, which would contain:

- practical guidelines for publishing open data, including on the Open Data Portal,
- requirements for technological, software and linguistic means necessary for the placement of information by state authorities and local self-governments on the Internet in the open data form,
- right to use open source software products (Open Source) and open APIs.

Opening up government data is a worldwide trend. The Open Data Watch holds an annual assessment of the coverage and openness of data provided on the websites of the national statistical offices and any official government website. The Open Data Registry compiled based on these studies

helps to identify critical gaps, promote open data policies, improve access to data, and encourage dialogue between the national statistical offices and data users.

Thus, according to an assessment of 187 countries at the end of July 2021, Singapore, Poland and Finland are in the lead. Denmark, Sweden, the Netherlands, Slovenia, Norway, Mongolia, Slovakia, Germany, Ireland, Canada, the UAE, Lithuania, the Philippines, Moldova, and Palestine are also in the lead.

In December 2014, the largest European Union state, the **Federal Republic of Germany**, published the Federal Government's National Action Plan for the Implementation of the G8 Open Data Charter. Under this action plan, the federal government has made commitments:

- to ensure the publication of as much data as possible through the development of regulations and other tools;
- publish as many existing government data sets as possible;
- GovData will be a central portal for the federal, regional and local authorities;
- maintain regular dialogue with civil society, business, journalists, and the research community.

Besides, Germany is unique, as the state has created a library of open data-based projects. The Datalook library is a collection of the best projects based on the use of different types of data. You can use the service to find existing projects and applications to solve any kind of task. In addition, users can discuss the existing projects, add their own publicly significant projects, and contact the project's authors.

**The United States** was one of the first countries to launch an open government data portal. The federal portal Data.gov was launched in 2009 to collect and publish data from various government agencies for future use.

The US open data legislation is represented by the Freedom of Information Act, which was enacted in 1967. The law requires full or partial disclosure of previously unpublished information and documents held by the US Government. Advanced information technologies have led to a better understanding of the importance of government information for oversight, analysis, and use. In 2013, the Barack Obama Administration passed the Open Data Executive Order, Open Data Policy Manual for Agencies, which became an open data disclosure policy using standardized machine-readable data formats. In 2019, the Open, Public, Electronic, and Necessary (OPEN) Government Data Act was enacted in the United States, which already requires federal agencies to publish information online as open data, using standardized machine-readable data formats, and their metadata must be included in the Data.gov catalog.

Besides, a resource reflecting the authorities' openness is the website - congressspeaks.com, which analyzes the congressmen's public statements (what terms are used in speech, how they vote, etc.). The portal presents the activity of political figures from various parties and states, and all this is packed into an attractive site animation, which leads to high attendance of the resource by the population.

**The United Kingdom** is also among the leading countries in terms of government data openness. The existing legislation is a good model for other countries in the transition to an open data policy. The 2000 Freedom of Information Act states:

- the right of any person to access information held by public authorities;
- right to be informed of the availability of relevant information in the public authority;
- right to receive this information upon a person's request;
- right to reuse the data sets.

In 2011, the UK government published a document called "Principles of Information" that all authorities in the information sphere should follow.

The Regulation on the Reuse of Information Held by Public Authorities (adopted in 2015) regulates the right of private entities to reuse information for commercial and non-commercial purposes. The act specifies the requirements for a reuse request, and obligation of public authorities to publish lists of data for reuse and the conditions for access to such data.

Approaches to legal regulation of unification of formats for presentation of information and information exchange technologies in the state information systems are regulated by the Open Standards Principles (2018), which contain the following criteria for the selection of standards, which should:

- meet user needs,
- give suppliers equal access to government contracts,
- support flexibility and change,
- support sustainable cost,
- be transparent.

The principles ensure that future technologies will be affordable, safe and innovative. They describe how the government will define and select open standards and how those standards can be implemented in open source and proprietary software. All government departments and agencies should use these principles.

For example, Tesco which is No.1 retailer in the UK and No.3 in the world, which operates about 2,700 food and industrial goods shopping centers, using an open data portal, namely data provided by weather services, has created an hourly model of consumer demand.

The GP Ratings app rates medical clinics in England using publicly available data on the clinics, displays multiple parameters rating information, allowing users to locate, compare and identify clinics according to their requirements. The app is available on iTunes, and the source code is on Github, so everyone can create apps like School Ratings, Hospital Ratings, and many others.

**The Republic of Moldova** is one of the first countries in Europe to begin the electronic transformation of government. More than ten years ago Moldova began to resolve the problems that many countries have just begun to consider. In the 2021 assessment, Moldova ranked 19th out of 187 in the global ranking for data coverage and openness. The Moldovan legislation contains a special law "On the Reuse of Public Sector Information"<sup>10</sup>, which obliges state bodies and institutions to publish on the Unified Open Data Government Portal, all the information accumulated and collected by state bodies and institutions, in a format that allows automatic processing of documents and metadata. To implement this Law, the Resolution of the Republic of Moldova Government "On Approval of the Methodology for Publication of the Open Government Data" was adopted<sup>11</sup>, which describes the type of information that will be open and published, the procedure for compiling and publishing it, the procedure for accessing this information, the use of APIs (application programming interface) and other issues related to interaction with the Unified Government Data Portal of the state bodies and institutions. Besides, there is an approved "Concept of the Open Data Principles"<sup>12</sup>, which reveals the main problems with the implementation of the Act and how to solve them in the short and long term. In general, the Republic of Moldova extended experience, which can help to repeat the successes and avoid mistakes, when implementing the open government data initiatives. The government data portal [date.gov.md](http://date.gov.md) currently includes three main modules:

- public datasets of ministries and the central state administration agencies, made public in computer-readable formats. Based on the open government data, presented as primary data directly from the source, legal entities (private and public) and individuals can develop applications that have a significant social impact on citizens and the business environment, and implement analysis and research in areas of interest and etc. (Open Government Data).
- Open Data Search module, which allows to search, retrieve, simply and conveniently view open data in various registers, databases, etc., held by the government agencies and made public for quick and easy visualization;
- a module of access to data of public interest, including personal data from state registers and information systems, for categories of users who - on the basis of a legitimate purpose and on legal grounds - have the right and ability to open them after electronic authentication and confirmation of legal grounds (authorized access).

<sup>10</sup> <http://lex.justice.md/viewdoc.php?action=view&view=doc&id=347200&lang=2>

<sup>11</sup> <http://lex.justice.md/viewdoc.php?action=view&view=doc&id=354534&lang=2>

<sup>12</sup> <http://lex.justice.md/viewdoc.php?action=view&view=doc&id=354533&lang=2>

Based on the information published on the Open Government Data Portal, the Expert-Grup (an independent think tank from Chisinau) has launched the BudgetStories.md, an open budget website that includes infographics, visualization of the budget data and analysis of the use of the public money in Moldova in sectors such as public administration, agriculture, education, and health care. In recent years, the Moldovan government has become more transparent about budget data and other types of data. The Ministry of Finance used the World Bank's BOOST tool to release detailed and disaggregated government spending data. Currently, 1,126 datasets and 10,488 files have been published on the Moldovan Government Open Data Portal and have been downloaded about 5.5 million times.

**Ukraine** has the Law “On Access to Public Information”<sup>13</sup>, which defines public information in the open data form as public information in a format that allows its automated processing by electronic means, free and free of charge access to it, and its further use. The information processors are obliged to provide public information in the form of open data upon request, publish and regularly update it on the unified state open data web-portal and on their websites.

Resolution of the Cabinet of Ministers of Ukraine<sup>14</sup> approved the “Regulations on the Data Set to be Published as Open Data” and the “Procedure for Annual Evaluation of the Status of Disclosure and Updating of Open Data by the Information Processors on the Unified State Open Data Web Portal”.

Business in Ukraine has begun to actively use any data that can be monetized. Excessive demand for open data has led to the emergence of many startups, products and services. Open data has become a resource that opens up new ways for development. The opening of public data has already had a huge impact on the economy of Ukraine, on the work of government agencies and on society as a whole.

Thus, the publication of data by the Ministry of Ecology of Ukraine resulted in the emergence of the "Clean Water" online service. This is a map with 400 water control points marked on it. The pollution level in a particular point or region is monitored by 16 parameters. Using the Cost Ukraine service, one can monitor the state of the roads and find out where repairs are made. Open data from the Ministry of Health contributed to the emergence of the Donor.UA project. Its purpose is to monitor the donor blood stock, and to attract those who wish to donate blood.

Among the most famous Ukrainian startups that use open data for business is Agri Eye (an outgrowth of the 1991 Open Data Incubator). The team developed a field analytics system using Deep Learning. Drones are launched over the fields to generate data. Based on the collected indicators, the crop yields are forecasted. The financial sector is not lagging behind either. OTP Bank together with the Open Data Incubator launched the Open Banking Lab project. The open banking data are used to develop products to automate processes and decision-making in the financial sector. YouScore is a scoring system that uses different open data registries. Its task is to assess the financial solvency of an individual or a company based on the set criteria.

Dissemination of government data in open formats will have an economic and socio-cultural effect on the country, such as increased transparency of government bodies and local authorities, strengthening citizens' trust in the state, development of an innovative environment, the market of applications and services useful to citizens, including savings in budget expenditures when developing socially useful services, etc. At the same time, it is necessary to take into account the important role of the use of open standards - one of the most powerful tools available to open government. They allow the smallest business to compete with the largest ones. They make the data open to inspection by any citizen. They reveal the transformative power of open-source software.

The KR legislation does not include basic information protection and **cybersecurity** provisions. The specialized law that should contain such provisions - on electronic governance - contains only provisions to protect the right of access to information and to protect the information holders' rights. These rights are important elements of cybersecurity, but neither information protection nor cybersecurity can be reduced to the main actors' rights in the digital environment. In this regard, the basic provisions on cybersecurity, in particular on standardization and technical regulation in this area should be enshrined in the law.

---

<sup>13</sup> <https://zakon.rada.gov.ua/laws/show/2939-17#Text>

<sup>14</sup> <https://zakon.rada.gov.ua/laws/show/835-2015-%D0%BF#n12>

Kyrgyzstan lags far behind the global trends in cybersecurity. Today, the information security paradigm has begun to change and more and more states and companies have begun to realize that it is utopian to build security that cannot be broken. A few years ago, information technology was considered, to a greater extent, as a means of facilitating document management and automation of business processes. Therefore, there has been an increase in demand for highly intelligent protection tools that can meet the challenges of timely detection of attacks and incidents (security information and event management (SIEM), network traffic analysis (NTA), integrated anti-APT solutions). Under such conditions, the main task of any security system was to detect an attack and the attacker in the system as quickly as possible, to reduce a window of opportunity so that he did not have time to do irreparable harm. It was enough to create the necessary perimeter security, which would be aimed at finding and detecting a perimeter security intruder. However, as processes go beyond the security perimeter, as technology continues to evolve, and as actors become more mobile, specific security perimeters blur. Under such circumstances, it becomes difficult to find a point of application of the above security tools. Because of these risks, we have to accept them and understand that it is almost impossible to prevent cybercrime.

Given these circumstances, today, the IT community, in addition to information protection, is increasingly talking about **cyber resilience**, the essence of which is to ensure the smooth and sustainable functioning of the information infrastructure in the face of ongoing cybersecurity risks. Thus, the main efforts should be focused on the design of systems taking into account the requirements for their cyber resilience. At the same time, one of the main and important areas of cyber resilience is the resilience of international Internet connections. As the digital economy develops, the financial and business sectors are increasingly using the technological capabilities of the Internet for international transactions and other types of international interaction. As a result, most international experts conclude that in the XXI century, there is an urgent need to move toward cyber resilience, which implies the ability to quickly recover from cyber incidents.

Another trend in the global cybersecurity practice is the use of **supply chain security** approaches, aimed at securing the entire supply chain (of goods, services, works, etc.). Today, the supply chain is becoming transnational and global, and supply chain security is becoming increasingly important. The presence of a wide range of cybersecurity risks, including those related to human factors in one participant can cause difficulties for all other partners interconnected by the information and communication technologies. In most cases, we encounter problems when the supplied information and telecommunications equipment or software products are deliberately or unknowingly supplied with unlicensed software or with malware already installed. That is, because of the interconnectedness of supply chains, poor security in one link can jeopardize the functionality of the entire supply chain. An attack on the supply chain can occur in any industry, whether in the financial, public or private sector.

In addition to the above trends in cybersecurity, many countries have begun to pay special attention to the **security of the critical information infrastructure** (hereinafter - CII). In international practice, there are different approaches to regulating the CII security. Based on the results of a comparative legal analysis of such methods, it is possible to distinguish two basic models of the CII regulation, depending on the direct subject of regulation: the "object" (RF, Kazakhstan, Germany) and the "subject-activity" (EU except for Germany, Georgia, Singapore, China, Japan).

## Section 7. Personal data

### Content

- principles and bases of the processing
- data categories
- subject's rights
- operator responsibilities
- cross-border transfer
- control and supervision

### Current regulation (existing legislation):

1. Law of the Kyrgyz Republic "On Personal Information" dated April 14, 2008, No. 58
2. Law of the Kyrgyz Republic "On Biometric Registration of Citizens of the Kyrgyz Republic" dated July 14, 2014, No. 136
3. Resolution of the Kyrgyz Republic Government "On Approval of the Procedure for Obtaining the Consent of the Personal Data Subject for the Collection and Processing of His Personal Data, the Procedure and Form for Notifying the Personal Data Subject of the Transfer of Their Personal Data to a Third Party" dated November 21 2017, No. 759
4. Resolution of the Kyrgyz Republic Government "On Approval of the Requirements for the Security and Protection of Personal Data at Their Processing in Personal Data Information Systems, the Implementation of Which Provides the Established Levels of Protection of Personal Data" dated November 21 2017, No. 760
5. Resolution of the Kyrgyz Republic Cabinet of Ministers "On the State Agency for Personal Data Protection under the Cabinet of Ministers of the Kyrgyz Republic" dated December 22, 2021, No. 325

### Brief description of the identified shortcomings and international practice benchmarks

No.	Description of the shortcoming	Type <sup>15</sup>	Best practice
7.1	There are no definitions of: - biometric personal data - pseudonymization; - profiling  Amendments are required to Article 3 of the Law - Terms and Definitions	G	The definitions are given in the Regulation (EU) 2016/679 of the European Parliament and of the EU Council dated April 27, 2016 on the protection of individuals in the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Regulation on the Protection of Personal Data). data) (General Data Protection Regulation) (GDPR)
7.2	Biometric personal data are not classified as highly sensitive/special category of PD  Decision of the Constitutional Chamber of September 14, 2015 N 11-r states that "Biometric data is a particularly sensitive category of personal data, the illegal use of which creates a threat and can cause significant harm to the rights and legitimate interests of the data subjects."	G	Biometric data fall under special categories of personal data in both the GDPR (Article 9) and the updated Europe Council's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

<sup>15</sup> The following types of regulatory deficiencies are listed in the table:

- (G) regulatory gap (regulation is required, but it is missing)
- (O) obsolete provision (the existing provision should be changed)
- (N) non-working provision (the existing provision is non-working for the reasons described)
- (B) this provision is an unreasonable barrier to the implementation of activities

7.3.	The scope of grounds for processing particularly sensitive (special categories) data does not cover all necessary cases (the current law specifies only two exceptions - availability of consent, and when processing is necessary to protect health and safety)	G	Article 9 of the GDPR contains at least 10 grounds for processing special categories of personal data, each serving a specific purpose in the digital society
7.4.	The law requirement to sign consent to the processing of personal data in the form of an electronic document with an electronic signature is an outdated provision - more than 10 years have passed since the adoption of the Law "On Personal Information", during which time global technologies changed, new information and communication technologies are being introduced. However, the current law does not yet recognize the expression of a person's will by electronic or other technical means (for example, by transmitting a signal, by filling out a form on the Internet, in an information system, including in a smartphone application, by pressing the OK button) for a full legal expression of a will to have their personal data processed, along with an electronic signature.	O	<p>Articles 4 (11) of GDPR:  "Consent" of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her;</p> <p>Article 7 of GDPR. Conditions for consent  1. Where the processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to the processing of his or her personal data.  2. If the data subject's consent is given in the context of a written declaration that also concerns other matters, the request for consent shall be presented in a manner that is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.</p> <p>Guidelines on consent under Regulation 2016/679</p> <p>79. Without prejudice to existing (national) contract law, consent can be obtained through a recorded oral statement, although due note must be taken of the information available to the data subject, prior to the indication of consent. The use of pre-ticked opt-in boxes is invalid under the GDPR. Silence or inactivity on the part of the data subject, as well as merely proceeding with a service cannot be regarded as an active indication of choice.</p>
7.5.	The law does not provide for the withdrawal of consent at any time and in the same manner/form as the expression of consent.	G	Article 7 of GDPR. Conditions for consent 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed

			thereof. It shall be as easy to withdraw as to give consent.
<b>7.6.</b>	<p>The number of grounds for personal data processing in the Kyrgyz Republic law does not meet the digital economy needs and international standards, in particular, it is not specified that the personal data processing may be necessary for the contract performance.</p> <p>This is a gap in the current legislation, which leads to the fact that banks, telecom operators, or companies to conclude an employment contract, or any service providers, are forced to withdraw consent to the personal data processing, which neutralizes the very essence of the consent as a free will, which is thereby put under the condition of receiving or not receiving a certain service (banking, communication services, etc.).</p>	<b>G</b>	<p>Article 6 of GDPR. Lawfulness of processing</p> <p>1. Processing shall be lawful only if and to the extent that at least one of the following applies:</p> <p>(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;</p> <p>(b) processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;</p> <p>(c) processing is necessary for compliance with a legal obligation to which the controller is subject;</p> <p>(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;</p> <p>(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;</p> <p>(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.</p> <p>Point (f) of the first subparagraph does not apply to processing performed by government agencies in the performance of their tasks.</p>
<b>7.7.</b>	<p>The law does not fully consider all the rights of personal data subjects contained in international standards, which affects the ability to protect them.</p> <p>Such as:</p> <ul style="list-style-type: none"> <li>- The right to delete data (“right to be forgotten”);</li> </ul> <p>(Any application of the “right to be forgotten” should be strictly limited, since certain minimum requirements should be</p>	<b>G</b>	<p>Articles 15-22, 34 GDPR</p> <p>Guidelines Information Commissioner’s Office, Right of Access (2020).</p> <p>EDPB, Guidelines 8/2020 on the targeting of social media users (2020).</p>

<p>met so that such a right does not conflict with the right to freedom of expression, both in the content and in the procedural sense. In particular, the subjects of the “right to be forgotten” should be individuals, the “right to be forgotten” should apply only to search systems (as personal data operators), and not to hosting services and content providers. All remedies should explicitly refer to freedom of expression as a fundamental right, with which such remedies should be balanced)</p> <ul style="list-style-type: none"> <li>- Obligation to notify regarding modification or destruction of personal data or restriction of processing;</li> <li>- Right to data portability;</li> <li>- Right to object (against profiling, direct marketing);</li> <li>- right not to be subject to a decision, which may include specific measures assessing personality characteristics, based solely on automated processing and entailing legal consequences (such as automatic rejection of an online loan application form or online recruitment without any human mediation; such processing should be subject to appropriate safeguards, which should include specific information on the data subject and the right to require human intervention, to express their point of view, to demand an explanation of the decision taken as a result of such an assessment, and to change the decision. This measure should not apply to the child);</li> <li>- The right to receive information about a personal data security breach (the obligation to notify the data subject about a personal data security breach)</li> </ul>	<p>EDPB, Guidelines 3/2019 on Processing of Personal Data through Video Devices (2020).</p> <p>EDPB, Guidelines 02/2021 on Virtual Voice Assistants (2021).</p> <p>EDPB, Guidelines 01/2022 on data subject rights — Right of access (2022).</p> <p>Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679; European Commission, Commission Guidance on the application of Union data protection law in the electoral context, A contribution from the European Commission to the Leaders’ meeting in Salzburg on 19-20 September (2018).</p> <p>EDPB, Guidelines 8/2020 on the targeting of social media users (2020).</p> <p>European Commission, Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection Brussels (2020).</p> <p>ICO, Data sharing: a code of practice (2020).</p> <p>Spanish Data Protection Agency (AEPD), Guide on use of cookies (2021).</p> <p>Article 29 Working Party, Guidelines on the Implementation of the Court of Justice of the European Union Judgment on Google Spain Inc. v. Agencia Española de protección de datos (AEPD) and Mario Costeja González C-131/12 (2014).</p> <p>EDPB, Guidelines 5/2019 on the Criteria of the Right to be Forgotten in the Search Engines Cases under the GDPR (part 1) (2019).</p> <p>EDPB, Guidelines 02/2021 on Virtual Voice Assistants (2021).</p> <p>Article 29 Working Party, Guidelines on the Right to Data Portability (2017).</p> <p>Information Commissioner’s Office, Right of Access (2020).</p>
--	---

			<p>EDPB, Guidelines 02/2021 on Virtual Voice Assistants (2021).</p> <p>Article 29 Working Party, Opinion 03/2014 on «Personal Data Breach Notification (2014).</p> <p>Article 29 Working Party, Guidelines on Personal data breach notification under Regulation 2016/679 (2018).</p> <p>EDPB, Guidelines 1/2021 on Examples regarding Data Breach Notification (2021).</p> <p>DPC (Ireland), Guidance for Individuals who Accidentally Receive Personal data (2020).</p>
7.8.	The law does not encourage the use of promising practices such as data protection by design and by default	<b>G</b>	<p>Article 25 of GDPR</p> <p>Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymization, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.</p> <p>WP29, Opinion 05/2014 on Anonymisation Techniques (2014).</p> <p>WP29, Opinion on data processing at work (2017).</p> <p>Spanish Data Protection Agency (AEPD), A Guide to Privacy by Design (2019).</p> <p>EDPB, Guidelines 4/2019 on Article 25 – Data Protection by Design and by Default (2020): Data protection by design should be implemented both at the time of determining the means of processing and at the time of processing itself. It is at the time of determining the means of processing that controllers shall implement measures and</p>

			<p>safeguards designed to effectively implement the data protection principles. To ensure effective data protection at the time of processing, the controller must regularly review the effectiveness of the chosen measures and safeguards. The EDPB encourages early consideration of data protection by design when planning a new processing operation.</p> <p>EDPB, Guidelines on the use of location data and contact tracing tools in the context of the COVID-19 outbreak (2020).</p> <p>EDPB, Guidelines 3/2019 on Processing of Personal Data through Video Devices (2020).</p> <p>Spanish Data Protection Agency (AEPD), Guidelines for DataProtection by Default (2020).</p> <p>Information Commissioner’s Office, Right of Access (2020).</p> <p>EDPB, Guidelines 01/2021 on Examples regarding Data Breach Notification (2021).</p> <p>EDPB, Guidelines 02/2021 on Virtual Voice Assistants (2021).</p>
<b>7.9.</b>	<p>An obsolete provision, as well as a corruption barrier and an opportunity for punitive sanctions is also the presence in Article 30 of the Act of the mandatory obligation to register the personal data arrays and holders (owners) of these arrays, and the functions of the authorized body to keep a register of personal data holders (owners).</p> <p>There is a risk of punitive sanctions against any legal entities for formal non-compliance with this requirement (not registering as a holder).</p> <p>At the same time, the law does not establish procedures, such as the simplest possible notification of online registration of personal data holder only for the purpose of accounting and understanding purposes of the personal data processing.</p>	<b>B</b> <b>O</b>	<p>According to Article 36 of GDPR. Prior consultation. The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.</p>
<b>7.10</b>	<p>The authorized state body’s functions and powers do not meet the standards of autonomy, independence, competence, tasks and powers of supervisory bodies, which are an essential and necessary component of the individuals protection,</p>	<b>G</b>	<p>Articles 51-59 of GDPR</p>

	with regard to their personal data processing.		
<b>7.11</b>	<p>Requirements for security and protection of personal data in their processing in personal data information systems, the execution of which ensures the established levels of personal data security:</p> <p>The following requirements have not been developed:</p> <ul style="list-style-type: none"> <li>- Model list of threats to the personal data security, containing all types and types of alleged threats;</li> <li>- methodology for determining security threats to personal data information systems;</li> <li>- as well as industry-specific lists of threats to the personal data security in the performance of relevant activities</li> </ul> <p>There is a provision that such documents should be developed, but it has not been executed, the documents have not been developed.</p>	<b>G</b>	This gap is caused by the peculiarities of the Kyrgyz Republic legislation
<b>7.12</b>	<p>There is no provision for the publication of a document defining the policy of the holder (owner) of an array of personal data regarding the personal data processing;</p> <p>(it is only provided to bring the content of this document to information of the employees and counterparties of the holder (owner) of the array of personal data)</p>	<b>G</b>	<p>Article 12 of GDPR</p> <p>The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means.</p> <p>Preamble 58</p> <p>This information may be made available electronically, for example, if it is addressed to the public, on the website</p>
<b>7.13</b>	<p>Regulations on the State Agency for Personal Data Protection under the Cabinet of Ministers of the Kyrgyz Republic: The functions and powers of the authorized state body do not meet the standards of autonomy, independence, competence, tasks and powers of supervisory bodies, which are an essential and necessary component of the individuals' protection, with regard to the processing of their personal data</p>	<b>G</b>	Articles 51-59 of GDPR

<p><b>7.14</b></p>	<p>Liability for many offenses and crimes with personal data are not defined (amendments to the codes are needed).</p> <p>The determining factors in this case should be the issues not so much of penalties for violations, but rather the restoration of violated rights of the subjects and compensation of harm caused to them by illegal actions.</p>	<p><b>G</b></p>	<p>GDPR, Articles 83-84</p>
--------------------	--	-----------------	-----------------------------

### Comments

The Law of the Kyrgyz Republic "On Personal Information" was adopted in 2008 (hereinafter - the Law), amendments were made in 2017 (in connection with the adoption of the E-Governance Law of the Kyrgyz Republic and the Electronic Signature Law of the Kyrgyz Republic).

In 2017, amendments were made in the Law on Personal Information, which:

- established the competence of the Government of the Kyrgyz Republic to issue legal acts regulating the sphere of personal data, including security;
- detailed the issues on the form of subject's consent to the processing of his/her personal data, established the possibility of obtaining consent in the form of an electronic document;
- introduced a separate article on the status and functions of the authorized body on personal data protection.

These amendments made it possible to adopt (in November 2017) a number of regulations and legal acts at the Kyrgyz Republic Government level, clarifying the issues of personal data protection in information systems.

The Law of the Kyrgyz Republic "On Personal Information" is aimed at legal regulation of handling the personal data on the basis of generally accepted international principles in order to protect the rights and freedoms of a man and citizen associated with the collection, processing and use of personal data.

In general, the Law complies with the main international standards for the personal data protection, including the Council of Europe (Strasbourg) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS N 108) of January 28, 1981, but does not take into account the changes made to this Convention protocol ETS N 223.

However, there are a number of shortcomings and gaps, because the Act was passed in the "pre-technology" era and does not comply with today's realities and challenges, including those related to responding to the challenges posed by the COVID-19 pandemic.

The approaches to legal regulation of the telecommunications sector, which the European Union demonstrates, are currently of great practical importance for many states. The dynamic development of regulation of personal data relations in the European Union indicates a consistent, systematic and comprehensive formation, development and improvement of the relevant regulatory and institutional framework in their organic relationship.

Therefore, as a guideline for best international practice, it is proposed to consider the Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR).

The situation with personal data protection is exacerbated by the **outdated legislation** - more than 10 years have passed since the adoption of the Law "On Personal Information", during which time global technologies changed, new information and communication technologies are being introduced. Not only has the approach to collecting personal information changed, but also the public attitudes toward this also changed. In this regard, there is a need to fix the current level of development of information and other technologies, to respond to the current challenges and threats posed by the ever-expanding opportunities for processing and cross-border transfer of personal data.

One of these global changes in international standards for the protection of personal data - is the definition of new rights granted to citizens to manage their personal data during its processing, including those based on mathematical algorithms, artificial intelligence, and the obligation of personal data holders to notify the authority and citizens about leaks of personal data.

Another disadvantage of the current Personal Information Law is the requirement for the form of consent to process personal data - in writing (Online) or in electronic form (online), signed with an electronic signature. The current law does not yet recognize the expression of a person's will by electronic or other technical means (for example, by transmitting a signal, by filling out a form on the Internet, in an information system, including in a smartphone application, by pressing the OK button) for a full legal expression of a will to have their personal data processed, along with an electronic signature. There is a critical issue of creating a nationwide online platform for managing the obtained/expressed consent of citizens for data processing.

The situation with legal grounds for personal data processing is not clear. The law does not establish all the legal grounds recognized by international acts for dealing with personal data (e.g., the existence of a contract), nor is it clear about the exceptions to receive consent for lawful data processing, such as for schools, which are not state bodies that have an exception from the requirement to get consent in the performance of their functions.

In the general context of advanced approaches to the protection of citizens' rights to privacy is the right to receive information about unauthorized access by third parties to their personal data, the right to assert their disagreement, regardless of the place of residence to receive qualified protection, including from the authorized body. These provisions are also missing in our legislation.

The law should also address the gaps associated with the development of digital technologies, to respond to current challenges and threats posed by the constantly expanding opportunities for processing and transborder transfer of personal data; define new rights for citizens to manage their personal data during its processing, including those based on mathematical algorithms, artificial intelligence, the obligation of personal data holders to notify the authority and citizens about leaks of personal data.

As a response to the challenges that emerged during the COVID-19 pandemic, legal issues related to the processing and transfer of personal data in emergency situations, the cross-border transfer of personal data when it is not possible to obtain the subject's consent, issues of access to sensitive (special category) medical data should be addressed.

Measures of responsibility for offenses and crimes with personal data are not defined (amendments to the codes are needed - on offenses)<sup>16</sup>, criminal code<sup>17</sup>). The determining factors in this case should be the issues not so much of penalties for violations, but rather the restoration of violated rights of the subjects and compensation of harm caused to them by illegal actions.

The procedural legislation does not provide for methods and means of computer forensics, fixing digital evidence of violations with personal data (not only) for the purpose of investigation, their examination in court.

The regime of cross-border data flows is also a challenge in the integration of Kyrgyzstan into the Eurasian Economic Union, the digital agenda of which stipulates the creation of a common market for the EEU and the circulation (free movement) of personal data of citizens.

In the future, it is necessary to raise the issue of creating a data-CERT that will monitor and respond to leaks of personal data.

So far, the powers and competence of the authorized state body on personal data protection are not clearly defined.

---

<sup>16</sup> In the Code of Offenses of October 28, 2021, there is one article - 228-1. Violation of the requirements for the protection of personal and commercial information (Violation of the requirements for the organization of protection of electronic documents, personal and commercial information, and the misuse, provision of access and transfer to third parties of such information - entails a fine on individuals in the amount of 200 calculation indices).

<sup>17</sup> The Criminal Code of 28.10.2021, provides for punishment for violation of privacy (Art. 190 CC), violation of the secrecy of correspondence (Art. 193), unauthorized access to computer information and electronic documents in an information system or telecommunications network (Art. 319).

According to Article 29-1 of the Personal Information Law, the authorized state body is responsible for the control of compliance of personal data processing with the requirements of this Law, and protection of the rights of the personal data subjects. The authorized state body cooperates with authorized bodies on personal data protection in foreign countries, in particular, in the international exchange of information on the protection of the personal data subjects' rights. Decisions of the authorized state body for the protection of the personal data subjects' rights may be appealed in the manner prescribed by the Law of the Kyrgyz Republic "On Fundamentals of the Administrative Activity and Administrative Procedures".

Resolution of the Cabinet of Ministers of the Kyrgyz Republic dated December 22, 2021 No. 325 approved the Regulations on the State Agency for the Protection of Personal Data under the Cabinet of Ministers of the Kyrgyz Republic as a state executive body that develops and implements a unified state policy in the field of personal information, which performs the functions of ensuring the protection of the personal data subjects' rights, registration of holders (owners) of personal data arrays, maintenance of the Register of holders of personal data arrays. In accordance with the provision, the purpose of the Agency is to protect the rights and freedoms of a man and citizen associated with the collection, processing and use of personal data, regardless of the means of processing this information, including the use of information technology.

The Agency's objectives include: 1) ensuring control over the compliance of the personal data processing with the requirements of the Kyrgyz Republic legislation on personal information by state bodies, local self-governments, state and municipal institutions and enterprises, and legal entities and individuals, regardless of the form of ownership; 2) protection of the personal data subjects' right; 3) informing the public on the situation with the personal data protection in the Kyrgyz Republic; 4) implementation of other tasks assigned to the Agency in accordance with the Kyrgyz Republic legislation.

The functions include to control by checking compliance with requirements of the Kyrgyz Republic legislation on protection of personal data and rights of the personal data subjects; keeping records and registration of the personal data arrays and their holders (owners); formation and maintenance of the Register of the personal data array holders (owners); coordination of lists of personal data arrays holders (owners); giving recommendations on controversial issues arising between the participants of the information interaction in the processing, storage and transfer of personal data, assisting the personal data subjects in the exercise and protection of their rights; consideration of appeals by the personal data subjects about violations of the personal data legislation and making conclusions; sending materials related to the violation of the personal data subjects' rights provided for by the Kyrgyz Republic legislation on personal data to law enforcement agencies to take appropriate measures to enforce the Kyrgyz Republic legislation; providing the methodological assistance in organizing the personal data protection.

However, the regulatory, coordination, supervisory and control functions do not apply to personal data obtained as a result of activities of the prosecution bodies of the Kyrgyz Republic, law enforcement agencies and bodies engaged in operational and investigative, intelligence and counterintelligence activities, production of official statistics<sup>18</sup>. This is a significant and unreasonable limitation in terms of supervision in the field of personal data protection and is not consistent with the status of authorized bodies in other countries. In general, the functions and powers of the authorized state body do not meet the standards of autonomy, independence, competence, tasks and powers of supervisory bodies in this area according to generally accepted international standards<sup>19</sup>, which are an essential and necessary component of the individuals' protection in relation to the processing of their personal data.

Failure to comply with the principles of independence when creating the institution of the Commissioner for the Personal Data Protection, in absence of the powers of such a body established by law and the approved and published standards for its work, is fraught with negative consequences for

---

<sup>18</sup> P.10 Regulations

<sup>19</sup> The European Union's General Data Protection Regulation (GDPR) is proposed as the main reference point in this area; the standards for the supervisory authorities are stipulated in Articles 51-59 of the GDPR.

the observance of human rights in the process of such reform, creation of another government structure with the police / punitive functions, which is especially alarming against the backdrop of high-profile journalistic investigations of corruption, personal data leaks from the Safe City cameras, the installation and use of cameras with face recognition, which was done in the absence of the necessary legal framework and public discussions with the expert community, the use of digital surveillance based on geolocation data, processing of digital photo and video images, transmission of telemetric health data via communication channels, digitization of public services with the requirement of unambiguous identification/proof of identity with the receipt and storage of personal data, including biometric data, in a digital environment.

The presence in the Personal Information Law of the Kyrgyz Republic of the authorized body's functions to maintain a register of holders of an array of personal data is a possibility for corruption and punitive sanctions, and there is a risk of punitive sanctions against any legal entities for formal non-compliance with this requirement (not registering as a holder).

At the same time, the law does not establish procedures, such as the simplest possible notification of online registration of the personal data holders only for the purpose of accounting and understanding the purposes of the personal data processing.

According to the experts, another gap in the proper regulation of personal data is the existence of another special law **“On Biometric Registration of Citizens of the Kyrgyz Republic”** dated July 14, 2014.

This Law independently, in ways different from the Law on Personal Information, regulates relations arising from the collection, processing, storage and use of biometric data of the Kyrgyz Republic citizens, (hereinafter referred to as the biometric data), updating and protecting the biometric database.

According to Article 4 of the Law, biometric data are collected, processed, stored and used on the principles of mandatory biometric registration, and every Kyrgyz Republic citizen should undergo biometric registration in accordance with this Law.

As can be seen from the Law wording, the biometric data are excluded from the regulation of the Personal Information Law, although in fact it is sensitive personal data - a special category of personal data under Article 8 of the Personal Information Law.

The procedures regarding the biometric data specified in the Biometric Registration Law are not synchronized with the procedures provided for in the Personal Information Law and do not comply with the European standards for sensitive data protection.

The law does not make any exceptions from the mandatory biometric registration, including for minors, citizens with mental disorders, citizens permanently residing abroad, and people whose beliefs do not allow them to provide biometric data. The main difficulties of the Law are related to compulsory registration: both in terms of its contradiction to acts of higher legal force and in terms of implementation of the Law provisions.

Mandatory biometric registration requires, first, an extremely specific definition of the purposes for which the collected biometric data are used, and second, a reasonable list of exceptions to mandatory registration. The law provides for neither: it extremely vaguely defines the purposes, for which the collected biometric information is to be used (Articles 2 and 7) and does not provide for any list of exceptions at all.

These circumstances were the subject of consideration by the Constitutional Chamber of the Supreme Court of the Kyrgyz Republic, which, at the request of experts, considered the compliance of the said Law with the Constitution provisions.

By decision of the Constitutional Chamber of September 14, 2015 N 11-r, the provisions of the Law under consideration were recognized as not contradicting the Constitution.

The decision also states that when creating the government information systems, the following conditions should be observed: fixing the biometric data of citizens without humiliating the dignity of the individual or causing harm to health; avoiding the possibility of illegal reproduction, use and distribution of biometric data of citizens; ensuring the confidentiality and security of information

contained in the state information system, and limiting this information to only the information that is necessary to verify the authenticity of the new generation identification documents.

According to the decision of the Constitutional Chamber, the Jogorku Kenesh of the Kyrgyz Republic should make appropriate amendments to the Law of the Kyrgyz Republic "On Biometric Registration of Citizens of the Kyrgyz Republic" arising from the motivational part of this decision<sup>20</sup>.

In 2017, Resolution of the Kyrgyz Republic Government dated November 21, 2017 No. 760 approved **“Requirements for ensuring the security and protection of personal data when they are processed in the personal data information systems, the implementation of which ensures the established levels of personal data security”**.

The Model List of threats to the personal data security, containing all types and types of alleged threats, a methodology for determining security threats in personal data information systems, as well as industry-specific lists of threats to the personal data security in the performance of relevant activities that have not yet been developed.

Another gap is the lack of requirements for mandatory publication (including on the website) of a document defining the policy of the holder (owner) of the personal data array regarding the processing of personal data (provides only to communicate the content of this document to employees and counterparties of the personal data array holder (owner)).

In addition, with the OSCE support, the CIIP PF developed Methodological guidelines for organizing the personal data security in accordance with the Personal Information Law of the Kyrgyz Republic No. 58, which were recommended by the State Information Technologies and Communications Committee (now – the State Service for Digital Development ) to PD holders. The guidelines have been drawn up taking into account the upcoming regulatory novelties and should serve as a guide to action for a wide range of citizens, experts, IT auditors, specialists and managers, one way or another involved in the process of ensuring the security of personal data. Besides, the CIIP PF conducted trainings on the application of these Methodological Guidelines for various PD holders.

### **One of the major challenges to the right to privacy and the lawfulness of the personal data processing was the COVID-19 coronavirus pandemic.**

The authorities in many countries are resorting to unprecedented measures that have the potential risks of violating civil rights with the danger of continued interference with privacy after the end of the pandemic. Governments are taking various measures to combat the virus, including the use of Internet technology. These include tracking infected or quarantined people - facial recognition, tracking mobile traffic and user geolocation, and many other ways to interfere with people's privacy.

Therefore, monitoring of restrictions on digital rights and freedoms of citizens related to the global pandemic of 2020 and legitimacy of the use of digital surveillance technologies is particularly relevant today.

Governments use mass surveillance with city surveillance cameras and video recording devices to identify those who violate quarantine. Tracking the movement of citizens, using mobile communication networks, GPS, fixing the localization of transactions on cards and accounts. Government services and agencies have unlimited access to almost all people's personal data.

Various technological elements of surveillance, control of communications, and censorship of publications are introduced, justifying their actions by the fight against the coronavirus. This creates the preconditions for violation of the right to privacy, freedom of speech, and secrecy of communication.

Often these measures are excessive or non-transparent for public control, or raise many questions among experts about the effectiveness of such measures in balancing the interests of society and state control.

In addition, there are high risks that all these tough measures may remain after the pandemic. It is declared that these restrictions are temporary and will be promptly removed once the crisis has passed. However, human rights activists have objective doubts about this.

---

<sup>20</sup> Only now the Kyrgyz Republic Jogorku Kenesh (Parliament) is considering relevant amendments to this law, prepared by the Cabinet of Ministers of the Kyrgyz Republic to implement the decision of the Constitutional Chamber.

Therefore, monitoring restrictions on digital rights and freedoms of citizens related to the global pandemic of 2020, the legitimacy of the use of digital surveillance technologies, is particularly relevant today.

It is important that technology supports freedom, justice, and innovation for citizens.

Despite the generally progressive nature of legislation in the field of personal data protection, its (generally) compliance with existing international standards in the field of privacy and personal data protection, the Law on Personal Information, adopted in the pre-technological era in 2008, is outdated and needs to be updated to consider the new challenges and threats associated with the automated, digitally-assisted collection and processing of personal data in order to better comply with the European standard in the field of personal data protection, since the individuals' protection in relation to the personal data processing is a fundamental right.

Considering the above, based on the legal analysis of the personal data protection legislation, **we note the following gaps and shortcomings** in the legal regulation of this area:

1. There are no definitions of:

- personal biometric data
- pseudonymization;
- profiling

Amendments are required to Article 3 of the Law "Terms and Definitions".

2. Biometric personal data are not classified as highly sensitive/special category of PD.

Decision of the Constitutional Chamber of September 14, 2015 N 11-p states that "Biometric data refer to a particularly sensitive category of personal data, the illegal use of which poses a threat and can cause significant harm to the rights and legitimate interests of these data subjects."

3. The law does not take into account all cases of exceptions - when the processing of particularly sensitive (special categories) data is allowed.

For example:

- processing is necessary in order to fulfill the obligations and certain rights of the data controller or data subject under labor law, social security and social security law;
- processing concerns the personal data that the data subject has explicitly made public;
- processing is necessary for the assertion, enforcement or defense of legal claims or as part of the administration of justice by courts;
- processing is necessary for preventive or occupational medicine purposes, to assess an employee's ability to work, to diagnose a medical condition, to provide medical or social care, or to provide treatment;
- processing is necessary for reasons of public health interest, such as protection from serious cross-border health threats.

4. The presence in the law of a requirement to sign by electronic signature consent to the personal data processing in the form of an electronic document

This provision is outdated - more than 10 years have passed since adoption of the Law "On Personal Information", during which time global technologies changed, new information and communication technologies are being introduced. However, the current law does not yet recognize the expression of a person's will by electronic or other technical means (for example, by transmitting a signal, by filling out a form on the Internet, in an information system, including in a smartphone application, by pressing the OK button) for a full legal expression of a will to have their personal data processed, along with an electronic signature.

Solution option:

The written form of consent is also considered as observed if the subject expresses his/her will through the information technologies, and the person performs actions using electronic or other technical means that allow the consent content to be reproduced on a tangible medium unchanged, while the requirement for a signature is considered fulfilled if any method is used, which allows to reliably

determine the person who expressed the will. Regulatory legal acts of the Cabinet of Ministers of the Kyrgyz Republic and / or agreement of the parties may provide for a specific method for reliably determining the person who has expressed consent to the personal data processing.

(For example, consent to the personal data processing may be given by checking the appropriate box and pressing the “Send” button when registering (submitting an electronic application) on the website and/or in the relevant application of the personal data holder or processor installed on the personal data subject's device. Identification should include the digital identification of the data subject, for example, through a credential-based authentication mechanism, which is used by the data subject to log in to an online service provided by the data holder/processor. The holder (processor) may use all acceptable means to verify and confirm the identity of the data subject (who requests access, in particular in the context of online services and online identifiers).

5. The law does not provide for the withdrawal of consent at any time and in the same manner/form as the expression of consent.

The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

6. Absence of a contract as a legal basis for personal data processing - when personal data processing is necessary for the contract performance.

Supplement Article 5 with new legal basis:

- if the processing is necessary for performance, for the execution of a contract, to which the data subject is a party, or for the implementation, on behalf of the data subject, of actions preceding the contract conclusion.

7. The law does not fully take into account all the rights of personal data subjects contained in international standards, which affects the ability to protect them.

Such as:

- The right to delete data (“right to be forgotten”);

(Any application of the “right to be forgotten” should be strictly limited, since certain minimum requirements should be met so that such a right does not conflict with the right to freedom of expression, both in the content and in the procedural sense. In particular, the subjects of the “right to be forgotten” should be individuals, the “right to be forgotten” should apply only to search systems (as personal data operators), and not to hosting services and content providers. All remedies should explicitly refer to freedom of expression as a fundamental right, with which such remedies should be balanced).

- Obligation to notify regarding modification or destruction of personal data or restriction of processing;

- Right to data portability;

- Right to object (against profiling, direct marketing);

- right not to be subject to a decision, which may include specific measures assessing personality characteristics, based solely on automated processing and entailing legal consequences (such as automatic rejection of an online loan application form or online recruitment without any human mediation; such processing should be subject to appropriate safeguards, which should include specific information on the data subject and the right to require human intervention, to express their point of view, to demand an explanation of the decision taken as a result of such an assessment, and to change the decision. This measure should not apply to the child);

- the right to receive information about a personal data security breach (the obligation to notify the data subject about a personal data security breach).

8. The law does not establish mandatory technical and organizational measures to protect personal data as Data protection by design and by default

(obligation to implement appropriate technical and organizational measures, such as pseudonymization, designed to effectively implement the personal data protection principles, such as data minimization, and to integrate necessary safeguards into processing for compliance purposes).

9. An obsolete provision, as well as a corruption barrier and an opportunity for punitive sanctions is also the presence in Article 30 of the Act of the mandatory obligation to register the personal data arrays and holders (owners) of these arrays, and the functions of the authorized body to keep a register of personal data holders (owners).

There is a risk of punitive sanctions against any legal entities for formal non-compliance with this requirement (not registering as a holder).

At the same time, the law does not establish procedures, such as the simplest possible notification of online registration of personal data holder only for the purpose of accounting and understanding purposes of the personal data processing.

10. The authorized state body's functions and powers do not meet the standards of autonomy, independence, competence, tasks and powers of supervisory bodies, which are an essential and necessary component of the individuals' protection, with regard to their personal data processing.

11. The requirements provided by the specified Requirements for ensuring the security and protection of personal data during their processing in the personal data information systems have not been developed, the execution of which ensures the established levels of the personal data protection:

- Model list of threats to the personal data security, containing all types and types of alleged threats;

- a methodology for determining security threats to personal data information systems;

- as well as industry-specific lists of threats to personal data security in the performance of relevant activities.

12. There is no provision for the publication of a document defining the policy of the holder (owner) of an array of personal data regarding the personal data processing;

(it is only provided to bring the content of this document to information of the employees and counterparties of the holder (owner) of the array of personal data).

13. Liability measures for many offenses and crimes with personal data are not defined (amendments to the codes are needed).

The determining factors in this case should be the issues not so much of penalties for violations, but rather the restoration of violated rights of the subjects and compensation of harm caused to them by illegal actions.

## Section 8. Big Data

### Content

- principals, operators and data users
- data portability
- data localization
- artificial intelligence and neural networks

### Current regulation (existing legislation):

1. Innovation Activities Law of the Kyrgyz Republic
2. Decree of the Kyrgyz Republic President “On the National Development Program of the Kyrgyz Republic to 2026” dated October 12, 2021, UP No.435
3. Resolution of the Kyrgyz Republic Government “On approval of the Action Plan of the Kyrgyz Republic Cabinet of Ministers for the Implementation of the National Development Program of the Kyrgyz Republic until 2026” dated December 25, 2021, No. 352

### Brief description of the identified shortcomings and international practice benchmarks

No.	Description of the shortcoming	Type <sup>21</sup>	Best practice
8.1	<p><b>There is no legislation regulating the use of big data and artificial intelligence.</b></p> <p>The following are also missing: terminology, regulatory principles, rights and obligations of subjects, localization requirements, the possibility of using government data, requirements and restrictions on AI systems, measures to support innovation, authorized bodies, AI code of ethics</p>	G	<p>Advanced countries and associations, realizing the importance and relevance of big data technology and artificial intelligence are attempting to regulate these technologies, as well as adopt strategic documents (programs, concepts, strategies) aimed at their support and development.</p> <p><b>In 2020, the European Union</b> adopted the European Data Strategy, which aims to create a common European data space for the operation of a single data market. The EU Regulation 2018/1807 “On the System of Free Flow of Non-Personal Data in the European Union” dated November 14, 2018, consolidated the basic principles of the free flow of data, by establishing rules regarding the data localization requirements, data availability for competent authorities and data portability for professional users.</p> <p>As part of the Artificial Intelligence Strategy implementation, the European Commission presented a Member State Harmonized Plan for Artificial Intelligence on December 7, 2018. The plan proposes joint action for closer and more effective cooperation among member states. In 2019, the</p>

<sup>21</sup> The following types of regulatory deficiencies are listed in the table:

- (G) regulatory gap (regulation is required, but it is missing)
- (O) obsolete provision (the existing provision should be changed)
- (N) non-functioning provision (the existing provision is non-functioning for the reasons described)
- (B) this provision is an unreasonable barrier to the implementation of activities

European Commission's AI Expert Group presented the Policy and Investment Recommendations for Robust AI and the Ethics Guidelines for Robust Artificial Intelligence. In 2021, the European Commission developed and proposed a document "On the adoption of harmonized rules on artificial intelligence (Artificial Intelligence Law)". This document is not yet legally binding, but if adopted, will be the first of its kind, a large-scale law regulating AI.

**In 2014, the US** approved the National Strategy for Big Data, which sets the main provisions of US public policy for the development and use of big data by citizens, businesses and government, primarily to achieve the economic and social effects. In 2015, NIST adopted a series of standards in the areas of terminology, big data architecture, privacy and personal data security in the use of big data technologies. In 2018 and 2019, the standards were revised and amended. In 2020, a new federal strategy "Using Data as a Strategic Asset" was adopted.

In 2016, the National Artificial Intelligence Research and Development Strategic Plan was adopted, which contains a strategic plan for federally funded AI research and development (updated in 2019). In 2019, the Executive Order "Preserving the US Leadership in Artificial Intelligence" was signed to establish federal principles and policies to strengthen the nation's capabilities in artificial intelligence to advance scientific discovery, economic competitiveness and national security. On January 1, 2021, the National Artificial Intelligence Initiative was launched, which provides a coordinated program across the federal government to accelerate research and application of AI for national economic prosperity and national security, clarifies the concept of artificial intelligence.

In 2019, **the Russian Federation** adopted the "Passport of the national project "National program "Digital economy of the Russian Federation", which highlighted the development of big data technology as one of the main directions contributing to the digital economy development. Besides, on

		<p>December 12, 2019, the “Data Ethics Code” was signed by the largest Russian companies, and by the Analytical Center under the Government of the Russian Federation, in order to consolidate the basic principles of interaction between stakeholders - the state, citizens and businesses, create the basis for subsequent regulatory initiatives in the data field, and form universal rules defining the limits of acceptable behavior for the entire professional community. In 2021, GOST R ISO/IEC 20546-2021 “Information Technology. Big Data. Overview and Dictionary”, which fixed the main terms related to big data technologies.</p> <p>The artificial intelligence technologies regulation was laid down by Decree of the President of the Russian Federation “On the Development of Artificial Intelligence in the Russian Federation” dated October 10, 2019 No. 490 with the approval of the “National Strategy for the Development of Artificial Intelligence for the period up to 2030”, in order to ensure the accelerated development of artificial intelligence, conduct scientific research in the field of artificial intelligence, increasing the availability of information and computing resources for users, as well as improving the system of training in this area. As part of the program to support AI developers, about 1,200 companies are expected to receive a total of more than 17 billion rubles by 2024 to develop AI technology. In 2020, a five-year experiment was launched to introduce artificial intelligence technologies in Moscow as part of the National Program “Digital Economy of the Russian Federation” (Federal Law No. 123-FZ of April 24, 2020 “On conducting an experiment to establish special regulation in order to create conditions for the development and implementation of artificial intelligence technologies in the subject of the Russian Federation - the city of federal significance Moscow and amendments to Articles 6 and 10 of the Federal Law “On Personal Data”). Besides, Decree of the Russian Federation Government dated August 19, 2020 No. 2129-r approved the “Concept for the development of regulation of relations in the field of artificial intelligence and</p>
--	--	--

		<p>robotics technologies for the period up to 2024”, the purpose of which is to determine the main approaches to transforming the system of regulatory legal regulation to ensure the possibility of creation and application of artificial intelligence and robotics technologies in various sectors of economy, while respecting the rights of citizens and ensuring the security of the individual, society and the state, at the same time, the following goals are pursued: creating prerequisites for the formation of foundations for the legal regulation of the new social relations emerging due to the development and application of artificial intelligence technologies and robotics and systems based on them, and identification of legal barriers that prevent the development and use of these systems. In 2020, two AI standards were approved: GOST R 59276-2020 “Artificial Intelligence Systems. Ways to ensure trust. General provisions” and GOST R 59277-2020 “Artificial Intelligence Systems. Classification of Artificial Intelligence Systems.” The Alliance in the field of artificial intelligence, the Analytical Center under the Government of the Russian Federation, and the Ministry of Economic Development of the Russian Federation developed and signed (10/26/2021) the “Code of Ethics for Artificial Intelligence”, which established general ethical principles and standards of behavior that should guide the participants in relations in the field of artificial intelligence, in their activities.</p>
--	--	--

### Comments

In the Kyrgyz Republic, there is no normative-legal regulation of big data technology and artificial intelligence, or the conceptual framework of these technologies is not fixed.

The issue of legal regulation of the collection, processing and use of big data is quite complex and composite. The complexity of regulation makes it difficult to distinguish between favorable regimes and restrictions on the use of big data. The benefits of using big data seem attractive for both the economic sphere and the sphere of public administration. However, at the same time, the use of big data threatens privacy, the equality of citizens, by imposing an aggressive policy of collecting personal consumer data (a condition for access to products and services is compliance with the rules of use, which are often just a means of obtaining personal consumer data); processing open information in social media about the bank's customers, for the priority right to receive loans based on the information collected; receiving free services, in exchange for providing personal data, etc. In addition, legal regulation is not currently able to adequately resolve all issues. Strict legal frameworks will significantly limit the

possible benefits, while the lack of a legal framework creates the risk of a “gray” zone in the circulation and use of big data.

The development of artificial intelligence technology poses serious challenges to the legal system, the system of state governance, and society as a whole. They are due to a certain degree of autonomy of actions of artificial intelligence systems in solving the tasks and their inability to perceive ethical and legal provisions, take them into account when performing any actions. The commercialization of artificial intelligence, such as facial recognition, image recognition technologies, speech recognition, natural language understanding, user portraits, etc., is rapidly advancing, making artificial intelligence technologies a new driving force leading to socio-economic development. As a consequence, the development of artificial intelligence technology requires the creation of a regulatory environment that is comfortable for safe development and implementation, based on a balance of interests of a man, society, government, companies - developers of artificial intelligence, and consumers of their goods, works, and services.

However, Decree of the Kyrgyz Republic President “On the National Development Program of the Kyrgyz Republic until 2026” dated October 12, 2021, UE No. 435, provides for a management reform that includes full automation of management processes, through the introduction of the concept of “Data-Based Governance” , according to which all decisions should be based on the Big Data analytics accumulated by public and private systems, and launch of the project “Artificial Intelligence as a Big Data Database”, and the “Action Plan of the Cabinet of Ministers” approved by Resolution of the Kyrgyz Republic Government for implementation of the National Development Program of the Kyrgyz Republic to 2026” dated December 25, 2021 No. 352, assigns those responsible for fulfillment of tasks, deadlines and funds that will be allocated for the implementation of these activities.

At the same time, a review of successful practices and approaches to legal regulation of these technologies has shown that there are various practices and approaches in the world practice, each of which has its positive and negative sides. Taking them into account, it seems most promising to implement a method based on combining the experience of different countries in terms of implementing the best practices of each approach studied, which will create the necessary conditions for the digital economy development in the Kyrgyz Republic.

Thus, the legal regulation of big data technology and artificial intelligence should include, but not be limited to, the following elements:

- terms and definitions, according to the best international standards (ISO/IEC, NIST);
- fundamental regulatory principles (free movement mode for data, data accessibility and portability, etc.);
- rights and obligations of subjects (big data principals, operators and users; developers, users and operators of AI);
- localization requirements for certain types of data (financial, medical and biometric data) or cross-border transfer with the consent of the data subject (alternatively, the transfer of the specified list of data after anonymization (a process, by which data are irreversibly changed so that the data subject can no longer be identified directly or indirectly);
- Increasing the use of government data for research and development, while ensuring the security and confidentiality of such data;
- requirements and restrictions imposed on the AI systems (requirements for AI systems, the use of which may cause harm, requirements to notify individuals about interaction with AI systems, restrictions on AI systems, the use of which may be unsafe for people);
- measures to support innovation in the field of AI (creation of regulatory sandboxes, priority access of SMEs and startups to regulatory sandboxes);
- definition of the authorized body in the field of AI;
- development of codes of ethics and other mechanisms for ethical regulation of the development, implementation and use of AI technologies.

## Section 9. National spatial data infrastructure

### Content

- Spatial data infrastructure
- Spatial metadata
- Principles and rules of the spatial data infrastructure use

### Current regulation (existing legislation):

1. Criminal Code of the Kyrgyz Republic;
2. Code of Administrative Offences of the Kyrgyz Republic;
3. Law of the Kyrgyz Republic "On geodesy and cartography" dated March 20, 2002, No. 43;
4. Decree of the Kyrgyz Republic President "On the National Development Program of the Kyrgyz Republic to 2026" dated October 12, 2021, UP No. 435;
5. Resolution of the Kyrgyz Republic Government "On the Ministry of Agriculture of the Kyrgyz Republic" dated March 9, 2021, No. 83;
6. Resolution of the Kyrgyz Republic Cabinet of Ministers "On subordinate subdivisions and organizations of the Ministry of Agriculture, Water Management and Regional Development of the Kyrgyz Republic" dated August 6, 2021, No. 116;
7. Resolution of the Kyrgyz Republic Government "On approval of the Instruction on defining and ensuring secrecy of topographic-geodetic, cartographic, gravimetric, aerial-photo survey materials and space survey materials on the territory of the Kyrgyz Republic" dated November 11, 2013, No. 622;
8. Resolution of the Kyrgyz Republic Government "On approval of the Regulation on the rules of writing and applying measurement units in the Kyrgyz Republic" dated March 6, 2013, No. 119;
9. Resolution of the Kyrgyz Republic Government "On the interdepartmental commission to review issues of administrative-territorial structure and geographic names under the Cabinet of Ministers of the Kyrgyz Republic" dated August 19, 2008, No. 467;
10. Resolution of the Kyrgyz Republic Government "On establishing a unified state coordinate system (KyrG-06)" dated October 6, 2010, No. 235;
11. Resolution of the Kyrgyz Republic Cabinet of Ministers dated January 12, 2022 approved the Action Plan for Governance Digitalization and Development of the Digital Infrastructure in the Kyrgyz Republic for 2022-2023, No. 2-r.

### Brief description of the identified shortcomings and international practice benchmarks

No.	Shortcomings	Type <sup>22</sup>	Best practices
9.1	The Law of the Kyrgyz Republic "On geodesy and cartography" is outdated and does not meet the existing needs to ensure legal regulation of spatial data. The law lacks sufficient conditions for the creation and development of the national infrastructure	O	The legislations of Korea and South Africa provide for a comprehensive approach to the legal regulation of the NSDI creation and development. The concepts of NSDI, metadata, rights and obligations of the NSDI subjects and powers of the coordinating body on NSDI are enshrined in the legislation of these countries. The legislations of these countries provide for spatial data standards, collection, storage, protection, accounting for spatial data and requirements for databases in detail. As for NSDI development, the legislation of the Republic of Korea provides for analyzing stakeholders' needs for spatial data.
9.2.	NSDI related terms and definitions are missing at all	G	General definitions of the NSDI, metadata, geoportal and other terms are outlined in the legislation of almost all countries with adequate NSDI regulation (USA, South Africa and Korea). Basic concepts are legally enshrined even in Kazakhstan and the Russian Federation. The CIS Model SDI Code being developed has the most complete list of terms and definitions and can be used as the basis for the development of new normative legal regulation.
9.3	The legislation of the Kyrgyz Republic does not regulate spatial metadata related issues	G	The South Africa NSDI Act dated January 28, 2004 (SPATIAL DATA INFRASTRUCTURE ACT 54 OF 2003) defines metadata and establishes general issues of its regulation. The procedure for metadata collection and publication is enshrined in subordinate legislation. The Russian Federation has GOST R 52573-2006 "Metadata" establishing a methodology of metadata formation and defining: - a basic set of metadata necessary and sufficient for basic operations, such as data retrieval, determination of data compliance with the requirements, access to data and its use;

<sup>22</sup> The following types of regulatory shortcomings are listed in the Table:

- (G) regulatory gap (regulation is required, but it is missing)
- (O) obsolete provision (the existing provision should be changed)
- (N) non-functioning provision (the existing provision is non-functioning for the reasons described)
- (B) this provision is an unreasonable barrier to the implementation of activities

			<ul style="list-style-type: none"> <li>- mandatory and conditional metadata packages, metadata entities and elements;</li> <li>- additional (optional) metadata elements that allow using their extended descriptions if needed.</li> </ul>
<b>9.4</b>	Principles for the creation and development of the spatial data infrastructure are missing	<b>G</b>	<p>The draft model NSDI Act within the EAEC establishes the following principles for the NSDI formation:</p> <ul style="list-style-type: none"> <li>- obligatory use of the regulated coordinate systems and existing basic spatial data by the state authorities, local governments and self-governments and other entities when creating state information resources and new basic spatial data;</li> <li>- the subordination of the SDI creation and development processes to the priority tasks of socio-economic development of the country, environmental protection, environmental security, public administration, defense and national security of the country;</li> <li>- mandatory coordinate description of spatial objects when creating state information resources;</li> <li>- relevance, reliability, completeness, integrity and established accuracy of spatial data;</li> <li>- the compatibility of spatial data based on the use of a unified bank of basic spatial data, regulated coordinate systems, unified technical regulations and standards;</li> <li>- priority use of spatial objects with the coordinate data having the highest established accuracy, completeness of description, reliability and legal significance;</li> <li>- interoperability of geoservices, basic spatial data and their metadata;</li> <li>- harmonization of technical regulations, SDI national standards with the relevant international standards;</li> <li>- stage-by-stage approach in the SDI creation and development as a complex organizational and technical system characterized by the indefinite functioning, development and continuous improvement using a comprehensive and programmatic approach;</li> </ul>

			<ul style="list-style-type: none"> <li>- openness and accessibility of basic spatial data and its metadata to all stakeholders;</li> <li>- planning the sequence of creation and updating basic spatial data sets;</li> <li>- state support for the creation and updating of the basic spatial data sets.</li> </ul>
<b>9.5</b>	The current regulatory legal acts of the Kyrgyz Republic do not regulate the collection, storage, processing, distribution, protection and use of spatial data at all	<b>G</b>	The legislations of the Republic of Korea and South Africa provide for detailed rules and procedures for the collection, storage and publication of spatial data. Furthermore, this procedure in Korea stipulates functions of each responsible authority at each stage of the process of collection and storage of spatial data.
<b>9.6.</b>	Spatial data standardization issues are not legally regulated	<b>G</b>	In practice the State Agency "Goskartografiya" (State Cartography) under the Land Resources Service under the Ministry of Agriculture of the Kyrgyz Republic strives to use uniform standards, create a unified geodatabase and ensure that different entities use uniform standards when creating spatial data. At the same time, in order to address these issues, the normative legal mechanisms for spatial data standardization should be enshrined.

### Comments

As shown by the review and analysis of the current regulatory framework of the Kyrgyz Republic and analysis of the practices of foreign countries, the existing regulatory framework of the Kyrgyz Republic is outdated and does not meet the current needs to ensure legal regulation of spatial data. Many developed countries began to create and develop their national spatial data infrastructures (NSDI) about 20 years ago and even earlier, while the Geodesy and Cartography Law was adopted in the Kyrgyz Republic in 2002 and compared with the regulations of the Republic of Korea, USA and South Africa was already quite archaic and had not even a hint at the introduction and application of new technologies in the field of geodesy and cartography. Moreover, this Law does not provide sufficient conditions for creating and developing the national spatial data infrastructure, thereby jeopardizing the implementation of the national strategic documents. The above Law, which is the main law in this sphere, does not correspond to modern development trends and at least most of its provisions shall be revised and the development and adoption of a new Law might be required. At the subordinate level, attempts to ensure legal regulation are fragmented. At the legislative level, the concepts of spatial data, spatial data objects, spatial metadata, not to mention the procedures and rules for preservation, processing, using, providing access, data exchange, updating, standards, and protection of spatial data are not enshrined.

Based on the review and analysis of the existing regulatory framework, in general the NSDI creation and development in terms of legal and institutional aspects is characterized by the following issues:

1. There is currently no authorized body to coordinate the activities of the state bodies, local authorities, commercial and scientific organizations in the field of NSDI creation and development.
2. The current normative legal acts do not clearly stipulate the powers of the state bodies involved in spatial data creation and development.
3. The procedure for interaction between subjects of spatial data is missing;
4. Spatial data exchange, rules and procedures for updating spatial data, and access to spatial data are not regulated;
5. Spatial data standardization issues are not regulated.

In this regard, to ensure adequate regulation of the NSDI creation and development, the Law of the Kyrgyz Republic "On Geodesic and Cartographic Activities" shall be significantly revised. Given the number of necessary changes, it might be appropriate to draft a new Spatial Data Law based on the legal regulation experience of the Republic of Korea.

The development of new normative legal acts including subordinate normative legal acts should primarily aim at:

- Revision of the terms and definitions in the current normative legal acts in the field of geodetic and cartographic activities;
- Introduction of the NSDI creation and development principles;
- Determining the NSDI organizational structure;
- Establishing and enshrinement of the powers and responsibilities of all parties for the NSDI creation and functioning;
- Approving in accordance with the established procedure the regulations for interaction (including interdepartmental interaction) and formats for spatial data exchange between the developers, right holders and users of NSDI;
- Approval of standards regulating NSDI functioning in accordance with the established procedure;
- Observance of property rights when creating and using NSDI data;
- Addressing the issues of collection, storage, processing, distribution and protection of NSDI;
- Establishing responsibility for violation of legislation in the field of NSDI.

## Section 10. Electronic message, record and document

### Content

- Legal treatment of electronic messages
- Legal treatment of digital records, creation and use of digital records
- Electronic documents: legal treatment of documents, copies and originals, transfer between media, etc.

### Current regulation (existing legislation):

1. Civil Procedure Code of the Kyrgyz Republic
2. Criminal Procedure Code of the Kyrgyz Republic
3. E-Governance Law of the Kyrgyz Republic
4. Electronic Signature Law of the Kyrgyz Republic
5. Innovation Activities Law of the Kyrgyz Republic
6. Virtual Assets Law of the Kyrgyz Republic
7. E-Commerce Law of the Kyrgyz Republic
8. Law of the Kyrgyz Republic "On Telecommunications and Postal Service"
9. Law of the Kyrgyz Republic "On biometric registration of citizens of the Kyrgyz Republic".
10. Resolution of the Kyrgyz Republic Government "On certain issues related to the use of electronic signature" dated December 31, 2019, No. 742;
11. Resolution of the Kyrgyz Republic Government "On approval of the Regulation on the state system of telecommunications and rules of its use" dated December 31, 2019, No. 745;
12. Resolution of the Kyrgyz Republic Government "On approval of the Regulation on the automated information system "State Electronic Document Management System" dated October 30, 2020, No. 526;
13. Resolution of the Kyrgyz Republic Government "On model instruction on record keeping in the Kyrgyz Republic dated March 3, 2020, No. 120.

### Brief description of the identified shortcomings and international practice benchmarks

No.	Shortcomings	Type <sup>23</sup>	Best practices
10.1	The current legislation of the Kyrgyz Republic (Electronic Signature Law and E-Governance Law of the Kyrgyz Republic) is outdated, because it regulates electronic document management as an auxiliary, alternative one to paper-based document management or has significant transitional mechanisms allowing to preserve paper-based document management, where there is no need for this. Instead, the legislation shall enshrine mechanisms that encourage the transition to purely digital interactions in various areas and provide for the elimination of paper-based documents	O	The US legislation provides for complete elimination of paper-based documents based on the Government Paperwork Elimination Act (GPEA) for already more than 20 years. It requires that, when practicable, federal agencies use electronic forms, electronic records and electronic signatures in their official activity with the public. The Act established that agencies must, by October 21, 2003 allow individuals or entities dealing with agencies to provide information or transact with the agency electronically when practical, and to maintain electronic records when practicable. The Act specifically states

<sup>23</sup> The following types of regulatory shortcomings are listed in the Table:

- (G) regulatory gap (regulation is required, but it is missing)
- (O) obsolete provision (the existing provision should be changed)
- (N) non-functioning provision (the existing provision is non-functioning for the reasons described)
- (B) this provision is an unreasonable barrier to the implementation of activities

			<p>that electronic records and related electronic signatures should not be denied validity, authenticity or enforceability simply because they are submitted in an electronic form, and encourages the federal government to use a range of signature alternatives.</p>
<p><b>10.2</b></p>	<p>The Kyrgyz Republic has not fully deployed the infrastructure for electronic signatures or other more modern methods of identity management, while the applicable standards are commercial and are developed by the Russian Federation and the Republic of Kazakhstan, which entails dependence of the domestic market of the Kyrgyz Republic. It is necessary to introduce the requirements, rules and standards for electronic signatures generation at the national level in accordance with the international requirements, and simultaneously adopt uniform requirements for electronic signature certificates at the Eurasian Economic Union level</p>	<p><b>N</b></p>	<p>The most relevant practice at the international level is summarized and presented as a legal text in the UNCITRAL Draft Model Law on the Use and Cross-Border Recognition of Identity Management and Trust Services and Guidelines on the model Law implementation.</p> <p>Despite the diversity in the electronic signature types and legal models that mediate their use, the approaches to the legal regulation of electronic signatures can be classified into three types.</p> <p>The first approach, the "minimalist" one, aims to recognize the legal value of electronic signatures and electronic documents and to create legal conditions for their use by removing from the existing legislation the norms that impede the use of electronic signatures. In this case, no new legal mechanisms are created; the only exception is a set of norms asserting "technological neutrality", i.e. the legislation is not bound to any technology of electronic signatures formation. This approach is used, for instance, in the USA based on the E-SIGN Act 2000.</p> <p>The second approach is based on the recognition of electronic digital signatures only; thus, it is linked to a single public key technology. Electronic digital signatures and the documents signed using them are recognized by legislation, but they are subject to particular requirements which differ from those applied to paper-based documents and handwritten signatures. The use of electronic digital signatures is subject to a "public key infrastructure" made up of certification centers that act as intermediaries between digital signature</p>

			<p>holders and recipients of authenticated documents.</p> <p>The third approach is a hybrid of the first two. On the one hand, it does not leave the majority of electronic signatures beyond the regulation scope, as is the case with the second approach. The legislation recognizes all kinds of electronic signatures, both already in use and those which may arise in the future. On the other hand, the legislation guarantees certain reliability of documents signed using electronic signatures by outlining "reinforced" electronic signatures; as a rule, reinforced signatures are those which use the public key technology.</p>
<b>10.3</b>	The judiciary bodies do not currently recognize digital evidence in court proceedings because of a lack of competence and understanding of the digital legislation	<b>N</b>	All court proceedings in Great Britain and the US are electronic at their core, which, in addition to convenience and speed of handling documents, allows all parties to a case, including the judge, access to the same set of evidence existing electronically. This not only reduces corruption risks, but also virtually eliminates any potential discrimination in access to justice.
<b>10.4</b>	The procedure for preservation of electronic documents, records (information) in digital form, the legislation on digital (electronic) archives are missing	<b>G</b>	<p>The problems of long-term storage of documents originally created in electronic form in <b>Estonia</b> are increasingly addressed at the agency (organization) level. For this purpose, a special computer program the Universal Archiving Module (UAM) was created, which is available on the website of the National Archive of Estonia, intended for the archivists of an organization and allows exporting data from the electronic document management system (EDMS) to the organization's archive. The main functions of UAM meet all the technical and archival requirements for the successful preparation of documents and their metadata for transfer from an institution to the state archive.</p> <p>UAM is essentially just an intermediate device needed in the period between documents exporting from the EDMS and placing them in a permanent storage.</p>

		location. UAM has been used in practice since 2010 to transfer documents to the digital archive. The National Archives is in constant contact with all ministries and helps them to complete the transfer (import) of documents using UAM. This software module is thus a single, universal tool for transferring electronic documents from operational management to the public archives.
--	--	--

### Comments

Basic comments on the development of modern concepts of digital interaction and transition from electronic document management to management based on data presented as records in information systems and information resources as basic sources of information are presented in relation to Section 3 of this analysis. This Section discusses the legislative shortcomings related to the use of electronic documents and transition to electronic document management.

The current legislation of the Kyrgyz Republic (Electronic Signature Law and E-Governance Law of the Kyrgyz Republic) is outdated, as it regulates electronic document management as an auxiliary, alternative to paper-based document management or contains significant transitional mechanisms that allow maintaining paper-based document management where it is not necessary. Instead, the legislation shall enshrine mechanisms that encourage the transition to purely digital interaction in various spheres and provide for the elimination of paper-based document circulation. The US Government Paperwork Elimination Act (GPEA) has been the global benchmark in this area for nearly 20 years, requiring that, when practicable, federal agencies switch to electronic forms, electronic records and electronic signatures in their official activity with the public by 2003. The Act requires agencies to allow individuals or entities dealing with agencies to provide information or transact with the agency electronically when practical, and to maintain records electronically when practicable. The Act specifically states that electronic records and related electronic signatures should not be denied validity, authenticity or enforceability simply because they are in an electronic form, and encourages the federal government to use a range of signature alternatives.

The Act seeks to "prevent agencies or courts from systematically treating electronic documents and signatures less favorably than their paper-based alternatives" so that citizens can interact with the federal government electronically. The Act also addresses whether private employers can use electronic means to store and transmit information concerning their employees to federal agencies. The GPEA states that electronic records and related electronic signatures should not be denied validity, authenticity or enforceability simply because they are submitted electronically. It also encourages the federal government to use a range of signature alternatives.

The Act is technologically neutral, meaning that the law does not require the government to use one technology instead of another one. This approach has both advantages and disadvantages. By remaining neutral, it allows each government agency to decide which technology fits its particular needs. It also means that the government is not limited to using old technology as new and better systems become available. As a disadvantage, some may argue about which signature capture method is best, and such disagreements can slow down the implementation process.

Despite the variety of types of electronic signatures and the legal models that mediate their use, **approaches to the legal regulation of electronic signatures use** can be classified into three types<sup>24</sup>.

The first approach, the "minimalist" one, aims to recognize the legal value of electronic signatures and electronic documents and to create legal conditions for their use by removing from the existing legislation the norms that impede the use of electronic signatures. In this case, no new legal

<sup>24</sup> See: *Spyrelli, Christina*. Electronic Signatures: A Transatlantic Bridge? An EU and US Legal Approach Towards Electronic Authentication // *The Journal of Information, Law and Technology (JILT)* 2002(2).

mechanisms are created; the only exception is a set of norms asserting "technological neutrality", i.e. no the legislation is not bound to any technology of electronic signatures formation. This approach is used, for instance, in the USA based on the *E-SIGN Act 2000*<sup>25</sup>.

The second approach is based on the recognition of electronic digital signatures only; thus, it is linked to a single public key technology. Electronic digital signatures and the documents signed using them are recognized by legislation, but they are subject to particular requirements which differ from those applied to paper-based documents and handwritten signatures. The use of electronic digital signatures is subject to a special mechanism, the so-called "public key infrastructure", which is made up of certification centers that act as intermediaries between digital signature holders and recipients of authenticated documents. The responsibilities of such centers include the issuance of digital signature keys, maintenance of a register of such keys and authentication (verification) of signed documents. *Certification centers* are subject to certain requirements, which include, as a rule, minimum financial guarantees of compensation for damages in the event that such damages are caused by a failure in their operation (delayed or erroneous signature authentication).

The third approach, let's call it the "two-tier" approach, is a hybrid of the first two ones. On the one hand, it does not leave most electronic signatures beyond the regulation framework, as is the case with the second approach. The legislation recognizes all kinds of electronic signatures, both already in use and those which may arise in the future. On the other hand, the legislation guarantees certain reliability of the documents signed using electronic signatures through separation of "reinforced" electronic signatures; as a rule, signatures using the public key technology are considered reinforced. The requirement of using reinforced electronic signatures is set for certain types of legal relations demanding greater formality than usual (relations with governmental authorities, foreign trade transactions and some others). On the one hand, this approach allows for a universal legislative model capable of adapting to future changes in signature technologies; on the other hand, it makes it possible to guarantee the appropriate reliability of electronically certified documents in cases where this is rather important. The two-tier approach is stipulated in a number of international level acts, such as *MLES*<sup>26</sup> and *eIDAS Regulation*<sup>27</sup>.

The "minimalist" approach is recognized as the most effective in terms of identification and authentication in international commerce among the above three approaches, although unlike the other two, it does not provide any serious guarantee of reliability and trustworthiness of electronically signed documents, however, it does not restrict acceptance of a wide range of electronic signatures originating from different national legal regulatory models for electronic signatures. As this approach is based more on the electronic signatures functions than on the technologies used to form them and the way in which these functions are translated into concrete information exchange technologies, it also allows for achieving considerable progress in harmonizing the legislation of different countries regarding electronic signatures.<sup>28</sup>

Back in the 1990s, the EU adopted two Directives governing electronic signatures use: 1999/93/EC on Electronic Signatures and 2000/31/EC on Electronic Commerce. The e-signature Directive is much like the *MLES* in terms of its content, but their structure is slightly different. Whereas *MLES* focuses on signature validity issues and the rights and obligations of the parties, the Directive seeks primarily to create an organizational apparatus for dealing with electronic signatures and to establish a framework for its operation. In 2014, the structure of electronic signatures regulation in the EU was changed and the Directive was replaced by a Regulation (eIDAS) covering identification services and trust services in addition to electronic signatures. The *eIDAS Regulation*, in turn, is one of the elements of the EU *Digital Single Market* strategy. Therefore, the main principle of regulation outlined in the very beginning (Article 4) is the internal market principle. According to it, free circulation on the internal market of products and trust services complying with the requirements of the Regulation

<sup>25</sup> Electronic Signatures in Global and National Commerce Act 2000.

<sup>26</sup> UNCITRAL Model Law on Electronic Signatures, 2001// <https://base.garant.ru/2567278/>.

<sup>27</sup> Regulation (EU) № 910/2014 of the European Parliament and of the Council.

<sup>28</sup> See: Spirelli, Christina. Op. cit. P. 7.

should be allowed and there should be no restrictions on the provision of trust services in the territory of an EU Member State by a trust service provider established in another EU Member State.

As for electronic signatures, the Regulation implements a two-tier approach. Any electronic signature cannot be regarded as lacking legal effect or recognized as inadmissible evidence in court proceedings merely on the grounds that it is in an electronic form or does not meet the requirements for a qualified signature. At the same time, only a qualified electronic signature has the same legal effect as a handwritten signature. A qualified electronic signature based on a qualified certificate that has been issued in one EU member state is recognized as a qualified electronic signature in all EU member states.

According to the Regulation, an enhanced electronic signature must meet the following requirements:

- (a) it is uniquely linked to the signatory;
- (b) it is capable of identifying the signatory;
- (c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and;
- (d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

The electronic signature authentication process shall confirm the validity of the electronic signature provided that:

- (a) the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with the requirements;
- (b) the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing;
- (c) the signature validation data corresponds to the data provided to the relying party;
- (d) the unique set of data representing the signatory in the certificate is correctly provided to the relying party;
- (e) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;
- (f) the electronic signature was created by a qualified electronic signature creation device;
- (g) the integrity of the signed data has not been compromised;
- (h) the system used to verify the electronic signature must provide the relying party with the correct results of the verification process as well as allow the relying party to identify any aspects important to information security.

When comparing two documents of the two international organizations, the *MLES UNCITRAL* and the *EU eIDAS* Regulation, one can find a difference in approaches to the electronic signatures regulation. They both define the concept of electronic signature in the same way and create the same structure of legal relations "sender-receiver-certification center". But the approach of the Regulations is more exact and tough. The rights, duties and responsibilities of the parties are established, the signature recognition criteria become a closed list and focus is on certification. This leads to unification within the Community, but complicates interaction with other states. Having first adopted the Directive on the electronic signatures use and then the Regulation on identification services, the EU failed to solve the problem of incorporating its information and legal space into the global one. According to Article 14 of the Regulation, the identification services from a third country are recognized only based on the international treaty between the EU and that third country or international organization.

In the United States, two documents were adopted at the federal level. The first was the Model *Uniform Electronic Transactions Act, 1999 (UETA)*. The second was the *Electronic Signatures in Global and National Commerce Act, 2000 (E-sign Act)*<sup>29</sup>. They became the basis for the laws on electronic signatures currently adopted in 49 states.

*UETA* was not originally designed as a Code, i.e. a comprehensive act covering all possible applications of electronic signatures, but as a model law adapting existing legislation to a new type of activity. The official commentary on *UETA* emphasizes that: "...The purpose of *UETA* is to overcome

---

<sup>29</sup> Available at [http://www.law.upenn.edu/bll/ulc/ulc\\_final.htm](http://www.law.upenn.edu/bll/ulc/ulc_final.htm)

existing obstacles to electronic commerce by giving legal effect to electronic documents and electronic signatures. *UETA* is not a statute codifying contract law - the basic rules of contract law remain unchanged. Nor is it a statute on electronic digital signatures. *UETA* is only intended to supplement and support electronic digital signature law already existing in the states".

The Act neither focuses on the technical side of the issue. The definition of an electronic signature here covers practically any way of signing (EDS, fingerprint, retinal scan, voice sample), the main thing is the intention of the signatory to sign the document - in the sense as it is used in the paper-based document flow. The Act neither mentions obligatory certification of signatures; it is a question of *bonafide* of the parties or expertise in the framework of court proceedings.

Generally, under the *UETA*, electronic documents and electronic signatures (mainly in commercial transactions, as this is the main subject of the Act) will be given the same legal effect as paper-based documents ("the form of presentation of a contract, other document or signature - electronic or paper-based - does not in itself give rise to differences in its legal recognition"). However, the Act establishes a number of exceptions to this rule, for example, real estate transactions, trusts and wills. The list of exceptions proposed by the Act is not very clear, but it is quite obvious; it does not vary much from state to state.

The *E-Sign Act* settled the issue of electronic signatures directly at the federal level. It repeats the *UETA* rule of equal recognition of electronic and paper-based signatures, electronic and paper-based documents. It is emphasized that a signed document can entail both positive and negative consequences, for example in case of fraud, signing without legal authority, as well as in other cases under civil law (rules on defects of will and willfulness).

The *E-Sign Act* also deals with some special cases of using electronic signatures. For example, an electronic signature may be notarized (also electronically). The scope of application of electronic signatures is limited in matters of inheritance, family law, judicial decisions, other relations involving public authorities, and the transfer of items dangerous to human life and health. Particular attention is paid to the use of electronic signatures in the relations involving consumers: here the right of consumers to receive all necessary information related to the use of an electronic signature is stipulated, the possibility of the consumer to revoke his/her signature and consequences of such revocation are considered.

The Act implements a "minimalist" approach to the recognition of foreign electronic signatures. The provision in paragraph (1) of Article 301 of the Section "Promotion of International Electronic Commerce", which contains a sort of preamble to the entire Section, provides for the Federal Secretary of Commerce (who is the state agency responsible for implementing the *E-Sign Act*) to "take all measures ... necessary to remove or reduce as far as possible obstacles to trade when using electronic signatures to facilitate interstate and foreign commerce".

In order to eliminate obstacles to international trade as much as possible, the Foreign Signature Recognition Mechanism includes just a few principles:

- (A) *A.* "Remove paper-based obstacles to electronic transactions by adopting relevant principles from the 1996 *MLEC* principles". The principle seeks to remove obstacles to the use of electronic documents based solely on the fact that such documents were not executed in "paper-based" form, and is fully implemented in the *E-Sign Act*.
- (B) *B.* "Permit parties to a transaction to determine the appropriate authentication technologies and implementation models for their transactions, with an assurance that those technologies and implementation models will be recognized and enforced". The principle embodies the general conditions of *optionality* (freedom of the parties to determine technologies to be used as electronic signatures and to determine the models of using electronic signatures at their own discretion) and *legal protection* (transactions performed on the basis of an agreement between the parties to use electronic signatures are given full legal effect as if they had been performed in "paper" form). But it is worth noting once again that the use of electronic signatures based on the agreement of the parties poses certain problems.

- (C) C. "Permit parties to a transaction to have the opportunity to prove in a court or other proceedings that their authentication approaches and their transactions are valid". This principle in fact refers to the possibility of recourse to a court to prove the validity of an agreement to use electronic signatures and the validity of the transactions concluded on its basis. Although the *E-Sign Act* does not establish substantive rules concerning the validity of such transactions, the procedural safeguards are extremely important: they overcome difficulties in concluding an agreement on the use of electronic signatures referred to in the previous paragraph.
- (D) D. "Take a nondiscriminatory approach to electronic signatures and authentication methods from other jurisdictions". Despite the vagueness and potential ambiguous interpretation of this provision, it is (even in its most general form) fundamentally important: foreign signatures in the United States must be recognized equally as signatures formed in the United States. Consequently, it allows extending to foreign signatures all those requirements concerning the validity of electronic signatures established by the E-Sign Act for national electronic signatures.

This "minimalist" approach to the recognition of electronic signatures is a consequence of the "minimalist" approach to the regulation of electronic signatures in general. On the whole, US and EU laws demonstrate two different approaches to the international legal aspects of identification based on electronic signatures. The first suggests automatic recognition of foreign electronic signatures if they meet the requirements for validity of signatures set out in the national legislation. The second approach requires the signature or signature certificate were secured under the national legal system of the state, where recognition of the signature is required, first and foremost, by virtue of the relevant international treaty.

Issues of recognition and use of electronic documents and electronic records are relevant from the perspective of proof in court. In the USA, the Case Management / Electronic Case Files (CM/ ECF) filing system has proven to be very successful and was introduced in all federal courts of the country already in 2005. Since that time, the system has been continuously improved and actively used, since the US has established an obligation for parties to file electronically through CM/ECF. Today, paper filing in the US is used in court as an exception in case of special need. In this case, a party should write a "Non-Compliance with the Electronic Filing Obligation" statement. In order to help users, training on system usage is available in each court.

The Case Management / Electronic Case Files system allows courts to accept applications and provides access to filed documents online. In order to file documents using the CM/ECF system, one needs a login and password issued by the appropriate court. Electronic documents using the CM/ECF system are filed only in PDF format. Thus, the Case Management / Electronic Case Files (CM/ECF) system ensures electronic filing, while the Public Access to Court Electronic Records (PACER) system provides public access to court materials. Both systems are managed, but case files are accessed centrally through a common access system.

In US federal courts, evidence provision is governed by a separate legal act, the Federal Rules of Evidence. In December 2017, the Federal Rules of Evidence were amended to make it easier to authenticate data from electronic sources. The changes describe the process for authenticating documents provided, such as a printout from an Internet page or a document extracted from files stored on a personal computer. They also provide for the use of a digital identification process (hash value) to verify the authenticity of the electronic data.

E-justice elements are also being actively implemented in Great Britain. The main directions of its judicial system reform are:

- The transition to electronic document management at all stages of court proceedings, including the formation of information on the court case electronically;
- Online consideration of minor administrative offenses and criminal acts of low public danger not punishable by imprisonment, as well as civil disputes (with the claim value up to 25 thousand pounds);
- Handling most civil disputes via remote Internet access to court by 2022.

Electronic filing of documents, as well as public access to the electronic court case in Great Britain are available through the Electronic Working Pilot Scheme. The system operates in the specialized courts of the King's Bench Division and the Chancery Division of the High Court.

Since 2017, claims to the specialized divisions of the High Court of England and Wales dealing with disputes involving businessmen, are filed exclusively electronically using the Courts Electronic Filing system (CE-File). In addition, there is CaseLines, an online portal through which claims, complaints and evidence can be filed electronically, and Her Majesty's Online Court (HMOC), which allows cases to be heard online.

One of the major transition issues is now the archival legislation, which provides for the preservation of documents similar to the preservation of paper-based documents. There is a lack of procedures for the preservation of electronic documents and electronic information.

The **US National Archives' (NARA)** 2014-2018 Strategic Plan considers the receipt, preservation and accessibility of electronic documents as one of the challenges of the modern digital age and one of the main conditions for the success of the archives. The problem of document management and public records management in general was once again raised at the highest government level in the USA in 2011, when a special Memorandum "Government Records Management" was issued, which put forward the task for all federal agencies to switch to a maximum extent to electronic document management by 2019, including for documents with a permanent storage period. To do so, NARA needs to revise its guidelines for transferring permanent electronic records to the archives and regularly update its implementation requirements. Today, the US National Archives contains about seven hundred terabytes (TB) of electronic documents, of which 79 TB were received during President Bush's term and 250 TB during Obama's, indicating a significant intensification in the transfer of electronic documents to the Archives.

In Great Britain, a strategic plan "Archives Inspire: Plans and Priorities for Great Britain National Archives 2015-2019", has been developed to meet the objective of electronic document preservation. The plan consists of the five main areas, the first of which focuses on document expertise and research needed to maintain and improve records management in government agencies. In January 2017, the British National Archives published its new "Electronic Strategy" outlining the goal of becoming an innovative electronic archive that fundamentally redefines archival practice starting with foundational principles. Such an archive should ensure the long-term preservation of all kinds of electronic documents created by public authorities, not just those created in a few widely used formats.

The ideology of this plan was affected by the documents continuum model treating them as archival from the moment of their creation. That is why the National Archives of Great Britain has positioned itself as 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.

The **European Union** is also concerned with the permanent preservation of electronic documents. The E-ARK project (European Archival Records and Knowledge Preservation) has been developed and financed by the European Commission as part of the Information and Communication Technology Support Program included in the Competitiveness and Innovation Program. The project aims to ensure efficient document management related to the three main archival activities, namely, acquisition, preservation and reusability of archival information. The E-ARK project is a three-year multinational scientific research effort scheduled for implementation from February 1, 2014 to January 31, 2017. In addition to archives, it includes universities, ministries, foundations and state institutions.

The project priority is to create a pan-European methodology for archiving electronic documents based on the existing national and international practices in the field of authenticity and the possibility to reuse digital materials over a long period of time.

Apart from the above-mentioned project, some European states implement archival preservation of electronic documents quite effectively. The countries of Northern Europe are most actively involved in this process.

In **Estonia**, the problem of long-term preservation of documents originally created electronically is being solved at the agency (organization) level. For this purpose, a special computer program Universal Archiving Module (UAM) available on the website of the National Archive of Estonia was

created for the archivists of an organization and allows exporting data from the Electronic Document Management System (EDMS) to the organization's archive. The main functions of UAM meet all the technical and archival requirements for the successful preparation of documents and their metadata for transfer from an institution to the state archive. UAM is essentially just an intermediate device needed in the period between exporting documents from the EDMS and placing them in a permanent storage location.

UAM has been used in practice since 2010 to transfer documents to the digital archive. The National Archives is in constant contact with all ministries and helps them to complete documents transfer (import) using UAM. Thus, thanks to this software module, a single universal tool has been implemented to transfer electronic documents from the operational management to the state archive.

In the **Netherlands**, the work to create a unified national repository of electronic documents has been implemented since 2013. By now, the concept of the repository has been formed, appropriate processes have been regulated, the information architecture has been created, the metadata model for all state structures which are sources of acquisition of the Dutch archives has been designed, etc. At the same time, the National Archives developed a prototype of a digital repository for the documents of the central government, which corresponds to the OAIS (Open Archival Information System) model of building electronic data storage systems. In 2014-2016, the necessary infrastructure was created, and in 2017 it was planned to transfer all digitized and originally created electronic documents to the repository.

In this regard, archives of the Netherlands started pilot projects to receive documents from the electronic document management systems of the authorities and administrations. The Public Records Act of the Netherlands stipulates that government documents must be permanently archived for 20 years after their creation, but the national e-repository allows for documents to be accepted even up to the expiry of that period.

In **Finland**, the National Archives Service has developed standards for the Finnish electronic records management systems (known as Sähke, Sähke2) that define the metadata and functions required to operate in these systems. The Sähke requirements were first published in 2005 and updated in 2008. If the state and municipal institutions wish to keep permanent documents only in electronic form, they should meet the requirements stipulated by Sähke and obtain permission from the National Archives to store documents electronically. In addition, the standard also specifies how to transfer electronic documents for permanent preservation from an institution to the National Archives.

In recent years the National Archives of Finland received databases and registers from various government agencies for safekeeping. The main strategy of the National Archives is to preserve only the data, not the functionality, data processing rules or algorithms. The data are extracted from the database management system (DBMS) and separated from the database structures. National Archives does not set strict rules for data file formats. Instead, key requirements relate to mandatory metadata elements. Data description and transfer to the National Archives are performed using standardized transfer structures for ZIP information folders and metadata. Additional documentation regarding context, data origin, database management system (DBMS), data models, processing rules, and usability recommendations are also stored in PDF format. The question of what documentation should be included in a ZIP folder is decided on a case-by-case basis.

In the Sähke2 framework, the national archives have developed a ZIP-folder structure to ensure that documents from different electronic document management systems are transferred in a uniform structure to their long-term preservation service. The Sähke2 structure is also used when transferring databases and registry data. This approach ensures that all materials are transferred to the National Archives of Finland in a single structure with the same metadata.

In the **Federal Republic of Germany**, as a result of the rapid growth of electronic documents, a huge amount of data that is not actively used is on servers and document management systems in federal organizations. Federal organizations require that documents that are no longer in active use must be kept by the organization for 5 - 30 years. Thus, federal organizations are required to ensure that their materials are securely stored and can be used in 30 years. At the same time, the Federal Archive cannot handle such a large number of electronic documents and formats simultaneously after 30 years.

For this reason, a Digital Intermediate Archive is being created in the Federal Republic of Germany for federal organizations. Off-site storage of documents that are no longer of operational importance relieves the administrative systems for electronic document management from the documents that are not actively used anymore and contributes to a more efficient operation of the system. Federal organizations create an Information Presentation Package (ZIP), including master data in a compressed file and metadata in an XML file. This Package is sent through a secure network to the Digital Intermediate Archive Access Interface. The Information Presentation Package is then converted into a XAIP package and the metadata is extracted into a database for research. After verification and legalization, the XAIP package is saved and the federal organization gets its identification. The first data transfer and testing was scheduled for 2015.

In **France**, the VITAM Project (Valeurs Immatérielles Transférées aux Archives pour Mémoire – Intangible Values Transferred to Archives for Memory Preservation) for interinstitutional electronic documents archiving system was launched in 2011. VITAM aims to develop a modular software platform for document storage in ministries, adapted to their needs and specificities. It will also serve as a base for the development of software for the permanent preservation of electronic documents for scientific purposes in the National Archives and in the archives of the Ministries of Defense and Foreign Affairs.

In 2015, the VITAM project implementation slowed down. The 2016 publications no longer refer to the creation of a "super platform for the short-term, intermediate and permanent preservation of the electronic archives of the French central institutions", but only to the development of software "electronic archive" which the three pilot ministries and then other interested institutions could use. The pilot ministries currently implementing VITAM are the Ministry of Culture (AD-Essor project), the Ministry of Foreign Affairs (Saphir project) and the French Ministry of Defense (GardeV2-Archipel project).

In **Poland**, as part of the goal of improving digital efficiency of institutions, a project for the application of the EZD (Electronic Document Management) system at the level of public administration - Voivodeship Offices is being implemented. In the first quarter of 2012, preparations for the pilot implementation of the EZD system in several institutions of the consolidated administration of two voivodeships were initiated. Thus, the local public administration is equipped with a single and jointly developed system for electronic document management, which will enable electronic interaction between institutions through the e-PUAP platform (Electronic Public Administration Services Platform).

Considering solutions of different countries to ensure the long-term preservation of electronic documents, we can identify some common trends, which obviously can be implemented in the Kyrgyz Republic as well.

First, in order to ensure electronic documents preservation in accordance with the prescribed timeframes, information systems of organizations, where these documents are created and/or used for operational purposes, should implement certain functions enabling the selection of documents based on preservation timeframes. These systems should also guarantee document preparation for transfer to the information system of the archive in accordance with the requirements of the latter, i.e. archival requirements are embedded into the systems of operational work with documents.

Second, it is necessary to discuss a new organizational solution for the long-term preservation of electronic documents. The model, where documents from operational records management are transferred to the archive of their organization and then to the state archive, may be ineffective. The option, where electronic documents from different organizations (authorities) are transferred to a unified electronic documents archive with relevant software and hardware is considered more appropriate.

Thirdly, practice shows that under continuously improving information technologies, changes in the software and hardware and rapid obsolescence of all known electronic media, it is impossible to preserve electronic documents without conversion and migration procedures. It is necessary to find solutions to ensure their authenticity, integrity, reliability and suitability for long-term preservation.

## Section 11. Digital identification

### Content

- Identification methods (codes, tokens, signatures, biometric identification)
- identification means
- Identification systems

### Current regulation (existing legislation):

1. Constitutional Law of the Kyrgyz Republic "On Elections of the President of the Kyrgyz Republic and Deputies of Jogorku Kenesh of the Kyrgyz Republic" dated July 2, 2011, No.68 (in terms of identification of voters).
2. Constitutional Law of the Kyrgyz Republic "On Referendum of the Kyrgyz Republic", October 31, 2016, No. 173 (in terms of identification of voters).
3. E-Governance Law of the Kyrgyz Republic dated July 19, 2017, No. 127 (in terms of establishing the legal basis for a unified identification system).
4. Electronic Signature Law of the Kyrgyz Republic dated July 19, 2017, No. 128.
5. Law of the Kyrgyz Republic "On biometric registration of citizens" of July 14 2014, No. 136 (in terms of biometric data collection and processing).
6. Law of the Kyrgyz Republic "On virtual assets" dated January 21, 2022, No. 12 (the legal basis for a token as a means of validation of property and (or) non-property rights, including the rights of claim on other objects of civil rights).
7. Law of the Kyrgyz Republic "On payment system of the Kyrgyz Republic" dated January 21, 2015, No. 21 (in terms of identification of clients).
8. Law of the Kyrgyz Republic "On combating the financing of terrorist activities and legalization (laundering) of criminal proceeds" dated August 6, 2018, No. 87.
9. Law of the Kyrgyz Republic "On elections of Deputies of Local Keneshes" dated July 14, 2011, No. 98 (in terms of identification of voters).
10. Decree of the Kyrgyz Republic President "On urgent measures to enhance implementation of digital technologies in public administration of the Kyrgyz Republic" dated December 17, 2020, UP No. 64.
11. Resolution of the Kyrgyz Republic Government "On identification card - passport of a citizen of the Kyrgyz Republic of 2017 sample (ID card)" dated April 3, 2017, No. 197, including:
  - a. Regulation on the identification card - passport of a citizen of the Kyrgyz Republic of 2017 sample (ID card) (Annex).
12. Resolution of the Kyrgyz Republic Government "On certain issues related to the use of electronic signature" dated December 31, 2019, No. 742.
13. Resolution of the Kyrgyz Republic Government "On certain issues related to the state information systems" dated December 31, 2019, No. 744, including:
  - a. Requirements for the protection of information contained in the databases of the state information systems (Annex) (in terms of identification of users).
14. Resolution of the Kyrgyz Republic Government "On certain issues of electronic governance implementation in the Kyrgyz Republic" dated December 31, 2019, No. 748, including:
  - a. Regulation on the Unified Identification System of the Kyrgyz Republic (Annex 1);
  - b. Requirements for details and form (format) of the information presentation in electronic documents of state bodies, local self-governments, as well as in electronic documents that are citizens' appeals to the state bodies and local self-governments (Annex 2).
15. Resolution of the Board of the Kyrgyz Republic National Bank "On approval of the Regulation "On the minimum requirements for the provision of remote/distant services in the Kyrgyz Republic" dated April 15, 2015, No. 22/3, including:

- a. Regulation on the minimum requirements for the provision of remote/distant services in the Kyrgyz Republic (Annex).
16. Resolution of the Board of the Kyrgyz Republic National Bank "On approval of the Regulation "On the requirements for ensuring information security in commercial banks of the Kyrgyz Republic" dated May 26, 2010, No. 36/7, including:
  - a. Regulation "On the basic requirements for the activities of commercial banks when entering into the agency agreement for the provision of banking retail services" (Annex).
17. Resolution of the Board of the Kyrgyz Republic National Bank "On approval of the Regulation "On the requirements for ensuring information security in commercial banks of the Kyrgyz Republic" dated December 22, 2021, No. 2021-P-20/72-8-(NPA), including:
  - a. Regulation on information security requirements in commercial banks of the Kyrgyz Republic (Annex).
18. Resolution of the Board of the Kyrgyz Republic National Bank "On approval of the Concept of Digital Payment Technology Development in the Kyrgyz Republic for 2020-2022" dated March 27, 2020, No. 2020-P-14/17-4-(PS), including:
  - a. The Concept of development of digital payment technologies in the Kyrgyz Republic for 2020-2022 (Annex).
19. Resolution of the Board of the Kyrgyz Republic National Bank "On the Procedure for remote identification and verification of customers" dated May 13, 2020 No. 2020-P-12/27-1-(NPA), including:
  - a. Procedure for remote identification and verification of customers (Annex).

#### Brief description of the identified shortcomings and international practice benchmarks

No.	Shortcomings	Type <sup>30</sup>	Best practices
11.1	<p>The legislation governing the use of the identification card - a citizen's passport (ID card) does not allow using this tool widely.</p> <p>The electronic chip in the ID card contains necessary biometric data (a color image of the face, graphic structure of the fingerprints on both hands, holder's handwritten signature) and the electronic digital signature key.</p> <p>However, the legislation does not contain any legal possibilities for using ID cards for digital (electronic) identification. For example, biometric identification technologies are used for voter identification at polling stations, but not an ID-card</p>	N	<p>Identification cards as a means of identification have become widespread in the <b>European Union</b>. The use of an electronic identification card in accordance with the Directives 2002/21/EC, 2009/140/EC, 2002/20/EC, 2009/140/EC allows to implement a two-factor verification process: a user's data is checked first, then each step in an electronic transaction requires a digital signature, which guarantees a conscious, explicit authorization to perform a specific action. For example, in <b>Great Britain</b> there is a system for the public services provision based on a unified identification/authentication system. In <b>Holland</b>, an infrastructure of authorization and delegation of rights (CARF) is implemented; it allows citizens and legal entities to delegate their rights to carry out transactions and receive public services on their behalf. Individuals are identified and</p>

<sup>30</sup> The following types of regulatory shortcomings are listed in the Table:

- (G) regulatory gap (regulation is required, but it is missing)
- (O) obsolete provision (the existing provision should be changed)
- (N) non-functioning provision (the existing provision is non-functioning for the reasons described)
- (B) this provision is an unreasonable barrier to the implementation of activities

			<p>authenticated in obtaining government services, financial services and commercial relationships, including in e-commerce.</p> <p>All residents in <b>Singapore</b> are issued a National Registration Card (NRIC) being a mandatory element for user identification and authentication for virtually all government, financial and telecommunications services.</p>
11.2	<p>Legislative possibilities for digital identification are limited to EDS and biometric identification means.</p> <p>Opportunities to use other means, such as tokens, codes, sms identification, video identification, etc. are missing</p>	O	<p>The provision of services based on user identification on the basis of information contained in telecom operators' databases is highly developed in the <b>European Union</b>.</p> <p><b>Estonia</b> has implemented the Mobil-ID technology (embedding an EDS identification application into a sim-card). This technology allows a user to identify himself/herself using a cell phone with no ID-card reader.</p> <p><b>Singapore</b> has developed a National Authentication Platform allowing for two-factor authentication. Users of this Platform are government agencies and institutions, services, banks, major financial institutions of the state. Authentication is based on the identification number, as well as by sending a password via sms. Two-factor identification is used when providing a wide range of government and financial services. Authentication by sending sms to a Singapore mobile number can be used to confirm digital signature transactions - for making transactions, confirming documents, concluding contracts and other business transactions.</p> <p>In <b>India</b>, authentication by phone number and sms is available when obtaining government and municipal services. Authentication by sending sms to the mobile operator's number can be used to confirm transactions with a digital signature - to perform transactions, certify documents, enter into contracts and perform other business transactions.</p>
11.3	<p>Legislative opportunities for digital identification are significantly restricted by the sphere of public administration, i.e. the provision of state services and voter participation in elections and referendums.</p>	G	<p>In <b>Singapore</b>, the identification and authentication of persons is performed when providing government services, financial services, in commercial relationships, including in e-commerce.</p>

	For example, the legislation does not provide for digital identification in e-commerce transactions.		Spheres with legal possibilities for digital identification in various ways in the <b>European Union</b> include: banking services, including money transfers on behalf of individuals without opening bank accounts; raising funds from natural and legal persons for deposits; placement of the above-raised funds; and performing legally significant actions.
<b>11.4</b>	Legislative regulation of biometric identification is limited to the areas of migration and electoral legal relations.  At the same time, the legislation stipulates that biometric registration is mandatory for all citizens of the Kyrgyz Republic, which theoretically implies broad opportunities for using biometric databases of citizens, including in the provision of state and municipal services and banking services.	<b>N</b>	Areas of use of biometric identification in the <b>United States</b> are: migration relations, entry and exit procedures for foreign nationals; law enforcement; national security, counter-terrorism; commercial services; healthcare, obtaining medical services; financial relations and the banking sector.
<b>11.5</b>	The legislation regulating the legal status of the Unified Identification System neither provides for its widespread use directly for identification purposes, nor connecting commercial banks and other organizations to it.	<b>N</b>	The legislation of the <b>Russian Federation</b> stipulates that commercial organizations, telemedicine companies and certification centers are allowed access to the Unified Identification and Authentication System. In addition, the Unified Biometric System is widely used.

### Comments

The legislation of the Kyrgyz Republic and, in particular, bylaws of the authorized state bodies include significant prerequisites for wide use of various digital identification tools. Such identification, which allows for the interaction of stakeholders (the state, businesses and individuals) in a remote format, is one of the digitalization development trends.

At the same time, regulation of digital identification involves creating appropriate conditions for their application, including increased flexibility in the regulation, improved consumer protection tools, and establishing requirements for improving information security, protection of personal data, and other measures.

At the same time, the current legislative mechanisms allowing remote or digital identification primarily aim at the public sector and do not disclose all possibilities of such identification for commercial purposes, including banking services.

### International Principles for Legislative Regulation

Great Britain has a recommended document, the Identity Assurance Principles, outlining the governmental approach to user identification on the Internet and containing, among other things, the following principles:

- **Transparency principle** - user identification can be performed when the user is fully informed about the process and understands the purpose of these actions;
- **Multiplicity principle** - a user may use the services and select any identity providers as many times as they want
- **Data minimization principle** - the use of a minimally sufficient amount of data required to achieve the purpose of the interaction;
- **Certification principle** - the user must be confident in the reliability of the identification means, the activity of which is based on obligatory certification
- **Principle of competition and technological neutrality** (avoidance of restriction on the use of specific software and hardware on the grounds of origin, development method and licensing model).

Analysis of the FATF Recommendations reveals a certain set of principles and requirements for the content of the law governing the activities of the state bodies and the financial sphere in this area. Such a law should include:

- Basic provisions containing, among other things, a list of state institutions that ensure the implementation of the law;
- Actions to be taken by financial institutions in order to comply with the law;
- Indicators of suspicious transactions that are subject to special control and must be reported to the relevant authority;
- Identification of the body responsible for receiving and processing information on suspicious transactions;
- Identification of the body responsible for further investigation;
- Responsibility of the financial institutions for violation of the requirements of the law;
- Implementation of international cooperation.

## Section 12. Digital services

### Content

- Regulation of digital services in cyberspace

### Current regulation (existing legislation):

1. The E-Governance Law of the Kyrgyz Republic dated July 19, 2017, No. 127

### Brief description of the identified shortcomings

No.	Shortcomings	Type <sup>31</sup>	Best practices
12.1	<p>Ensure protection of the rights of the digital services consumers</p> <p>In accordance with Article 33 of the Constitution of the Kyrgyz Republic, it is important to ensure the right of consumers to access necessary information, including:</p> <ul style="list-style-type: none"> <li>- information on the quality of services provided, goods sold, as well as other information that is important to the consumer</li> <li>- information on the service provider and its services</li> </ul>	G	<p><b>Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (Digital Services Act)</b></p> <p>Article 12: "Providers of intermediary services shall include information on any restrictions that they impose in relation to the use of their service in respect of information provided by the recipients of the service, in their terms and conditions. That information shall include information on any policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic decision-making and human review. It shall be set out in clear and unambiguous language and shall be publicly available in an easily accessible format".</p> <p><b>E-Commerce Law of the People's Republic of China of 01.01.2019</b></p> <p>Article 17: " An e-commerce operator shall disclose information about commodities or services in a comprehensive, faithful, accurate and timely manner, so as to safeguard consumers' right to know and right of choice. It shall not engage in false or misleading commercial publicity activities by means of fictitious deals, fabricated user comments intended to cheat and mislead consumers".</p> <p>Article 15: "Any e-commerce operator shall always have information about its own</p>

<sup>31</sup> The following types of regulatory shortcomings are listed in the Table:

- (G) regulatory gap (regulation is required, but it is missing)
- (O) obsolete provision (the existing provision should be changed)
- (N) non-functioning provision (the existing provision is non-functioning for the reasons described)
- (B) this provision is an unreasonable barrier to the implementation of activities

			business license, the administrative license issued for its business, and its status as a party that is not required to register itself as a market subject according to the provisions of Article 10 herein, or the link to a webpage with such information, published in a prominent position on its homepage".
12.2	<p>To enshrine the principle of good faith advertising</p> <p>According to Article 6 of the Advertising Law of the Kyrgyz Republic dated December 24, 1998, No. 155, it is not allowed to disseminate unfair advertising. Since digital services are an integral part of the information space, the use of advertising is an integral part of them. In order to ensure the rights and freedoms of a person and citizen, special requirements shall be established for advertising in digital services</p>	G	<p><b>Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (Digital Services Act)</b></p> <p>Article 24: "Online platforms that display advertising on their online interfaces shall ensure that the recipients of the service can identify, for each specific advertisement displayed to each individual recipient, in a clear and unambiguous manner and in real time:</p> <p>(a) that the information displayed is an advertisement;</p> <p>(b) the natural or legal person on whose behalf the advertisement is displayed;</p> <p>(c) meaningful information about the main parameters used to determine the recipient to whom the advertisement is displayed".</p> <p><b>E-Commerce Law of the People's Republic of China of 01.01.2019</b></p> <p>Article 18: "While displaying search results of commodities or services to consumers tailored to their interests, preferences, consumption habits and other personal characteristics, an e-commerce operator shall also provide consumers with options irrelevant to their personal characteristics, and respect and equally safeguard the lawful rights and interests of consumers".</p>
12.3	<p>To enshrine the requirements to ensure fair competition in the information area</p> <p>The degree of citizens' engagement in the information space, the digital services commercialization and many other factors can affect the competition level in the product market due to various kinds of advantages of digital services over non-digital services, as well as among themselves</p>	G	<p><b>E-Commerce Law of the People's Republic of China of 01.01.2019</b></p> <p>Article 22: "E-commerce operators with dominant market position due to their technical advantage, number of users, controlling capacity of relevant industry or the dependence of other operators upon such e-commerce operators in transactions or the like shall not abuse their dominant market position to exclude or restrict competition".</p>

<p><b>12.4</b></p>	<p>Provide safeguards to ensure the protection of users' personal data Protection of personal data of entities is the matter of processing personal data, its analysis and transfer to third parties, as well as obtaining consent from the subject of personal data, the possibility of withdrawing it at any time</p>	<p><b>G</b></p>	<p><b>Article 7 of GDPR. Conditions for consent</b> 3. The data subject shall have the right to withdraw their consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.</p> <p><b>E-Commerce Law of the People's Republic of China of 01.01.2019</b> Article 24: "When collecting and using the personal data of users, an e-commerce operator shall abide by the provisions regarding the protection of personal data as stipulated in laws and administrative regulations".</p> <p>Article 25: " An e-commerce operator shall display the methods and procedures for searching, correcting and deleting users' information and deregistering users' accounts, and shall not set unreasonable conditions on the possibility to search, correct and delete users' information and deregister users' accounts. Upon receipt of an application filed by a user for searching, correcting or deleting its information, the e-commerce operator concerned shall, after verifying the user's identity, promptly provide query information or have its information corrected or deleted. When a user applies to deregister its account, the e-commerce operator shall immediately delete all information about the user; if the provisions of laws and administrative regulations require or both parties have agreed that the user's information shall be kept, such provisions or agreement shall prevail."</p>
<p><b>12.5</b></p>	<p>To enshrine the principle of independently ensuring the security of digital services by their operators from potential IT-threats the digital services are subject to various kinds of threats in cyberspace. Enshrining self-regulation in the field of the digital services security on a par with the state regulation will improve services security, which in turn will ensure:</p>	<p><b>G</b></p>	<p><b>Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (Digital Services Act)</b> Article 12 "Providers of intermediary services shall include information on any restrictions that they impose in relation to the use of their service in respect of</p>

<ul style="list-style-type: none"> <li>- uninterrupted operation of digital services</li> <li>- reduction of cyber-threat risks</li> <li>- security of information stored in digital services</li> <li>- security of users' personal data</li> </ul>	<p>information provided by the recipients of the service, in their terms and conditions. That information shall include information on any policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic decision-making and human review. It shall be set out in clear and unambiguous language and shall be publicly available in an easily accessible format".</p> <p>Article 26: " Very large online platforms shall identify, analyze and assess, from the date of application referred to in the second subparagraph of Article 25(4), at least once a year thereafter, any significant systemic risks stemming from the functioning and use made of their services in the Union. This risk assessment shall be specific to their services and shall include the following systemic risks:</p> <ul style="list-style-type: none"> <li>(a) the dissemination of illegal content through their services;</li> <li>(b) any negative effects for the exercise of the fundamental rights to respect for private and family life, freedom of expression and information, the prohibition of discrimination and the rights of the child, as enshrined in Articles 7, 11, 21 and 24 of the Charter respectively;</li> <li>(c) intentional manipulation of their service, including by means of inauthentic use or automated exploitation of the service, with an actual or foreseeable negative effect on the protection of public health, minors, civic discourse, or actual or foreseeable effects related to electoral processes and public security".</li> </ul> <p><b>E-Commerce Law of the People’s Republic of China of 01.01.2019</b></p> <p>Article 30: "An operator of an e-commerce platform shall take technical measures and other necessary measures to guarantee its network's safety and stable operation, prevent illegal internet crimes, effectively respond to cyber security incidents, and safeguard the security of e-commerce deals.</p> <p>An operator of an e-commerce platform shall prepare emergency plans to specify how to respond to cyber security incidents. When a cybersecurity incident occurs, it shall immediately activate its emergency</p>
--	---

			plans, take corresponding remedial measures, and report to the related governing authority".
--	--	--	--

### Comments

Different kinds of services provided to citizens by both government agencies and private companies are increasingly digitized under the influence of digital technology. The latest trend is the integration of a large number of digital services into one digital platform or ecosystem. Thus, digital services are a digital platform element. The objective of digital services is to provide services to meet the citizens' needs on the basis of information in digital form.

Most digital platforms, which include digital services, have the financial and technological resources, data and customer base to expand into international markets, and also use such resources to compete in the domestic market. Governments in many leading countries (USA, China, Great Britain, EU members) are concerned about the lack of regulation of digital platforms and digital services.

Concerns arise from the potential for significant domestic and international influence on the product market. Domestically, there is a dual opposition between digital services and digital and conventional services. It is obvious that services that have not been digitized underperform compared to competitors.

Competition with international counterparts can entail increased cyber threats, reduced security of digital services, leakage of information and personal data of users, and other consequences.

At the same time, it is important to ensure the uninterrupted functioning of services, including digital services, based on certain principles.

It is proposed that the following be enshrined:

- Security of the digital environment;
- Healthy competition between digital services within digital platforms' activity;
- Transparency of conditions for consumer access to the services of the digital ecosystem and platform, not allowing unrestricted discretion of the owner of the ecosystem;
- Freedom of user transition to other digital platforms, ecosystems;
- Freedom of users to dispose of their data stored and processed by the digital platform, ecosystem;
- No imposition by platforms and ecosystems of their own services, creating discriminatory conditions;
- No restriction on consumer choice;
- Guarantee of openness.

On April 23, 2022, an agreement was reached between the European Parliament and EU member states on the proposed Digital Services Act, which in turn is regarded by the global community as an unprecedented experience, since the Act for the first time enshrines the status of digital platforms and the legal regulation of their activities. At the same time, China already has the E-Commerce Law, which also contains certain provisions relating to the activities of the concerned market participants.

## Section 13. State and municipal digital services

### Content

- Ensuring the process of digital transformation of the public administration (4 stages of digital transformation) - backend
- Principles for the provision of state and municipal services in digital form - frontend
- Coordination in the area of digital transformation of public administration (between bodies responsible for digital transformation, economic development bodies, bodies ensuring public administration).

### Current regulation:

1. E-governance Law of the Kyrgyz Republic dated July 19, 2017, No. 127
2. Law of the Kyrgyz Republic "On state and municipal services" dated July 17, 2014, No. 139.
3. Resolution of the Kyrgyz Republic Government "On measures to optimize the system for providing public services to individuals and legal entities" dated March 31, 2011, No. 129
4. Resolution of the Kyrgyz Republic Government "On the model standard of the state and municipal services" dated September 3, 2012, No. 603.
5. Resolution of the Kyrgyz Republic Government "On approval of standards of public services provided to individuals and legal entities by the state bodies, their structural divisions and subordinate institutions" dated June 3, 2014, No. 303
6. Resolution of the Kyrgyz Republic Government "On approval of the Rules of using the State Portal of Electronic Services" dated October 7, 2019, No. 525
7. Resolution of the Kyrgyz Republic Government "On implementation of the pilot project "State as a platform" to implement innovative ways of providing state and municipal services" dated February 25, 2020, No.113
8. Resolution of the Kyrgyz Republic Government "On amendments to the Resolution of the Kyrgyz Republic Government "On approval of the Rules of using the State Portal of Electronic Services" dated October 7, 2019 No. 525" dated November 20, 2020, No. 573.

### Brief description of the identified shortcomings

No.	Shortcomings	Type <sup>32</sup>	Best practices
13.1	<p>To enshrine the concept of "proactive" services</p> <p>Article 3 "Basic concepts used in this Law" shall be supplemented</p> <p>Proactive provision of the state and municipal services provides for the electronic application, priority of the "register" model (priority of legally significant records in electronic registries), priority or only exclusive interaction between the body when providing the service and the recipient, etc.</p>	G	<p>Active work to implement proactive services and super services is currently underway in the <b>Russian Federation</b>. It is assumed that each super service will consist of interconnected state services, services of budget institutions, as well as non-state services (banking, insurance, etc.).</p> <p>The experience of <b>Denmark</b>, the leading country in the UN e-governance ranking, is interesting largely in terms of proactive services based on "interaction with citizens at special moments of their lives".</p>

<sup>32</sup> The following types of regulatory shortcomings are listed in the Table:

- (G) regulatory gap (regulation is required, but it is missing)
- (O) obsolete provision (the existing provision should be changed)
- (N) non-functioning provision (the existing provision is non-functioning for the reasons described)
- (B) this provision is an unreasonable barrier to the implementation of activities

			In <b>Estonia</b> , proactive services are currently being used to combat unemployment and the Unemployment Insurance Fund (EUIF) is already using artificial intelligence to provide job seekers with the jobs they need based on their years of experience. It is planned to cover healthcare and education as well.
<b>13.2</b>	Enshrine the principle of providing state and municipal services in an electronic form  Article 4 "Basic principles for the provision of the state and municipal services" shall be supplemented accordingly	<b>G</b>	<b>Article 4 of the Federal Law No. 210-FZ "On the organization of provision of the state and municipal services" dated July 27, 2010:</b> <b>Possibility of obtaining the state and municipal services in an electronic form</b> , unless it is prohibited by the law, as well as in other forms stipulated by Russian Federation laws, at the choice of the applicant, except in cases where on the basis of federal law the provision of a state or municipal service is performed exclusively in an electronic form.
<b>13.3</b>	Provide for the possibility of receiving state and municipal services in an alternative form by means of digital identification of a person	<b>G</b>	Starting from 2021, the <b>Russian Federation</b> established the possibility of receiving a wide range of financial and state services by means of biometrics through the Unified Biometric System and the Unified Identification and Authentication System. At the same time, the State Duma of the Russian Federation is considering the draft law prohibiting to condition the provision of services on the processing of biometric data.  <b>Estonia</b> ranks third in the UN e-governance ranking. It currently has the most advanced national ID card system in the world. In addition to a legal photo ID card, the mandatory national card provides digital access to all secure electronic services of the state. In collaboration with SK ID Solutions and Cybernetica, the so-called Smart-ID was developed - a new generation of electronic identification designed for convenient use on smart devices maintaining a high level of security.
<b>13.4</b>	Enshrine the possibility of introducing a "register model" of the public services rendering  "Register model" is a design where the outcome of a service provision is not the	<b>G</b>	The register model of the state services has been currently successfully implemented in a number of agencies of the <b>Russian Federation</b> - the Federal Tax Service, Rosreestr (Russian Register) and Rosakkreditatsiya (Russian Accreditation).

	<p>issuance of a paper-based permit document, but an entry in an electronic register (although the receipt of an extract from the register may be retained as a separate service).</p>		<p>In the latter, in particular, it allowed to stop using the paper-based accreditation certificate and replace it with an automatically generated excerpt with a QR code.</p> <p>The register model of public services in <b>Estonia</b> is now used only in certain spheres, for example, in the tax service.</p>
--	--	--	---

### Comments

Optimization of the public administration is closely related to the provision of state and municipal services. In turn, such optimization is currently impossible without the widespread implementation of digital technologies in public and municipal administration.

The first stage of digitalization of the state and municipal services is considered to be the introduction of the "one-stop shop" concept. In addition, the transformation of conventional public services into electronic services became their platformization.

The stage of digitalization implies the conversion of most state and municipal services exclusively into electronic form, with the priority of the principle of proactivity and exclusion of any face-to-face interaction between the recipient of the service and the body and replacement of the paper-based documents by electronic ones. In addition to proactivity, the principles of accessibility, uniqueness, seamlessness and some others will also be implemented. Application of the register models has started long ago in other sectors for documents and information management. Implementation of a register model in the sphere of service provision will allow solving several tasks:

- Reduction of face-to-face visits to service centers;
- Shortening the time for obtaining the result of a state or municipal service;
- Speeding up the transition to full electronic document turnover;
- Others

The greatest experience in the digitalization of public administration comes from Denmark and Estonia, which have long been the leaders in the UN e-governance rating. The experience of the Russian Federation might also be noteworthy, where the use of digital technology in rendering public and municipal services is actively pursued or is ready to be introduced.

## Section 14. Digital Health and Well-Being

### Content

- Approaches to the managing data on the human condition throughout their life
- Possibility of setting requirements for software and hardware for human health and well-being (reference norm)
- Application of ethical standards

### Current regulation (existing legislation):

1. Law of the Kyrgyz Republic "On public health" dated July 24 2009, No. 248;
2. Law of the Kyrgyz Republic "On healthcare of citizens in the Kyrgyz Republic dated January 9, 2005, No. 6;
3. Law of the Kyrgyz Republic "On healthcare organizations in the Kyrgyz Republic" dated August 13, 2004, No. 116;
4. Law of the Kyrgyz Republic "On citizens' health insurance in the Kyrgyz Republic" dated October 18, 1999, No. 112;
5. Law of the Kyrgyz Republic "On medical devices circulation" dated August 2, 2017, No. 166;
6. Law of the Kyrgyz Republic "On medicines circulation" dated August 2, 2017, No. 165;
7. Law of the Kyrgyz Republic "On single payer system in the financing of healthcare of the Kyrgyz Republic" dated July 30, 2003, No. 159;
8. Electronic Signature Law of the Kyrgyz Republic dated July 19, 2017, No. 128;
9. E-governance Law of the Kyrgyz Republic dated July 19, 2017, No. 127;
10. Law of the Kyrgyz Republic "On personal information" dated April 14 2008, No. 58;
11. Law of the Kyrgyz Republic "On biometric registration of citizens of the Kyrgyz Republic" dated July 14, 2014, No. 136;
12. Agreement on Uniform Principles and Rules for Medical Devices Circulation (Medical Devices and Medical Equipment) within the Eurasian Economic Union (Moscow, December 23, 2014, accession - Law of the Kyrgyz Republic dated July 14, 2015 No. 167).
13. Decree of the Kyrgyz Republic President "On the National Development Program of the Kyrgyz Republic to 2026" dated October 12, 2021, UP No. 435;
14. Resolution of the Kyrgyz Republic Government "On the Program of the Kyrgyz Republic Government on Public Health and Health System Development for 2019-2030 "Healthy People - Prosperous Country" dated December 20, 2018, No. 600;
15. Resolution of the Kyrgyz Republic Cabinet of Ministers "On approval of the Action Plan on digitalization of the digital infrastructure management and development in the Kyrgyz Republic for 2022-2023" dated January 12, 2022, No. 2-r;
16. Order of the Kyrgyz Republic Ministry of Health "On approval of the Architecture of e-health system of the Kyrgyz Republic for 2018-2023" dated March 15, 2018, No. 190;

## Brief description of the identified shortcomings and international practice benchmarks

No.	Shortcomings	Type <sup>33</sup>	Best practices
14.1	Fundamental principles of e-health system development are not enshrined.	G	<p>It is proposed to define the principles of digital transformation of public health.</p> <p>Best practices: 8 principles of digital transformation of public health of the WHO Regional Office - The Pan American Health Organization (PAHO). Based on this practice, it is proposed that the following principles be enshrined:</p> <ul style="list-style-type: none"> <li>- Unity of the e-health system;</li> <li>- Interoperability (compatibility) of the medical information systems;</li> <li>- Inclusiveness and free access to the electronic healthcare system;</li> <li>- Security of personal data;</li> <li>- Continuous improvement of the e-health system architecture.</li> </ul>
14.2	<p>There are certain gaps in the current legislation in terms of ensuring the security of personal medical data, for example:</p> <p>The procedure of giving and obtaining informed voluntary consent and consent to the processing of the patient's personal data based on conclusive actions when receiving medical services using telemedicine technologies is not defined;</p> <p>The procedure and cases of transfer of personal medical data to a third party have not been determined;</p> <p>Certain issues of processing personal medical data in medical information systems are not yet resolved</p>	G	<p>It is suggested to enshrine the basics of medical personal data protection in a separate structural element in the respective section (on personal data) of the certain legal act.</p> <p>Best practices: It is proposed to use the GDPR practice, as well as the Personal Data (Privacy) Ordinance (PDPO) of the Hong Kong SAR as a model for the formation of the fundamental general rules in the field of personal data protection.</p> <p>The Personal Data (Privacy) Ordinance and Electronic Health Record Sharing System (PCPD) of PRC Hong Kong SAR is proposed to be considered as a best practice for the protection of personal medical data with appropriate approbation.</p>
14.3	The procedure for co-payment for medical services with the use of telemedicine technologies for the participation of private companies in public-private partnerships is not defined.	G	<p>Make additions to the provision on co-payment for medical services and possibly to the laws on the single payer system and on public-private partnerships.</p> <p>Best practices: Federal Law "On Public-Private Partnership, Municipal-Private</p>

<sup>34</sup>The following types of regulatory shortcomings are listed in the Table:

- (G) regulatory gap (regulation is required, but it is missing)
- (O) obsolete provision (the existing provision should be changed)
- (N) non-functioning provision (the existing provision is non-functioning for the reasons described)
- (B) this provision is an unreasonable barrier to the implementation of activities

			Partnership in the Russian Federation and Amendments to Certain Legislative Acts of the Russian Federation" of 13.07.2015 No. 224-FZ.
<b>14.4</b>	The procedure for applying home-use devices for remote monitoring of health status and physiological parameters and hospital-substituting technologies is not regulated.	<b>G</b>	<p>It is proposed that the procedure and regulation of the home-use devices for remote monitoring of health status and physiological parameters and hospital-substituting technologies be defined in bylaws and that corresponding reference/blanket norms be provided in the legal acts for the above devices.</p> <p>Best practices: MDCG 2021-24 EC Guidance on classification of medical devices:</p> <ul style="list-style-type: none"> <li>- Section 10 "Active devices for diagnosis and monitoring or intended for diagnostic or therapeutic radiology".</li> <li>- Section 11 "Software designed to provide information for making decisions for diagnostic or therapeutic purposes, or software designed to monitor physiological processes.</li> </ul>
<b>14.5</b>	There is no procedure for the use of a simple electronic signature by a patient when receiving medical services using telemedicine technologies.	<b>G</b>	<p>It is proposed to amend the Electronic Signature Law of the Kyrgyz Republic dated July 19, 2017, No. 128 and/or the respective bylaws, with provisions on the use of a simple digital signature of the patient and, in certain cases of the need for medical care - the possibility of using e-health systems without identification and authentication procedures.</p> <p>Best practices: EU Regulation on Electronic Identification, Authentication and Trust Services (eIDAS) for electronic transactions on the European Single Market.</p>

### Comments

General architecture of e-health in the Kyrgyz Republic consists of the applications and system and infrastructure services component, integration bus of single health information space.

The segment of applications (clinical applications) includes the existing and being created information systems that provide information and technological support of management functions in healthcare and information interaction with citizens. The creation and improvement of clinical applications should be based on the comprehensive implementation of the electronic medical record as a basic software product that combines information from various information systems of healthcare organizations of various levels.

The electronic medical record will have to contain an exhaustive structured volume of general personal, clinical, biometric, social, economic, financial, insurance and other data about the patient, while documenting medical services rendered to him/her.

The main objectives of the implementing electronic medical record are to ensure uninterrupted operation, 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 saving relevant medical information and providing it in a timely manner to the patient by the authorized medical workers.

Electronic medical record implementation aims to address the following tasks:

- availability of information on the patient's health anywhere in the country, consistent and in full;

- prompt receipt of information in a convenient form structured in accordance with the accepted methodology of execution of medical documents.

Along with the introduction of electronic medical records as a basic product for sustainable development of e-health, it is necessary to transfer the work of laboratories, pharmacies, sanitary and epidemiological services and other specialized health organizations to an electronic mode.

In order to ensure access to information on medicines circulation and to improve transparency it is necessary to create an electronic database of medicines and medical products, which will cover all aspects of drug circulation, from the moment of registration to their sale and utilization.

Appropriate work to create an electronic database of medicines and medical products is performed in accordance with the Concept of creating an electronic database of medicines and medical products in the Kyrgyz Republic approved by the Kyrgyz Republic Government Resolution No. 743 dated October 27, 2015.

### **International experience**

An example of changes toward digital healthcare comes from **Portugal**. The country currently has 60 information and communications technology systems of different levels of development. The goal is to change the healthcare delivery paradigm by putting a citizen at the core of the system. This transition is performed through the implementation of a national electronic health record card. This card is intended to be retained throughout a person's life, providing the ability to obtain information from various healthcare providers with whom the person interacts at various points in their life. To meet this need, the General Services Division of the Ministry of Health is developing national systems using easy-to-use standards. Information is also available to individuals through a portable "health wallet" containing medication prescription data, medication timing alerts, and so on. Comprehensive, interoperable health-related systems go far beyond healthcare providers. National strategic leadership, multisectoral collaboration, and stakeholder alignment strategies are needed to bridge these gaps – as mentioned in one of the reports.

Shifting the focus to prevention - earlier and more targeted treatment, engaging an individual as an active partner, for example, through patient-reported outcome information. Ensuring timely knowledge - reliable data about the individual should be available at all times when needed through coordinated care using integrated information systems. The basis for this is the "Health Passport", which includes not only the medical information of the individual, but also information on his lifestyle (nutrition, physical activity, social conditions, etc.) in order to comprehensively assess possible risks and adverse trends in health deterioration and timely support through the health and social care system;

Three main components can be distinguished in the structure of healthcare systems:

- High-quality primary healthcare and public health services;
- The activities of multiple sectors aimed at meeting the needs;
- Actively engaged and empowered communities.

Digital health plays a key role in bridging these three building blocks.

"The medical public health model is slowly and cautiously moving toward wider use of personalized information, but consumers are less patient: they use the Internet for self-diagnosis. This

means that not only clinical data, but also all sorts of personal user data, or "social outliers" illustrating the digital landscape, can be used to determine an individual's disease status, tracking which can help shape many additional insights into health problems.

Data orientation is crucial with one basic rule: all data collected should be protected and treated with respect, but arguments about data ownership are complex, and ultimately all data will have many owners.

### **Artificial intelligence and machine learning in healthcare systems and healthcare services delivery**

The following three principles for using artificial intelligence in healthcare have emerged from the work done by the National Health Service in **England**:

- The creation of standards and norms to support the use of artificial intelligence in healthcare is important and requires changes in regulatory development and enforcement mechanisms.
- The art of the possible should be mastered, devoting time and effort to dispelling myths and actively working to demonstrate the practical application of artificial intelligence in healthcare.
- No one should be left behind along the way: an inclusive approach to AI in healthcare that involves health professionals, patients and the public must be ensured. Transparency and communication about initiatives and case studies are critical.

E-prescription, which should not be deemed as a one-time technological implementation, but as a model subject to continuous adaptation and evolution. In Sweden, the e-prescription system was introduced in the 1980s, when the state monopolized the pharmacies. In 2008-2009, this market was liberalized. Approximately at this period, the Swedish e-health agency was established and is now responsible for all e-prescription databases, with which 1,400 pharmacies across the country are linked. As a result - 99% of prescriptions are electronic, while the quality and safety for patients have improved, as well as services for citizens; time and cost are being saved, and control over the system has become tough. In Spain, the creation of a unified medication plan, which provides a consolidated overview of the medications prescribed to the patient, has been particularly successful. Medications are grouped for ease of understanding based on the duration and type of treatment (long course, as needed, short course, etc.), and the plan contains basic information on each medication and instructions on how to take it.

Effective use of information for healthcare decision-making. "Innovative visualization that presents information in the simplest form is crucial. The importance of using "success stories" to illustrate what the data are telling us should not be overlooked, and many approaches already exist to do this. The primary goal is to provide healthcare to citizens".

Policy in **Ireland** is determined by examining macro-level information about the healthcare system and analyzing the effectiveness of a system struggling with the increasing costs and long patient waiting lists. The healthcare data landscape is fragmented, so work was done to find out what technologies and processes were available to get a broader picture. The data analysis process was designed to minimize the data needed to optimally communicate appropriate messages. One of the analytical tools available on the market was purchased, with which all existing data sets were combined in a new architecture (MySQL database) with input and output software to make the best use of the data and support the core activities of the Ministry of Health.

The goal is to create a centralized health data management system that integrates tools in a single information space to handle data for all actors involved, from providers to patients, combined with decision support systems.

## Section 15. Digital governance technological infrastructure

### Content

- Principles for infrastructure use (reuse, non-discriminatory access to infrastructure, etc.)
- Authority to establish technical requirements for certain types of infrastructure

### Current regulation (existing legislation):

1. E-governance Law of the Kyrgyz Republic dated July 19, 2017, No. 127;
2. Law of the Kyrgyz Republic "On Telecommunications and Postal Service" dated April 2, 1998, No. 31;
3. Law of the Kyrgyz Republic "On the basis of technical regulation in the Kyrgyz Republic" dated May 22, 2004, No. 67;
4. Decree of the Kyrgyz Republic President "On the National Development Strategy of the Kyrgyz Republic for 2018-2040" dated October 31, 2018, No. 221;
5. Resolution of the Kyrgyz Republic Government "On certain issues related to the state infrastructure of e-governance" dated December 5, 2019, No. 661;
6. Resolution of the Kyrgyz Republic Government "On approval of the Rules of interconnection in the Kyrgyz Republic" dated August 13, 2020, No. 421;
7. Resolution of the Kyrgyz Republic Government "On approval of the requirements for the State Data Processing Centers and their connecting communication channels" dated December 31, 2019, No. 747;
8. Resolution of the Kyrgyz Republic Government "On approval of the requirements for the protection of information contained in the databases of the state information systems" dated November 21, 2017, No. 762;
9. Resolution of the Kyrgyz Republic Cabinet of Ministers "On approval of the Action Plan of the Kyrgyz Republic Cabinet of Ministers for implementation of the National Development Program of the Kyrgyz Republic to 2026" dated December 25, 2021, No. 352;
10. Resolution of the Kyrgyz Republic Cabinet of Ministers "Action Plan on digitalization of governance and development of digital infrastructure in the Kyrgyz Republic for 2022-2023" dated January 12, 2022, No. 2-r.

### Brief description of the identified shortcomings and international practice benchmarks

No.	Shortcomings	Type <sup>34</sup>	Best practices
15.1	Separate legal norms establishing the development principles for the technological infrastructure for digital (electronic) governance in the current legislation of the Kyrgyz Republic are missing.	G	Due to the complex nature of the tasks of the public administration digitalization, there are no separate practices dedicated to the legal regulation of the <i>technological infrastructure</i> of digital (electronic) governance. All such practices are implemented in the respective normative and non-legislative legal acts (including strategic planning documents) at various levels. At the same time, it is proposed that paragraph 2 "Basic principles for improving

34 The following types of regulatory shortcomings are listed in the Table:

- (G) regulatory gap (regulation is required, but it is missing)
- (O) obsolete provision (the existing provision should be changed)
- (N) non-functioning provision (the existing provision is non-functioning for the reasons described)
- (B) this provision is an unreasonable barrier to the implementation of activities

		<p>the infrastructure of electronic interaction" of Section IV of the Concept for the Development of Mechanisms for Providing State and Municipal Services in Electronic Form (approved by RF Government Resolution No. 2516-p of 25.12.2013) be considered as one basic practice</p> <p>It is proposed to include in the Draft legal act the principles of:</p> <ul style="list-style-type: none"> <li>• Non-discriminatory access to the infrastructure;</li> <li>• Alienability of the infrastructure for electronic interaction from its developers, suppliers and operating organizations;</li> <li>• Certainty of the procedure for using the infrastructure of electronic interaction;</li> <li>• Mutual compatibility of information systems of the electronic interaction infrastructure;</li> <li>• Stability and continuity of the characteristics of the electronic interaction infrastructure;</li> <li>• Maximum use of market opportunities;</li> <li>• Ensuring the security of personal data and other restricted information.</li> </ul> <p>In addition, it is proposed to provide a reference and (or) blanket norms to the respective sectoral laws and (or) bylaws governing the relations at the infrastructure level of the state e-governance infrastructure formed by the state data processing centers and their connecting communication channels.</p>
<p><b>15.2</b></p>	<p>In accordance with Article 24 of the E-governance Law of the Kyrgyz Republic dated July 19, 2017 No. 127, the requirements for the state data processing centers and their connecting communication channels, including the requirements for stability and security, as well as the procedure for including data processing centers and their connecting communication channels in the state e-governance infrastructure are established by the Kyrgyz Republic Government.</p> <p>Based on the results of the analysis of the respective regulatory and non-regulatory legal acts, it was found that the current regulation covers a narrow list of functional</p>	<p><b>G</b></p> <p>Purposes and objectives of the state data processing centers (hereinafter - DPCs), their parameters, structure, requirements for security and stability and their connecting communication channels are established by the Resolution of the Kyrgyz Republic Government "On approval of the requirements for the state data processing centers and their connecting communication channels" dated December 31, 2019, No. 747.</p> <p>The requirements for the systems of uninterrupted functioning of the technical means of the server equipment and server room of the state body, local self-government, organization are established by</p>

	<p>and technical parameters of the data processing centers.</p>		<p>the Resolution of the Kyrgyz Republic Government "On approval of the requirements for protection of information contained in the databases of the state information systems" dated November 21, 2017, No. 762.</p> <p><b>Best practices:</b>  GOST P 58812-2020 RF "Data Processing Centers. Engineering infrastructure. Operating model of operation. Specification" approved and enforced by the Order of the Federal Agency for Technical Regulation and Metrology No.68 CT on 19.02.2020, provides more detailed conditions for the design and operation of the data processing centers.  For example, GOST R 58812-2020 establishes requirements for organizational model of operation (organizational structure of the operation service and resource model), requirements for the processes of engineering infrastructure operation (equipment maintenance, quality control, safety assurance, interaction).</p> <p>Based on similar political, socio-economic and historical development factors, the Russian experience often has a more favorable development scenario in the Kyrgyz Republic in contrast to the practice of non-CIS countries, and does not require</p> <p>Thus, several options for ensuring legal regulation of SDPC are proposed:</p> <ul style="list-style-type: none"> <li>• Implementation of appropriate state (national) standards (as more flexible and effective tools of sectoral regulation) in the system of regulation of the technological infrastructure for digital governance through the inclusion of appropriate provisions in the text of the Draft legal act;</li> <li>• Development and adoption of appropriate state (national) standards establishing requirements for the technological infrastructure of digital governance in accordance with the requirements and standards corresponding to the current level of development in this industry.</li> </ul>
15.3	The Law of the Kyrgyz Republic On	N	Due to this shortcoming, it is proposed to

<p>Telecommunications and Postal Service dated April 2, 1998, No. 31 poses corruption and abuse of dominance risks due to the following factors:</p> <ul style="list-style-type: none"><li>- non-discrimination requirements established in the Law are discrete in nature;</li><li>- lack of development of these legal mechanisms in the subordinate acts;</li><li>- mechanisms of control of the authorized bodies over observance of telecommunications operators' rights is missing.</li></ul>	<p>establish appropriate rules for ensuring non-discriminatory access to telecommunication networks and incorporate appropriate provisions.</p> <p>An example of good practice is the Resolution of the Government of the Russian Federation "On approval of the Rules of non-discriminatory access to the infrastructure to host telecommunications networks" dated 29.11.2014, No. 1284.</p>
---	--

## Section 16. Telecommunications networks and resources

### Current regulation (main regulations of current legislation):

1. Law of KR "On Telecommunications and Postal Service"
2. Law of KR "On Postal Service"
3. Law of KR "On licensing and permit system"
4. Law of KR "On informatization and e-governance"
5. Law "On natural monopolies in the Kyrgyz Republic"
6. Law of KR "On the basis of Technical Regulation"
7. Law of KR "On the procedure for inspecting business entities"
8. Law of KR "On television and radio broadcasting"
9. Law of KR "On guarantees and freedom of access to information"
10. Law of KR "On electronic signature"
11. Tax Code of KR
12. Code on non-tax revenues of the Kyrgyz Republic
13. Misdemeanor Code of KR
14. Regulation "On licensing of radio frequency spectrum activities" (Resolution of the Kyrgyz Republic Government dated 17.11.2017, No.754)
15. Regulation "On licensing activities in the field of telecommunication and postal service" (Resolution of the Kyrgyz Republic Government dated December 31, 2019, No. 746)
16. National system and numbering plan of telecommunication networks of the Kyrgyz Republic (Resolution of the Kyrgyz Republic Government dated January 9, 2018, No.10)
17. Rules for the provision of mobile radiotelephone communication services (Resolution of the Kyrgyz Republic Government, February 17, 2014, No.97)
18. Methodology for calculating the annual fee for the use of radiofrequency spectrum denominations and (or) bands (Resolution of the Kyrgyz Republic Government dated July 7, 2015, No.460)

### Brief description of the identified shortcomings and international practice benchmarks

No.	Shortcomings	type <sup>35</sup>	Best practices
16.1	Legislative norms regulating the establishment of telecommunication networks, their operation, as well as the use of telecommunication resources are incorporated in various sectoral legislative acts and are often not harmonized with each other	O	Systematic harmonization of norms related to electric communication (telecommunication) networks and resources with sectoral (special) legislation, and their possible removal from other legislative acts to avoid unnecessary duplication and over-regulation
16.2	Remove the provisions on postal service in the Law of KR On Telecommunications and Postal Service, as there is a sectoral (special) KR Law On Postal Service" (Articles 18-20 and others)	O	The legislation of the European Union countries as a rule puts the regulation of (demonopolized or remaining in state ownership) postal services beyond the scope of any "non-core" legal acts

<sup>35</sup> The following types of regulatory shortcomings are listed in the Table:

- (G) regulatory gap (regulation is required, but it is missing)
- (O) obsolete provision (the existing provision should be changed)
- (N) non-functioning provision (the existing provision is non-functioning for the reasons described)
- (B) this provision is an unreasonable barrier to the implementation of activities

<b>16.3</b>	One of the principles of Article 1 of the Law of the Kyrgyz Republic On Telecommunications is "comprehensive support for the provision of high quality conventional and innovative telecommunication and postal service". This principle is not specified and is not implemented in practice.	<b>N</b>	It is necessary to specify this principle in the description of the relevant legal institutions (state support). For example, as it is stipulated in the US and European Union laws in terms of reimbursement of costs to telecommunication operators to achieve certain goals defined by the state, as well as the establishment of norms of technological neutrality, stimulating the transition to advanced technological solutions
<b>16.4</b>	Article 2 "Definitions" of the Telecommunications and Postal Service Law of the Kyrgyz Republic	<b>O</b>	Needs harmonization with the glossary of the International Telecommunication Union
<b>16.5</b>	Article 9 "Use of Radio Frequency Spectrum and Orbital Positions of Communication Satellites" of the Telecommunications and Postal Service Law of the Kyrgyz Republic does not contain provisions facilitating use of radio spectrum for the provision of advanced services and development of new technologies ("Internet of Things", artificial intelligence systems, etc.)	<b>G</b>	Legislation in many countries of the European Union and other regions of the world contains direct norms (positive prescriptions) aimed at encouraging the use of radio spectrum for the provision of advanced services and the development of new technologies
<b>16.6</b>	Article 13 of the Telecommunications and Postal Service Law of KR stipulates the requirements for Kyrgyztelecom's license. This violates the principle of equality of economic entities.	<b>O</b>	Following the worldwide trend towards de-monopolization of the telecommunication sector, this Article should be eliminated from the Law.
<b>16.7</b>	Article 26 of the Telecommunications and Postal Service Law of KR contains a non-functioning provision on compensation for losses incurred by telecommunication service operators due to the suspension of their activities. The same is in the following Article 27	<b>N</b>	The procedure for appropriate compensation from the budget should be regulated
<b>16.8</b>	Article 31 of the Telecommunications and Postal Service Law of the Kyrgyz	<b>N</b>	Appropriate norms should be introduced into the urban planning legislation and

	Republic contains a provision for construction and other organizations to take into account the requirements of telecommunication operators in terms of the location of their technical facilities. In practice, this norm does not work, as construction does not take into account the need for communication networks and there is no liability of the constructor for non-compliance with this norm		the Code of Administrative Offences of the Kyrgyz Republic
<b>16.9</b>	Dispositions of articles in the Misdemeanor Code of the Kyrgyz Republic do not comply with the current regulations in the field of communication	<b>B</b>	Harmonization is required; for example, as in the Misdemeanor Code of the Republic of Moldova (Chapter 14)
<b>16.10</b>	According to the Code of the Kyrgyz Republic on non-tax payments, "providers of telecommunication and postal services make contributions to the development of the telecommunication industry at the rate of 0.9% of revenues from Telecommunications and Postal Service". At the same time, no money is actually allocated for significant projects in the field of communication	<b>N</b>	Model Law on Electronic Communication for Eastern Partnership countries
<b>16.11</b>	The Tax Code of the Kyrgyz Republic levies taxes on "telecommunication services" (Article 249), but the legislation on communication does not provide for this terminology	<b>B</b>	Specify (harmonize) terminology
<b>16.12</b>	The highest sales tax rate in the Tax Code of the Kyrgyz Republic of 5%, while for the banking system and real estate developers the rate is 2% each (Article 368)	<b>B</b>	Additional taxation should be eliminated
<b>16.13</b>	Many norms in the Regulation on Licensing of Activities in the Field of Telecommunications and Postal Service became irrelevant, and/or are redundant, and/or are not specific enough for uniform interpretation.	<b>B</b>	Harmonize with the EU legislation and eliminate redundant requirements
<b>16.14</b>	The established efficiency coefficients in the Methodology for Calculating Annual Fee for the Use of	<b>B</b>	A similar methodology is used in the Russian Federation

	Radio Frequency Spectrum Denominations and/or Bands are not aimed at encouraging network expansion and reducing the financial burden on the telecommunication operator		
--	--	--	--

### Comments

Telecommunication infrastructure development and the use of telecommunication networks and resources in the Kyrgyz Republic are specific; this is largely due to its geographical location. The Kyrgyz Republic is landlocked. More than three-quarters of the country's territory is covered by rocky mountains (average height is 2,750 m above sea level), which has predetermined the use of mostly wireless communication technologies and active use of radio-frequency resources. Fiber-optic communication lines are also widely used. According to the International Telecommunication Union (ITU) ICT Development Index in 2017, Kyrgyzstan ranked 109<sup>th</sup> out of 176 countries in the world and 10<sup>th</sup> among the CIS countries.

In January 2022, Kyrgyzstan had 3.41 million Internet users (per 6.68 million population) with Internet penetration in Kyrgyzstan of 51.1% of the total population. Kyrgyzstan recorded 3.60 million users of social networks (53.9% of the total population); mobile (cellular) communication has the largest specific weight in terms of the volume of services provided in the communication market. At the end of 2021, mobile cellular communication holds the second place in the communication market with an index of more than 41,7% by volume of rendered services and made up 10,245.89 million KGS, which is 15,6% more compared to the similar indicator of the last year.

The telecommunication market in Kyrgyzstan is distinguished by relatively liberal legislation until recently, low cost of data transmission services, high competition between the major players in the industry.

The current regulation of telecommunications issues in the Kyrgyz Republic is based on the Telecommunications and Postal Service Law of the Kyrgyz Republic adopted in 1997, the main objective of the law was to develop competition and increase the number of operators in the telecommunication sector. At the same time, it limited the authority of the historical telecommunication operator OJSC "Kyrgyztelecom", which at the same time was recognized as the national one. The law also provided for differentiation of rights and authorities of the state body that determined the policy and the body responsible for market regulation (the National Communications Agency). The regulatory authority had the power to develop its own normative acts aimed at operational regulation. The acts are aimed at mandatory execution by all market participants. At the same time, the body in charge of developing policy in the field of radiofrequency spectrum use, was determined.

This structure was quite successful. The communication market began to develop actively, being attractive due to ease of entry into the market and obtaining the state resource (telephone numbering and radio-frequency resource). Four cellular operators started working, and Kyrgyzstan managed to introduce and use in its relatively small territory several standards of mobile communication such as DAMPS, GSM and CDMA. Such a breakthrough gave subscribers a significant choice. In addition, the regulator had the functions of supervision and control, as well as independent antimonopoly functions, which allowed for qualitative research and analysis of the market, a clear picture of the market participants and their position and consideration of citizens' complaints and appeals as part of the consumer rights protection. Later on, the system of management bodies in the field of telecommunication was modified several times.

Over the years since the adoption of the basic telecommunication law, the legislation of the Kyrgyz Republic has significantly changed and there emerged numerous normative acts related to different sectors and containing certain legal norms in the sphere of telecommunication regulation, but

without proper coordination with special (sectoral) legislation and even without proper terminological uniformity. Thus, there are in fact two "competing" laws with similar names and overlapping spheres of application - Telecommunications and Postal Service Law and Postal Service Law.

Reforming legislation in the field of telecommunication networks development and the use of telecommunication resources cannot be reduced only to "point-by-point" adjustments of certain provisions of sectoral (special) laws and Codes and other laws of the Kyrgyz Republic in force in certain aspects of telecommunication. Development of new economic models and technologies, including diversification of services provided by telecommunication operators, requires expansion of the resource base and opportunities for more efficient and less costly construction of infrastructure. In particular, the emergence of 5G technologies, the Internet of Things, unmanned transport (artificial intelligence systems), Smart City and others, inevitably poses the question of mastering new frequency bands, increasing the bands allocated to operators of radio frequencies, preventing "prohibitively high" fees for providing such resources. This also confirms that to ensure real digital transformation of not only the economy, but also the entire daily life of the country, the activities of public authorities of the Kyrgyz Republic, its citizens and businesses, telecommunication infrastructure (telecommunication) will long be the basis for deploying appropriate digital platforms, functionality and services. This, in turn, entails the need to ensure priority attention to the needs of operators of such infrastructure, with changes in approaches to licensing their activities and allocating them appropriate frequency and other resources for effective operation, as well as consistent facilitation (simplification) of permit procedures for placement and operation of necessary telecommunication equipment.

### International experience

The experience of reforming the regulatory system in the field of telecommunication in various countries with different economic and technological development is quite extensive and varied. Along with examples of legislative regulation of telecommunications in neighboring countries of Central Asia and other member states of integration associations involving the Kyrgyz Republic (Eurasian Union, Commonwealth of Independent States, etc.), in order to choose optimal directions for lawmaking in the field of communications (networks and telecommunication resources) the experience of the European Union, as well as such countries as USA, Canada and Australia should be used as well. To harmonize the legislation of the Kyrgyz Republic with the best international practices, it is important to study and apply the recommendations of the International Telecommunication Union and the World Bank.

### Conclusions and recommendations

Recognizing telecommunication infrastructure, networks and resources as the most important factor (foundation) for digital transformation of the Kyrgyz Republic, it is necessary to revise the approaches to the telecommunication regulation underlying basic Telecommunications and Postal Service Law over 25 years ago, based on best international practices and recommendations, as well as experience of the telecommunication industry of the country. First of all, it is necessary to achieve uniformity of legal approaches in general and special legislative acts of the Kyrgyz Republic regulating telecommunication issues from different sides.

#### **In particular, it is necessary to:**

- Ensure uniformity of the applied terminology and regulatory principles in telecommunication, creating opportunities (a reference terminology base) to adjust all other legal acts;
- Eliminate duplication in the subject area of regulation in different legislative acts, as well as as normative acts of different levels;

- Specify the legislative requirements and support measures to encourage the development and implementation of the latest technologies and services;
- Inventory and, if necessary, abolish restrictive measures and burdens that have become obsolete, irrelevant or ineffective, and impede operators' day-to-day operations;
- Provide non-discriminatory conditions to telecommunication operators (organizations) in terms of taxation, as well as access to infrastructure and resources controlled or provided by the state;
- Adjust approaches to telecommunication licensing in line with international practices; maximize the use of alternative (not relative to seeking public authorities' permissions) regulatory methods, including notification methods and self-regulation;
- Ensure de facto equality of telecommunication market players, including the model of retaining a national operator in the medium term while complying with antimonopoly regulations.

## Section 17. Inter-operator cooperation, network neutrality

### Current regulation (existing legislation):

1. Law of KR "On Telecommunications and Postal Service"
2. Law of KR "On licensing system"
3. Law of KR "On informatization and e-governance"
4. Law of KR "On natural monopolies in the Kyrgyz Republic"
5. Tax Code of KR
6. Code of the Kyrgyz Republic on non-tax revenues
7. Rules of Interconnection in the Kyrgyz Republic (Resolution of the Kyrgyz Republic Government dated August 13, 2020, No.421)
8. Regulation "On licensing activities to use radio frequency spectrum" (Resolution of the Kyrgyz Republic Government dated 17.11.2017, No.754)
9. Regulation of the Kyrgyz Republic Government "On licensing activities in the field of Telecommunications and Postal Service" (Resolution dated December 31, 2019, No. 746)
10. Regulation "On the procedure of interaction between mobile cellular operators and internal affairs bodies of the Kyrgyz Republic engaged in operational and investigative activities to search for stolen mobile devices" (Resolution of the Kyrgyz Republic Government dated March 25, 2009, No.192)

### Brief description of the identified shortcomings and international practice benchmarks

No.	Shortcomings	Type <sup>36</sup>	Best practices
17.1	Article 30 of the Telecommunications and Postal Service Law "Interconnection (interoperability)" is mainly addressed to "dominant" operators, contains ambiguous terminology and prevents the development of inter-operator relations based on equal agreements between operators and it departs from the logic of telephone (fixed) communication networks	B/O	The global trend when regulating inter-operator relations is based on the principle of technological neutrality in transmitting inter-network traffic, abandonment of strict requirements for the construction of hierarchical fixed-line networks and reduction of tariffs for interconnection: "operators should earn on their customers, not on their competitors".
17.2	Interconnection rules in the Kyrgyz Republic (Resolution of the KR Government dated February 13, 2020) retain the logic of the requirements for networks, which operate on the basis of channel switching, rather than packet routing	B/O	The foreign regulatory practice (European Union, North America, etc.) does not limit the interconnection issues exclusively to the "conventional telephony" networks

<sup>36</sup> The following types of regulatory shortcomings are listed in the Table:

- (G) regulatory gap (regulation is required, but it is missing)
- (O) obsolete provision (the existing provision should be changed)
- (N) non-functioning provision (the existing provision is non-functioning for the reasons described)
- (B) this provision is an unreasonable barrier to the implementation of activities

17.3	The current legislation in the field of communication does not contain provisions on the elimination (or significant reduction) of interconnection tariffs, first of all, in trans-border inter-operator cooperation within the integration associations involving the Kyrgyz Republic (EAEC, CIS, etc.) - the issue of reduction (to a minimum level) of interconnection rates and abolition of international roaming	<b>BG/B</b>	Roaming tariffs in the European Union are actually zeroed. Abolition of roaming in the EAEU member states is also under discussion (but not yet resolved).
17.4	The current legislation of the Kyrgyz Republic does not contain provisions ensuring the implementation of the principle of network neutrality	<b>BG</b>	Legislation of several states of the USA; General rules to ensure equal and non-discriminatory treatment of traffic when providing Internet access services and appropriate rights of end-users of the European Union

### Comments

Legislation of the Kyrgyz Republic in terms of regulation of inter-operator interaction (rules of network interconnection and traffic transmission) is generally consistent with the current stage of the telecommunication technologies development. However, it is still based on "conventional telephone" principles of communication networks building and does not actually take into account (or rather, does not regulate) the issues of interaction of data communication networks based not on switching communication channels, but on routing packets of information transmitted through the network. It also needs to ensure terminological uniformity in all normative documents and their compliance with the international practice (recommendations and documents of the International Telecommunication Union). In general, there should be a transition from directive rules of network connection to bilateral (and multilateral) inter-operator SLA (Service Level Agreement) type agreements.

As noted, one of the main barriers to network development and providing more affordable communication to the users is a high tariff for interconnection traffic transmission. The current global trend is to reduce interconnection rates and ensure technological neutrality in transmitting interconnection traffic. The most vivid illustration of this situation is users' willingness to "avoid" burdensome scenarios of using telecom infrastructure by using various mobile and other applications (OTT-services). This also poses the question of the advisability of regulating the interaction between telecommunication operators and OTT service providers similarly to inter-operator interaction between licensed telecommunication operators.

A further consequence of regulating inter-operator interaction at the national level will be the potential abolishment of the roaming fee for subscribers in the countries - members of integration associations involving the Kyrgyz Republic. Thus, in order to create favorable conditions for communication and information exchange between citizens of the EAEU member states, a comprehensive reform of inter-operator interaction between partner operators by reducing inter-operator roaming rates and rates for call termination services was discussed. This will allow reducing subscriber rates for roaming communication services to a level comparable to the conditions in the home region ("roaming as at home"). This was also demonstrated by the experience of the Russian Federation in abolishing national roaming, which was recognized in 2019 as the best global practice in the digital economy.

A separate problem to be addressed as part of adjusting the legislation of the Kyrgyz Republic on digital transformation is the implementation of the network neutrality principle, which, as a general rule, is the unacceptability of discrimination of customer service depending on the type of traffic

transmitted through the network. This problem should have been understood in the broadest possible sense. For example, originally, US network neutrality legislation was based on the following elements: consumer protection, transparency, elimination of redundant requirements to encourage broadband investment. In the European Union, this principle is reflected in the Regulation on Open Internet Access "General rules to ensure equal and non-discriminatory treatment of traffic in the provision of Internet access services and corresponding rights of end-users" dated November 25, 2015 No. 2120.

### International experience

The inter-operator interaction-related issues are outlined in good detail in the recommendations of the International Telecommunication Union. In addition, the legislation of the European Union and its member states is a positive example of regulation in this sphere.

As for interconnection tariffs reduction and potential abolishment of international roaming, the practice of the European Union countries can be used, as well as the experience of the Russian Federation in eliminating national roaming. Finally, progress and reasons for failures in discussing similar issues at the Eurasian Union level should be analyzed.

Regarding network neutrality, it seems optimal to follow the European Union Regulation on Open Internet Access, which states that "end users have the right to access and distribute information and content, use and provide applications and services, and use terminal equipment of their choice, regardless of the location of the end-user or service provider or the location, origin or destination of information, content, application or service through their Internet access service". This principle is of particular importance in the context of the forthcoming introduction of artificial intelligence (AI) technologies and the development of the related legislation.

### Conclusions and recommendations

Based on the (in general) adequate level of regulation of interoperability issues in the legislation of the Kyrgyz Republic it is proposed, in addition to the need to clarify and ensure applicable terminology, to focus on the regulation of issues with the current regulation gaps, **namely**:

- inter-operator interaction in relation to networks (data transmission) based on the routing of packages of information transmitted via them;
- procedure for the use of operators' networks by the OTT service providers;
- stimulating the reduction of interconnection tariffs;
- creating conditions for the abolishment of international roaming in the countries of integration associations involving the Kyrgyz Republic;
- consistent implementation of the network neutrality principle.

## Section 19. PPP in the context of digital transformation

### Content

- PPP facilities (information systems, information resources, technological systems and telecommunication networks)
- Special procedure for the PPP facilities use and monetization

### Current regulation (existing legislation):

1. Budget Code of the Kyrgyz Republic;
2. Law of the Kyrgyz Republic "On Public-Private Partnerships" dated August 11, 2021, No. 98
3. Resolution of the Kyrgyz Republic Government "On defining authorized bodies in the field of public-private partnership" dated September 14, 2012, No. 616;
4. Resolution of the Kyrgyz Republic Government "On financing of public-private partnership projects preparation" dated March 17, 2014, No. 147;
5. Resolution of the Kyrgyz Republic Government "On the establishment of the Public-Private Partnership Council in the Kyrgyz Republic" dated June 16, 2016, No. 328;
6. Resolution of the Kyrgyz Republic Government "On certain issues in the field of public-private partnership" dated February 21, 2020, No. 111.

### Brief description of the identified shortcomings and international practice benchmarks

No.	Shortcomings	Type <sup>37</sup>	Best practices
19.1	The PPP Law does not allow for inclusion in other laws any provisions, the subject of which is regulated by the PPP Law (Article 2). At the same time, neither the Law, nor the Budget Code provide for procedures for the use of budgetary investment, instead these procedures are established by a separate decision in the form of NLA on PPP in each case individually, which, firstly, significantly complicates the decision on each new PPP project, and secondly, poses a great risk of unintended utilization of the budgetary funds	N	The PPP Laws cannot restrict legal regulation of the norms, which provide for public relations in the sphere of PPPs in different normative legal acts. Accordingly, it is proposed not to limit the subject of PPP regulation in other legislative acts of the Kyrgyz Republic. The specifics of the PPP projects due to the social and economic development of the Kyrgyz Republic and the existing problems and challenges in various spheres of the society preclude from systematization of the PPP regulatory framework in a single law.

<sup>37</sup> The following types of regulatory shortcomings are listed in the Table:

- (G) regulatory gap (regulation is required, but it is missing)
- (O) obsolete provision (the existing provision should be changed)
- (N) non-functioning provision (the existing provision is non-functioning for the reasons described)
- (B) this provision is an unreasonable barrier to the implementation of activities

			<p>The legislation of foreign countries defines PPP relationship as cooperation between the public and private investors in order to develop and implement projects for the creation and/or modernization, operation and maintenance of infrastructure facilities and/or infrastructure services. Objectives faced by PPPs imply the availability of legal provisions relating to different areas of the investment projects:</p> <ul style="list-style-type: none"> <li>— (improving the efficiency and quality of creating infrastructure facilities and infrastructure services provision;</li> <li>— increasing the efficiency of the public expenditures on the design, construction and/or modernization, operation, maintenance of infrastructure facilities and infrastructure services provision;</li> <li>— attracting investment in the country's economy; involving additional management capacity of the private sector;</li> <li>— achieving an optimal price ratio over the assets life cycle and quality or fitness for purpose when implementing infrastructure projects;</li> <li>— using private sector innovation and efficiency; encouraging the growth and development of new technologies)</li> </ul>
<p><b>19.2</b></p>	<p>The law does not describe types of financial support from the state, as well as the procedure for risks distribution between the public and private partners, which is a prerequisite for a PPP project (in order to protect property; non-interference from the public partner; the right to compensation for losses, and etc.).</p>	<p><b>G</b></p>	<p>It is proposed to supplement the Law and define types of state guarantees, types of risks, timing and at what stage a private partner may rely on the compensation for losses, and etc.</p> <p>Various mechanisms of cooperation between the state and private business are used in foreign countries, when implementing PPP projects. Depending on the scope and conditions of cooperation,</p>

			<p>obligations of the parties, principles of risk-sharing between the partners and responsibility for various types of work, the PPP mechanisms vary.</p> <p>Article 36 of the PPP Law of the Republic of Belarus stipulates that a private partner shall be guaranteed the rights provided for by the legislation of the Republic of Belarus.</p> <p>Interference in the activities of a private partner is not allowed, except in cases where such interference is provided for by legislative acts in the interests of the national security, public order, protection of morality, public health, rights and freedoms of others;</p> <ul style="list-style-type: none"> <li>- a private partner is guaranteed protection of property and other rights acquired and exercised by it in accordance with the PPP agreement;</li> <li>- after payment of taxes, fees (duties) and other mandatory payments to the budget established by the legislation of the Republic of Belarus, a foreign private partner is guaranteed free transfer outside the Republic of Belarus of the profits and other lawfully obtained funds related to the performance of the PPP agreement.</li> </ul>
<p><b>19.3</b></p>	<p>The existing law of the Kyrgyz Republic lacks mechanisms to ensure competition and create equal and fair conditions for all bidders; this may entail a violation of the PPP principles (transparency, fairness, fair distribution of risks) when selecting a winner of the tender</p>	<p><b>B</b></p>	<p>There are no any rules in the foreign practice, where only one bid would be enough for a qualifying selection. The most widespread mechanism of the competitive selection or tenders in the EAEU countries is the one, which allows for one-stage, two-stage and closed tenders</p>
<p><b>19.4</b></p>	<p>Though the Law of KR mentions the possibility of PPP project award through direct negotiations, the procedure of direct negotiations is missing</p>	<p><b>G</b></p>	<p>It is suggested to supplement the Law with an Article outlining the terms and conditions of direct negotiations and the list of areas, where the conclusion of PPP agreements through direct</p>

negotiations is possible.

For example, the Law of the Republic of Kazakhstan dated October 31, 2015 No. 379-V "On Public-Private Partnership" provides that a private partner is determined on the basis of direct negotiations by the regulator for state planning, and this applies in cases where:

- 1) a public-private partnership project is initiated by the potential private partner with respect to a facility owned or long-term leased by it;
- 2) a project of public-private partnership is inseparably connected with exercising exclusive rights to the results of creative intellectual activity belonging to the potential private partner.

A private partner is determined on the basis of direct negotiations through the following consecutive stages:

- 1) initiation of the public-private partnership project by the potential private partner;
- 2) notification of PPP project initiation indicating the main technical and economic parameters of the PPP project and requested payments from the budget and (or) measures of state support;
- 3) expert examination of a business plan for the PPP project;
- 4) conducting negotiations between the potential parties to the contract of public-private partnership on the terms of the contract of the public-private partnership;
- 5) conclusion of the public-private partnership agreement

## Comments

Based on the reviewed international practice, analyzed legislation and PPP development in the Kyrgyz Republic, the following problems have been identified:

1. Lack of a clear strategic program for the PPP development and priority sectors with infrastructure facilities and infrastructure services in the Kyrgyz Republic.

2. Lack of awareness of citizens (private sector) and understanding of PPP mechanisms (one of the ways to improve the effectiveness of the legislation is to better inform the population about the rights to receive quality services, the opportunities to participate in the decision-making process. While a PPP project is still at the stage of planning and development, the Cabinet of Ministers of the Kyrgyz Republic should create mechanisms for public participation and organize groups of the population, which would use them, otherwise this right will not be exercised).

3. Low quality and shortcomings in the Law of the Kyrgyz Republic "On Public-Private Partnership" and other normative legal acts regulating PPP sphere limit the interest of potential investors. The main shortcomings include: contradictions in the normative legal acts, internal collisions, gaps in the normative legal acts; discretionary powers in the provisions of the Law; violation of the PPP principles - transparency, competition, fairness in selecting a winner (participation of only one bidder and its selection); high degree of corruption of the Law provisions.

Thus, as a matter of priority, it is necessary to bring into conformity all laws and regulations governing PPP, as imperfect legal regulation of PPP will prevent full-fledged initiation of the PPP projects by foreign investors.

A potential investor needs a predictable and reliable legal and regulatory framework, i.e. fewer, simpler and better regulations. In addition, the regulatory framework should take into account the interests of the recipients of services (private partners) and allow them to participate in legal procedures that protect their rights and guarantee their access to the decision-making process.

In most cases, investors prefer to work in countries where it is sufficient to rely on general legislation rather than sector-specific regulations for project implementation, such as transport or education, because interests of the increasingly more stakeholders are affected by the general legislation and there is less chance that problems would emerge as a result of changing laws.

Practice shows that it is much easier to make changes in the guidelines, instructions, and other regulatory acts than in-laws, because a single document regulating PPP can be more flexible and loyal. Sectoral regulation may be inconsistent and hinder the activities of investors, as amending the laws is a very long process.

However, the specifics of PPP projects due to the socio-economic development of our country and the existing problems and challenges in various spheres of the society preclude systematization of the regulatory framework on PPP in one single law.

Given that to create the foundations for the digital economy in the Kyrgyz Republic, in terms of determining the PPP objects aimed at digital transformation of the information systems, information resources, technological systems and telecommunication networks, it is necessary to take into account the specifics of the ICT sphere. Specifics of the development of information technology and the ever-growing volume of the database elements cannot be subject of a PPP agreement financed from the state budget (in the absence of budgetary funds), as there is a need for continuous improvement and modernization of ICT systems, while capacity of this process can be an object of the long-term support of private investment rather than the state. In this regard, it is proposed to develop an effective PPP Law in the field of ICT as a separate regulatory act or as part of the new legal act.

This regulatory act should create a new platform for interaction between the state and the private sector, to build a "smart partnership", the result of which will be the widespread implementation of PPP projects with the latest digital solutions and innovations in the country.

## International experience

The popularity of PPP in a particular country depends on the models of interaction between the government and private investors. The main condition for interaction is business-friendly legislation. The partnership mechanism is most widely used in the countries of the Anglo-Saxon legal system, which allows the use of PPP in small and medium-sized projects.

Depending on the socio-economic development level of the country, the use of PPP varies by country. In the G7 countries, healthcare is in the first place, education – in the second, and roads – in the third. For example, in the US the highest priority sector is roads, in Great Britain - health and education, in Germany – education, in Italy, Canada and France – healthcare.

The leading sector for the use of successfully completed PPP projects in such countries as Austria, Belgium, Denmark, Australia, Israel, as well as Ireland, Finland, Spain, Portugal, Greece, South Korea, Singapore and others, is road construction and only then – education and healthcare. This pattern in the use of PPP projects by industry can be seen in countries in transition and in the developing countries: the further a country is from the G7 level of development, the more PPP projects are implemented to build roads, tunnels and bridges, airports and prisons.

Thus, in developing countries and countries in transition, PPP in the healthcare and education sectors (as opposed to roads) will not be a priority. Given a lower level of economic development in these countries, transport infrastructure should be the first priority for attracting investment through PPP. In countries such as Central and Eastern Europe (Bulgaria, Czech Republic, Hungary, Croatia, Poland, Romania), the Baltics (Latvia) and the CIS (Ukraine), the leading PPP areas are roads, bridges and tunnels, light rail and airports.

In India, Brazil, Chile, Hong Kong, Mexico, Saudi Arabia, United Arab Emirates, as well as in the above countries, the roads are in the first place in terms of the number of PPP projects, followed by airports, prisons and water treatment facilities.

When studying the experience of certain states, it was found that Great Britain has long been considered the undisputed leader in the application of the PPP mechanisms, as this country is the leader both by the total number of projects and by the scope of PPP in various areas and industries.

The British Government is actively using in practice the concept of interaction and partnership between private business and the state in the form of PPP to attract private investment in infrastructure development and provision of services, which entails the reduction of the financial burden on the state budget. PPPs are used when private companies can perform public tasks just as well, and sometimes better, than the state itself.

This improved efficiency is achieved through the distribution of risks and tasks, the application of the life cycle principle, and the improvement of the incentive instruments.

In **Germany**, one of the main areas of PPP application is information and communication technology (hereinafter - ICT), which is deemed to have a major role in the process of transforming the national economy from industrial to informational. The roles of PPP participants are distributed as follows: the government creates the conditions for ICT development by adopting framework legislation and economic policy incentives, while the private sector ensures investment in scientific research and development ("R&D") in the field of ICT, implementation of ICT in the domestic economy and in foreign trade transactions.

In **Denmark**, social housing projects are financed through PPPs: the local authorities provide the developer with an interest-free government loan that is repaid during 50 years.

PPP in the **PRC** is now a widespread practice, but it is mainly used in infrastructure development (construction of roads and highways, bridges, educational institutions, etc.). At the same time, PPP mechanisms are implemented using such organizational and project forms as contracts and concessions.

An example of a practical digital PPP is the "Fifth-generation PPP" project in Europe. The state creates necessary physical infrastructure through the state order, and then transfers the right to use the infrastructure in the format of a concession. It should be noted that while in a conventional concession only one concessionaire can claim a facility, in the case of "digital PPP" the number of concessionaires is limited only by the network capacity.

As for the CIS countries, the emergence of the PPP institution in the **Russian Federation** (hereinafter - RF) began back in 2004 and is related to infrastructure projects.

In 2015, the PPP Law of RF was adopted, which enabled the use of new and effective PPP models in Russian practice. Specific legislation on PPP consists of the PPP Law, the Concession Agreements Law (CA Law), other normative legal acts of the Russian Federation, as well as normative legal acts of its constituent entities. However, as follows from the PPP Law, all legal provisions in the field of PPP contained in other normative legal acts of Russia must comply with the PPP Law and the CA Law.

These laws provide for transferring certain rights and obligations of a public partner (concedent) to other persons (state bodies, local self-governments and legal entities).

The most successful example of PPP in telecommunication in RF is the "e-governance" in the satellite city of Moscow - Zelenograd. This "virtual city" includes several dozens of databases and numerous services - a "one window" service, thematic SMS-notifications, Internet surveys, a navigation system of urban transport and electronic document management. A number of ER-Telecom Holding projects are being implemented in the Volga Region to connect schools and city video surveillance systems to the Internet, as well as monitoring of housing and utilities facilities.

On April 24, 2017, amendments were made to the Federal Law "On Public-Private Partnership, Municipal-Private Partnership in the Russian Federation and Amendments to Certain Legislative Acts of the Russian Federation" and "On Concession Agreements", **recognizing IT systems as PPP and concession objects** - previously only immovable property objects were recognized as such. Thus, according to paragraph 1 of Article 33.1, a private partner undertakes to create the object of the agreement and then to operate it, and a public partner grants the private partner the rights to use the results of intellectual activity. At the same time, it is not clear whether the creation of software and databases can be considered as an object of a PPP agreement. Other mandatory conditions of the agreement are the creation of the object of the agreement by a private partner and its full or partial financing of the creation of the object of the agreement, as well as operation and maintenance of the object by a private partner.

**In Kazakhstan**, the main driver of the ICT PPP projects development and implementation at the national level is the project of the state program "Digital Kazakhstan", in which a number of projects are provided for implementation through the PPP mechanism. By the Resolution of the Government of the Republic of Kazakhstan in 2016, the National Info communication Holding "Zerde" was defined as the National Institute for ICT Development (hereinafter - NID), one of the tasks of which is to attract and implement investment in industrial and innovation projects in the field of ICT, through participation in the authorized capital of subjects of the industrial and innovation activities, creation of legal entities, including with foreign participation.

Zerde Holding is the largest company and a leader in the field of ICT of the Republic of Kazakhstan, carries out extensive work to attract direct investment through the PPP mechanism. Participation of investors in the ICT projects, through the PPP mechanism allows the state to save budgetary funds and attract transfer of advanced technologies, ensuring performance of important tasks in the field of digitalization of conventional industries in the long term.

Examples include projects to create an intelligent transport system, projects in the field of medicine, a number of "Smart city" projects and many others. The intelligent transport system will be created to improve the efficiency of transport and road complex management at the national level. This will be a single platform, uniting through the integration bus a set of interconnected automated systems to solve the problems of traffic control, monitoring and management of all types of transport, informing citizens, carriers, companies, government agencies on the organization of transport services in the city, region and country.

The main purpose of building a "Smart city" is to increase the overall satisfaction of citizens by improving the infrastructure of Astana, as well as the development of a unified approach to the sustainable development of Astana through the implementation of the principles and mechanisms of the "smart city". "Smart city" makes optimal use of ICT to improve the quality of life, competitiveness of the economy, creating necessary innovative, energy-efficient infrastructure, the developing of

internationally competitive products and services for local and foreign tourists and ensuring its sustainable development.



## Section 20. Related changes in the CC

### Content

- Signing and executing digital transactions and accession agreements,
- Securing the rights to digital assets,
- Transactions with such assets, electronic payments.

### Current regulation (existing legislation):

1. Civil Code of the Kyrgyz Republic.
2. Law of the Kyrgyz Republic "On electronic signature".
3. Law of the Kyrgyz Republic "On virtual assets"
4. Law of the Kyrgyz Republic "On enactment of the Tax Code of the Kyrgyz Republic".
5. Law of the Kyrgyz Republic "On notaries".

### Brief description of the identified shortcomings and international practice benchmarks

No.	Shortcomings	Type <sup>38</sup>	Best practices
20.1	<p>Civil Code neither provides the definition, nor does it mention:</p> <ul style="list-style-type: none"> <li>- Smart contract, i.e. performing or execution of a transaction using digital technology.</li> </ul> <p>In addition, the following concepts are missing completely:</p> <ul style="list-style-type: none"> <li>- cryptocurrency,</li> <li>- blockchain,</li> <li>- mining,</li> <li>- tokens.</li> </ul> <p>It is necessary to enshrine these concepts in the Civil Code, based on which it would be possible to operate the market of new objects of economic relations ("tokens", "cryptocurrency", "mining", etc.) existing in the information and telecommunication network.</p>	G	<p>Members of the California Senate and Assembly approved a bill that would bring <i>blockchain</i>, <i>smart contracts</i> and related technologies into the legal realm. The <b>Russian Federation</b> has adopted a draft Federal Law "<i>On Digitalization of Financial Assets</i>", which will regulate the relations arising in the creation, issuance, storage and circulation of digital financial assets, as well as the exercise of rights and performance of obligations under smart contracts. This draft law clearly defines digital concepts, peculiarities of cryptocurrency, digital applications and similar issues.</p> <p>The Republic of Belarus has taken a more radical approach to the implementation of civil law digitalization. Similarly important are changes that have been introduced into the legislation of Belarus. Belarus was the first country in the world to enshrine smart contract in its legislation. The President of Belarus approved the <i>Decree "On the development of digital economy"</i>, where a smart contract is an independent civil law contract. In addition, the Resolution of the National Bank of Belarus "<i>On Performing and</i></p>

<sup>38</sup> The following types of regulatory shortcomings are listed in the Table:

- (G) regulatory gap (regulation is required, but it is missing)
- (O) obsolete provision (the existing provision should be changed)
- (N) non-functioning provision (the existing provision is non-functioning for the reasons described)
- (B) this provision is an unreasonable barrier to the implementation of activities

			<i>(or) Execution of Legally Significant Actions through Smart Contracts" was signed.</i>
<b>20.2</b>	<p>Currently, the Civil Code of KR provides that the objects of civil rights are things, including money and securities, other property, including property rights; works and services; protected information, results of intellectual activity and similar means of individualization (intellectual property), as well as other tangible and intangible benefits.</p> <p>In this regard, civil legal treatment of the digital rights and virtual assets has not been addressed</p>	<b>O</b>	<p>The Russian Federation has adopted the draft Federal Law "On Digital Financial Assets", which will regulate the relations arising in the creation, issue, storage and circulation of digital financial assets, as well as exercising rights and performing obligations under smart contracts.</p> <p>Besides that, the Federal Law "On Amendments to Part One, Part Two, and Article 1124 of Part Three of the Civil Code of the Russian Federation" amended the Civil Code of RF, according to which the concept of digital rights and obligations; a transaction performed using electronic or other technical means, fulfillment of certain obligations by using information technologies, determined by the terms of the transaction, etc., have emerged in the Civil Code of the Russian Federation.</p> <p>Since 2021 taxes in the Swiss canton of Zug can be paid in cryptocurrency - tax deductions will be accepted in bitcoins and ethers.</p> <p>On September 7, 2021, El Salvador enacted the Law granting bitcoin, the first cryptocurrency, the status of a legal tender on a par with the US dollar.</p> <p>Cryptocurrencies in Japan were granted, to a certain extent, the status of a means of payment, which can be used by any recognizing person to make payments for goods, works, services in relations with an indefinite range of persons.</p> <p>In Brazil, the definition of digital currency is broad enough that cryptocurrencies like bitcoin well fall under respective concept and regulation.</p>
<b>20.3</b>	Smart contracts in the Civil Code of KR should be referred to as self-executing transactions; and a clear definition of this type of contract should be provided.	<b>G</b>	<p>In addition to the US, Russian Federation, Belarus, and several other countries where smart contracts are enshrined in the legislation, smart contracts are also actively used in Central Asian countries.</p> <p>For example, Kazakh developers are introducing blockchain-based smart</p>

		<p>contracts in outdoor advertising for the first time. Citrix company known as the author of several innovative developments in the field of Smart City, presented its new technology for the automation and convenient launch of an advertising campaign. The company's IT department this year is introducing smart contracts based on hyperledger blockchain platform to manage and control smart boards, or more precisely, to automate business processes and make them transparent.</p> <p>The Ministry of Justice of Azerbaijan plans to introduce blockchain technology and smart contracts in the fields of housing and public utilities and consumer services.</p> <p>Several other US states (in addition to those mentioned above) have recognized the legal validity of the blockchain-based smart contracts or intend to do so soon. For example, Arizona did so back in spring 2017, Ohio made a proposal in May, and Florida did so in January. In addition, in July 2020, it was reported that Great Britain might legalize blockchain-based smart contracts.</p>
--	--	---

### Comments

The volume of digital services in Kyrgyzstan is also expected to grow rapidly every day, involving more and more citizens and legal entities as users. At the same time, the lack of any reference to digital law in the civil legislation of the Kyrgyz Republic leaves users and providers of such services outside of legal regulation and legal protection, which aims at an orderly stimulation of civil turnover. The lack of legal regulation in this area is certainly a serious constraint, making civil legislation increasingly archaic and inadequate to the current rapid progress.

Provisions that involve elements of the digitalization of civil law relations has just started to emerge in the Civil Code of the Kyrgyz Republic, but definitions such as cryptocurrency, blockchain, mining, and tokens are missing and such types of contracts as smart contracts, transactions using digital technology are not mentioned.

Here it should be noted that the Law "On enactment of the Tax Code of the Kyrgyz Republic" dated January 18, 2022, No.4, introduces the following concept in paragraph 1 Article 176 of the Civil Code: "The written form of the transaction is also considered to comply within the case of transactions performed by a person using electronic or other technical means, which allows reproducing the content of the transaction in the unchanged form on a material medium, and the requirement of a signature is deemed satisfied, if any method that allows reliably identify the person who expressed his/her will was used. The law, other legal acts and agreement of the parties may provide for special means of authentic identification of a person, who has expressed the will".

In addition, the Law "On electronic signature" of the Kyrgyz Republic dated July 19, 2017 No. 128 regulates the relations on the use of electronic signatures in civil law transactions, provision of the

state and municipal services, the performance of state and municipal functions, as well as in legally significant actions. This law defines electronic signature, signature key and signature key certificate, etc.

Since a smart contract is: first, a certain algorithm designed to automate the process of execution of contracts, that is, it is a set of rules and a sequence of actions for execution; second, these rules are stored to discuss the terms of the contract, then automatically checked, after which the conditions are fulfilled according to the digital protocol. In addition, smart contracts are confirmed by a digital signature, each party of the contract has its own digital signature key.

Based on the above, it is clear that the legislation of the Kyrgyz Republic does not prohibit the conclusion of smart contracts by the parties to the contract, i.e. civil law transactions using smart contracts can be concluded without violating the law. At the same time, there is no legal regulation of this type of contract and the parties' liability for the risks of entering into such contracts is also not indicated.

In addition to the above regulation, it should be noted that public discussion of the Law on Virtual Assets dated January 21, 2022, No. 12 is currently underway.

The purpose of the Draft Law "On Virtual Assets" is to create a legal framework for the cryptocurrencies circulation and cryptocurrency exchange service providers, as well as to reduce the risks of terrorist financing and legalization (laundering) of criminal proceeds.

The Draft Law refers to cryptocurrency as a type of virtual asset, which is a digital expression of value that is created, stored and circulated in electronic (digital) form and is not a monetary instrument, currency and/or means of payment, and does not certify property or non-property rights. However, the very definition of "virtual asset", as well as the entire draft law, does not answer the fundamental question: what a virtual asset is - is it a property, a commodity, an intangible/investment asset, an exchange commodity, a value, a service?

It becomes clear that there are questions to the interpretation of cryptocurrency in this definition, as well as to the cryptocurrency circulation in civil law. Since the concept of "cryptocurrency" is still ambiguous, would cryptocurrencies be fully liberalized, certain risks may arise.

The approach to the definition of a virtual asset is insufficiently elaborated from a legal point of view and leads to legal uncertainty, as well as does not take into account the established global practices and experience in regulating the crypto industry in other jurisdictions.

This draft law in the current version is not aimed at adequate regulation and development of the legal position, taking into account the interests of the crypto industry, which will lead to "over-regulation" (according to the Russian model) of the emerging market, leading to the fact that crypto-enthusiasts and professionals will work with cryptocurrency very carefully or will stop altogether, and develop crypto-projects in more comfortable jurisdictions.

One of the biggest shortcomings of this draft law is the ban on the use of virtual assets as a means of payment for goods, work and services, which contradicts the nature and purpose of cryptocurrency created as a simple payment instrument, a means of payment available for use by anyone.

For example, means of payment are those named in the draft law as "unsecured virtual assets" in relation to which there is no person/persons bearing obligations to each owner of such virtual assets are bitcoin, Ethereum, litecoin, other blockchain-based coins.

Crypto-businesses, in fact, will not be able to use cryptocurrency for their operations, it will not be profitable to operate in the Kyrgyz Republic, which will entail moving to more favorable jurisdictions. A ban on the use of a virtual asset as a means of payment reduces the economic feasibility of owning a cryptocurrency and will slow down this innovative industry in the country. Relevant cryptocurrency exchanges will either leave the country or close down. The bans will primarily affect commercial entities.

We emphasize that private transactions are almost impossible to trace, the use of cryptocurrencies as a means of payment can take place without the use of banking channels, which makes it impossible for financial supervisory bodies to fully implement control over money flows in the country; the authorized bodies of the state are unable to fully control private financial transactions with cryptocurrencies also due to technical limitations.

Thus, it becomes clear that at present the authorized bodies of the state are unable to fully control financial transactions with cryptocurrencies, both due to technical limitations and due to the lack of appropriate regulatory framework.

It should also be noted that, for example, taxation of the object, which is not recognized by the civil legislation in any particular capacity (property, investment asset, etc.), is impossible. If it is property - do the owners have obligations to declare ownership of such property and what threshold is, who determines it and where, in what NLA, payment of taxes due in case of disposal (alienation, e.g.) on the amount of income received, who and how keeps records, etc.

In general, the current normative legal acts of the Kyrgyz Republic do not provide a clear regulation of the smart contracts implementation, information on cryptocurrency, as well as the work of blockchain technology in the law.

As for the implementation of these innovations in different countries of the world, we can see that the use of cryptocurrency, implementation of contracts through smart contracts, and the use of blockchain technology in the law are already being actively implemented. However, only a small number of countries have established cryptocurrency as a "digital commodity" and the smart contract as a contract in civil law and have adopted normative legal acts related to the full legalization of cryptocurrency as a financial asset.

In some countries, as dated October 2021, cryptocurrency can be used to buy goods and services, a liberal regime is introduced to allow people to develop this sphere (Germany, Japan, Switzerland), while maintaining strict requirements on customer identification procedures, trying to effectively integrate cryptocurrencies into their economy.

In the Swiss canton of Zug, from 2021 it will be possible to pay taxes in cryptocurrency - tax deductions will be accepted in bitcoins and ethers. On September 7, 2021, a law came into force in El Salvador granting bitcoin, the first cryptocurrency, the status of a legal tender on a par with the US dollar. El Salvador's authorities bought bitcoins and the state owns a total of 1,120 BTC worth over \$66 million. Germany is a country where it is possible to pay with bitcoins. In Japan, bitcoin has been a digital means of payment since 2016. Singapore maintains a favorable environment in the electronic financial technology industry. Blockchain projects are underway in the UAE. Tesla Company considers allowing customers to pay for electric cars with cryptocurrencies. The online platform Amazon has announced work to integrate bitcoin payments.

In the US, cryptocurrency is considered in various capacities, including as a property asset for tax purposes or (by the US Futures Trading Commission) as an exchange-traded commodity for purposes of applying certain provisions of exchange-trading laws. In the opinion of the US Securities and Exchange Commission (SEC), when a cryptocurrency is used to attract investment as part of Initial Coin Offering, its placement may be subject to US securities law and the cryptocurrency (token) itself may be treated as a type of security (an investment contract).

In addition, members of the California Senate and Assembly approved a bill that would bring blockchain, smart contracts and related technologies into the legal realm. Bill No. 2658 would amend the state's civil, government, insurance and corporate codes. One of the major achievements of Calderon's bill is also the legal definition of DLT and cryptocurrency technology. A smart contract is defined as "an event-driven program operating in a distributed, decentralized and shared register that can take control of and mandate the transfer of assets in that register". In addition, under the amendments, smart contracts would be included in the general legal definition of "contracts."

Several other US states have recognized the legal validity of blockchain-based smart contracts or intend to do so soon. For example, Arizona did so back in spring of 2017, Ohio made a proposal in May, and Florida did so in January. Also in July, it was reported that Great Britain might legalize smart contracts on the blockchain.

The Russian Federation has adopted a draft Federal Law "On Digitalization of Financial Assets", which will regulate the relations arising in the creation, issuance, storage and circulation of digital financial assets, as well as in exercising rights and performing obligations under smart contracts. This draft law clearly defines digital concepts, peculiarities of cryptocurrency, digital circulation and similar issues. In addition, the Federal Law "On Amendments to Part One, Part Two, and Article 1124 of Part

Three of the Civil Code of the Russian Federation" amended the Civil Code, according to which the concept of digital rights and obligations; a transaction performed by electronic or other technical means, the performance of certain obligations through the use of information technology, determined by the terms of the transaction, etc. have emerged in the Civil Code.

However, it remains difficult to say for sure whether such changes in the civil legislation and the effort to implement legal regulation of blockchain technology, as well as cryptocurrency circulation in the state had a positive impact or not. Since in practice, it remains unclear whether it is possible to control and regulate the circulation of the same cryptocurrencies in digital reality, as well as the issues of liability for smart contracts also remain relevant, despite their regulation in the law.

The Republic of Belarus has taken a more radical approach to the implementation of digitalization in the civil law. Similarly important are changes that have been introduced into the Belarusian legislation. Belarus was the first country in the world to enshrine smart contract in the legislation. The President of Belarus approved the Decree "On the development of digital economy", where a smart contract is an independent civil law contract. In addition, the Resolution of the National Bank of Belarus "On Performing and (or) Executing Legally Significant Actions through Smart Contracts" was signed.

At the same time, many approaches to the qualification of cryptocurrencies, reflected in foreign legal orders, are due to specific terminology and a particular legal system, as well as specificity of the tasks for which one or another approach was developed.

As a rule, point-by-point regulation is used abroad: relevant acts and explanations are adopted on separate, mainly public law issues (taxation, applicability of anti-money laundering legislation, etc.), in other areas legislators and regulators take a wait-and-see approach, providing space for self-regulation to the participants of cryptocurrencies circulation. Such point-by-point regulation is also necessary in the Kyrgyz Republic.

The issue of developing a system to regulate cryptocurrencies circulation is directly related to understanding its essence and enshrinement of the respective term in the national legislation. By defining cryptocurrencies as a means of payment, regulatory authorities face the dilemma of private and public money (fiat currencies), so many countries consider cryptocurrencies as a type of digital asset.

Such innovations in civil legislation are crucial for law digitalization in post-Soviet countries. However, the issue of introducing such type of contracts as smart contracts into the Civil Code of the Kyrgyz Republic should be considered carefully.

Thus, it is worth considering, first of all, amendments to the Civil Code of the Kyrgyz Republic, namely:

- Classify digital rights and virtual assets as types of civil rights objects and define the object of such rights in civil-law transactions;
- Incorporate performance of obligations using digital technologies determined in terms of the transaction, as well as inconclusive actions, into the methods of performing obligations;
- Add the terms "digital" and "electronic" to the "form of the transaction" in certain types of contracts in accordance with the above changes;
- In addition, enshrine in the Civil Code the concepts, on the basis of which it would be possible to operate the market of new objects of economic relations existing in the information and telecommunication network ("tokens", "cryptocurrency", "mining", etc.).
- It is also necessary to name smart contracts in the Civil Code as a self-executable transaction and provide a clear definition of this type of contract.

Thus, it is necessary to make appropriate (package) changes to the Civil Code of the Kyrgyz Republic and refer to virtual assets as civil rights objects (it is expressly stated in the Law "On virtual assets" that a virtual asset is an object of civil rights), as well as specify category (what it is), incorporate the concept of smart contract into the category of self-executed transactions in the Civil Code of the Kyrgyz Republic).

Summarizing the overall results of the above approaches, it should be noted that amendments to the normative legal acts for compliance with the practical innovations are due to objective developments in the field of law digitalization, which will also affect the Kyrgyz Republic. In particular, legal

enshrinement of the smart contract status and regulation of the relations between the parties will be a necessary factor in the development of the economic and financial system of the state.



## Section 23. Related changes in the Law "On Civil Service"

### Current regulation (existing legislation):

1. Law of the Kyrgyz Republic "On Public Civil Service and Municipal Service" dated October 27, 2021, No.125
2. E-Governance Law of the Kyrgyz Republic dated July 19, 2017, No.127
3. Decree of the Kyrgyz Republic President "On the National Development Strategy of the Kyrgyz Republic for 2018-2040" dated October 31, 2018, UP No.221
4. Decree of the Kyrgyz Republic President "On urgent measures to enhance the implementation of digital technologies in public administration of the Kyrgyz Republic" dated December 17, 2020, UP No.64
5. Decree of the Kyrgyz Republic President "On the National Development Program of the Kyrgyz Republic to 2026" dated October 12, 2021, UP No.435
6. Resolution of the Kyrgyz Republic Cabinet of Ministers "On the issues of the State Agency for Civil Service and Local Self-Governance under the Cabinet of Ministers of the Kyrgyz Republic" dated November 15, 2021, No.258
7. Resolution of the Kyrgyz Republic Cabinet of Ministers "On approval of the Action Plan of the Kyrgyz Republic Cabinet of Ministers on implementation of the National Development Program of the Kyrgyz Republic to 2026" dated December 25, 2021, No. 352
8. Resolution of the Kyrgyz Republic Cabinet of Ministers dated January 12, 2022, No. 2-r
9. Resolution of the Kyrgyz Republic Cabinet of Ministers dated March 24, 2022, No. 134-r
10. Concept of digital transformation "Digital Kyrgyzstan 2019-2023" approved by the Decision of the Security Council of the Kyrgyz Republic dated December 14, 2018, No. 2

### Brief description of the identified shortcomings and international practice benchmarks

No.	Shortcomings	Type <sup>39</sup>	Best practices
23.1	<p>Legislation regulating professional retraining and advanced training of civil servants has no any requirements for training on digital skills and competencies.</p> <p>In addition, there are neither established performance indicators, nor online training and certification or the possibility for creating digital teams in the agencies</p>	G	<p>The development of the innovative digital reality poses special requirements for the professional competencies of a public servant, which should also include digital competencies, in accordance with which a public servant must improve his/her knowledge, skills and abilities, be able to work with modern information tools, platforms and programs.</p> <p>At the same time, the analysis shows that the majority of training programs for civil servants abroad (64%) focus on the following two areas: information security and the formation of successful leaders in the digital age. In the area of digital communication and citizen engagement, 55% of programs develop competencies of the public</p>

<sup>39</sup> The following types of regulatory shortcomings are listed in the Table:

- (G) regulatory gap (regulation is required, but it is missing)
- (O) obsolete provision (the existing provision should be changed)
- (N) non-functioning provision (the existing provision is non-functioning for the reasons described)
- (B) this provision is an unreasonable barrier to the implementation of activities

		<p>administration employees. In Singapore, for example, civil servants are trained to use an online office to jointly edit files with stakeholders, while the US offers a separate course to train staff on how to provide information to citizens in a simple form.</p> <p>Social media management and cooperation with the media have a special place in educational programs. For example, social media in Great Britain is perceived as a tool to increase innovation. Skills of working with data (their user-friendly analysis, interpretation and graphical visualization) when creating public services are taught to students in almost half of the surveyed curricula.</p> <p>The analysis of the foreign advanced training programs for civil servants showed that 11 leading countries in digital development pay special attention to such areas of training in ICT educational programs as security, leadership, and communication in the digital age.</p>
--	--	--

### Comments

The legislation of the Kyrgyz Republic does not contain any requirements on the need for training (professional retraining and advanced training) on digital skills and competencies for civil servants.

At the same time, the effectiveness of the public administration system depends on the professional performance of civil servants and the quality of implementation of public decisions. At present, the world is at the stage of transforming public administration institutions, conditioned by the development of digital technologies, a key factor in determining the economic growth rate.

The ongoing technological changes affect the structure of requirements for the level of qualifications of government agency employees. The introduction of digital technologies expands the toolkit for civil servants' work, which requires updating their skills and competencies.

National strategic documents note the importance and relevance of professional training of civil servants. Thus, the National Development Strategy of the Kyrgyz Republic for 2018-2040, draws attention to the need for large-scale programs for retraining and advanced training of civil servants. The Concept of Digital Transformation "Digital Kyrgyzstan 2019-2023", notes that, based on the challenges of digital transformation, there is a need for legal transformation of the entire public administration system. It should aim at improving normative legal acts, including in the civil service (digital competencies and digital skills of civil servants, their professional retraining and advanced training). Along with this, the Decree of the President of the Kyrgyz Republic "On urgent measures to enhance the implementation of digital technologies in public administration of the Kyrgyz Republic" dated December 17, 2020, UP No. 64 instructs to form a training and advanced training program for the state and municipal employees on digital skills and cybersecurity, as well as service delivery in the digital

economy by June 1, 2021, and the Decree of the President of the Kyrgyz Republic "On the National Development Program of the Kyrgyz Republic to 2026" dated October 12, 2021, UP No.435, provides for the launch of the national educational program "Systematic improvement of digital competencies of civil servants to support digital public administration".

Thus, there are currently plans to train civil servants to digital skills and competencies. For example, as part of the preparation for the implementation of the electronic document management system, employees of the Presidential Administration of the Kyrgyz Republic were trained to demonstrate the processes of document movement from the creation in the system to sending to the addressee. Employees were also trained to create internal orders, track the route and status of the sent document, as well as to form a report on the performance discipline <sup>40</sup>.

The ongoing technological developments have an impact on the qualifications requirements for the state agencies' staff. The introduced digital technologies expand the operational tools of civil servants, which requires updating their competencies. Therefore, there is a need to revise the qualification requirements for candidates for the civil service positions, by expanding the list of competencies.

However, civil servants training on digital skills improvement and digital competencies development must be systematic and ongoing.

The Law of the Kyrgyz Republic "On Public Civil Service and Municipal Service" stipulates that a civil servant must take advanced training at least once every 3 years. The established maximum period between the advanced training should be reduced when it comes to digital skills, based on the realities of a dynamically developing market. At the same time, today, every civil servant must-have digital skills and competencies, so it is necessary to provide advanced training for all civil servants, who lack digital skills. In addition, a fundamentally new approach to the interaction between the state and citizens puts forward completely new requirements for civil servants, who will implement this approach. Thus, there should be an opportunity within the state bodies to create "digital teams" - a symbiosis of competencies, i.e. a team built on the role model of project management, in which several main roles of team members are distinguished, each with its qualifications, competencies, area of responsibility, etc., to perform a specific task and achieve the goal (employees from different departments/divisions shall be involved).

### **International experience**

Areas for advanced training of civil servants on digital competencies abroad. According to the Global Digital Competitiveness Index, the US and Singapore have consistently been leaders in digital technologies adoption.

The rating is based on three factors: human capital, information technology and readiness for digital transformation.

Let's look at the top 15 countries in the rating to further explore the areas of advanced training on digital skills for civil servants.

In the group of 11 leading countries, we found organizations that provide advanced professional education programs for public sector employees (Table 1).

**Table 1: Organizations implementing digital development programs for civil servants in the leading countries in terms of digitalization in 2020**

	<b>Country</b>	<b>Organizations providing advanced professional education for civil servants</b>
<b>1</b>	USA	University of Digital Technology
<b>2</b>	Singapore	Civil Service College

<sup>40</sup>[https://24.kg/vlast/232805\\_chinovnikov\\_prezidentskoy\\_administratsii\\_uchat\\_elektronnomu\\_dokumentirovaniyu/](https://24.kg/vlast/232805_chinovnikov_prezidentskoy_administratsii_uchat_elektronnomu_dokumentirovaniyu/)

3	Sweden	Institute of Public Administration of Sweden
4	Hong Kong	Institute of Training and Public Service Development
5	Netherlands	European Institute of Public Administration
6	South Korea	National Institute of Human Resource Development
7	Finland	Finnish Institute of Public Administration
8	Canada	Digital Academy of the Canadian School of Public Administration
9	Great Britain	Academy of Digital Government Services; Civil Service College
10	UAE	Virtual Academy
11	Australia	Institute of Public Administration in Australia

To identify the leading key topics of digital skills development for public servants abroad, let's look at the content of the ICT advanced training courses for public servants in the top digital competitiveness countries that implemented programs for public servants on information technology in 2020.

Table 2 presents the most common areas for ICT training for civil servants and topics used by 45% or more of the above organizations in the surveyed countries.

**Table 2. Key areas of advanced training on digital skills for civil servants in organizations from the top countries in terms of digitalization in 2020**

<b>o.</b>	<b>Topics of programs</b>	<b>Number of organizations implementing programs</b>
1.	Information security	(7 of 11) 64%
2.	Leadership in the digital age	(7 of 11) 64%
3.	Digital communications and citizen engagement	(6 of 11) 55%
4.	Challenges and new technologies	(5 of 11) 45%
5.	Mass media and social media	(5 of 11) 45%
6.	Design in creating user-centered digital services	(5 of 11) 45%
7.	Data analysis and machine learning	(5 of 11) 45%
8.	Data visualization	(5 of 11) 45%

The analysis showed that the majority of overseas government employee training programs (64%) are focused on two areas: information security and the formation of successful leaders in the digital age. In the area of digital communications and citizen engagement, 55% of programs develop the

competencies of public administration employees. In Singapore, for example, government employees are trained to use an online office to jointly edit files with stakeholders, while the US offers a separate course to train staff on how to provide information to citizens in a simple form. Social media management and cooperation with the mass media have a special place in the training programs. For example, social media in Great Britain is perceived as a tool to increase innovation. Skills of working with data (their analysis, user-friendly interpretation and graphical visualization) in the creation of public services are taught to students of almost half of the surveyed curricula.

Note that the areas of digital technology learnt by civil servants are diverse in each country, but, in our view, we can identify common trends in the formation of ICT competencies: concern for information security, training of managers to digital transformation, and development of digital communications skills of all categories of employees.

### **Conclusions and recommendations**

Based on the above, the concept of the advanced training of civil servants can be defined as the improvement of qualifications for better performance of professional duties and compliance with the requirements of the socio-economic environment. It is confirmed that in modern conditions to match the qualifications of public sector employees to the changing professional environment, it is necessary to develop digital competencies, which include not only technical knowledge and skills in a specialized environment, but also personal qualities and digital culture.

The development of competencies in the field of information technology is the basis for the digital transformation of public administration. Digitalization changes social relations inside and outside the public sector: it requires improvement of work practices and digital skills of civil servants. By exploring the problem of developing digital competencies of the public administration personnel through surveying thematic areas of training for public sector employees in other countries, it was found that the following areas are key today: information security, leadership in the digital age, and digital communications and interaction with citizens.

Thus, legislative changes shall:

- Establish requirements for public servants to take advanced training courses in order to acquire digital skills and competencies;
- Reduce the maximum period between advanced training courses when it comes to digital skills;
- Incorporate digital skills and competencies into advanced training courses for civil servants in the following areas: cybersecurity, leadership in the digital age, etc.;
- Preference should be given to those potential civil servants, who have digital skills and competencies;
- Create opportunities for online training and certification;
- Establish performance indicators for civil servants;
- Provide opportunities for the creation of digital teams within government agencies.

## Section 24. Cloud technologies

### Content

- Legal regulation of cloud technology
- Personal data protection in the use of cloud technology

### Current regulation (existing legislation):

1. E-Governance Law of the Kyrgyz Republic;
2. Law of the Kyrgyz Republic "On Personal Information";
3. Decree of the Kyrgyz Republic President "On National Development Program of the Kyrgyz Republic to 2026" dated October 12, 2021, UP No. 435;
4. Decree of the Kyrgyz Republic President "On the National Development Strategy of the Kyrgyz Republic for 2018-2040" dated October 31, 2018, UP No. 221;
5. Resolution of the Kyrgyz Republic Government "On approval of the requirements for the protection of information contained in the databases of the state information systems" dated November 21, 2017, UP No. 762;
6. Resolution of the Kyrgyz Republic Cabinet of Ministers dated January 12, 2022, No.2-r;
7. The Concept of Digital Transformation "Digital Kyrgyzstan 2019-2023" approved by the Decision of the Security Council dated December 14, 2018 No.2.

### Brief description of the identified shortcomings and international practice benchmarks

No.	Shortcomings	Type <sup>41</sup>	Best practices
24.1	The legislation of the Kyrgyz Republic does not directly regulate the use of cloud technologies. The concept of "cloud technology" is not legally defined.	G	The Republic of Korea applies a systematic approach to the legal regulation of the ICT industry, which is characterized by the fact that each area of digital development requires a special law. As for cloud technology, the Cloud Computing Development and Protection of Its Users Act No. 13234, dated March 27, 2015, as amended on July 26, 2017 (ACT ON THE DEVELOPMENT OF CLOUD COMPUTING AND PROTECTION OF ITS USERS Act No. 13234, March 27, 2015 Amended by Act No. 14839, July 26, 2017) is in force. The Act establishes three requirements for quality assurance of cloud services and protection of information: - protection of the rights of the cloud service users, rights and obligations of the cloud service providers On February 17, 2022, the Verkhovna Rada of Ukraine adopted the Law on Cloud Services No. 2075-IX, signed by the President of Ukraine on March 17,

<sup>41</sup> The following types of regulatory shortcomings are listed in the Table:

- (G) regulatory gap (regulation is required, but it is missing)
- (O) obsolete provision (the existing provision should be changed)
- (N) non-functioning provision (the existing provision is non-functioning for the reasons described)
- (B) this provision is an unreasonable barrier to the implementation of activities

		<p>2022. The law defines legal relations arising in the provision of cloud services and establishes features of cloud services used by public authorities, local governments, military formations formed in accordance with the laws of Ukraine, state enterprises, institutions, and organizations.</p> <p>The law introduces the concepts of "clouds", "cloud computing technology" and "cloud services".</p> <p>The law establishes the following types of cloud services:</p> <ul style="list-style-type: none"> <li>- infrastructure as a service;</li> <li>- platform as a service;</li> <li>- software as a service;</li> <li>- security as a service.</li> </ul> <p>In accordance with this law, cloud services are provided by:</p> <ul style="list-style-type: none"> <li>- a private cloud;</li> <li>- a collective cloud;</li> <li>- a public cloud;</li> <li>- a hybrid cloud</li> </ul> <p>The participants in the cloud services relationship are:</p> <ul style="list-style-type: none"> <li>- users of cloud services, including public users;</li> <li>- cloud service providers;</li> <li>- providers of data processing center services;</li> <li>- public authorities.</li> </ul> <p>The Law requires cloud and data processing center providers to maintain a list of cloud services and/or data processing center services. At the same time, according to Article 10 of the Law, cloud and data processing center services are provided on a contractual basis. The Cabinet of Ministers shall approve a contract to provide cloud services. Provision of cloud and data processing center services to the public users of cloud services shall comply with legislation on personal data protection, data protection and cyber security.</p> <p>The contract for the provision of cloud services shall be approved by the Cabinet of Ministers. Provision of cloud and data processing center services to public users</p>
--	--	--

			<p>of cloud services shall be subject to the requirements of legislation on personal data protection, data protection and cyber security. As for the restrictions on the provision of cloud services, the prohibition of processing information constituting state secrets, official information, state and unified registers, the creation and operation of which is established by law, through cloud resources and/or data processing centers located abroad should be noted.</p> <p>In essence, the adopted law is an attempt to introduce the Cloud-first concept at the legislative level in Ukraine.</p>
<b>24.2.</b>	<p>E-Governance Law of the Kyrgyz Republic, being the main in the sphere of legal regulation of digital development issues, establishes the e-governance principles, one of which is the right of e-governance participants to use any information technology at their discretion, provided that their use meets the requirements established by this Law and other laws of the Kyrgyz Republic. In this case, the only provision, which may violate the Law is the storage of confidential data in cloud services. Thus, Article 13 establishes access to confidential information. In this regard, when using cloud services, restrictions may be set in terms of storing data related to confidential information.</p>	<b>G</b>	<p>Article 12 of the Law of Ukraine "On Cloud Services" provides for a separate procedure for cloud services related to the processing of the state information resources or those with restricted access. This procedure provides for:</p> <ul style="list-style-type: none"> <li>- mandatory backup and storage of backups in independent systems;</li> <li>- data transfer from the cloud services user to the cloud services and/or data processing center services to provide cloud services, as well as from the cloud services provider to the cloud services user;</li> <li>- data transfer from one cloud services provider and/or data processing center services to another;</li> <li>- provision of information necessary for evaluating security of the network and information systems of cloud services and/or data processing center services, including documented security policies.</li> </ul>
<b>24.3</b>	<p>The Law of the Kyrgyz Republic "On Personal Information" defines the conditions of working with personal information, the procedure for the formation of the personal information arrays, the rights and obligations of subjects of personal information, holders (owners) and recipients of such information arrays. The law considers personal data to be confidential. At the same time, Article 25 of the Law allows</p>	<b>G</b>	<p>Analysis of the legal regulation practices in different countries shows that in matters of personal data protection, it is difficult to identify unambiguously best practices that are suitable in terms of the Kyrgyz Republic. Partially among the best practices are the General Data Protection Regulation of the European Union (GDPR), according to which service providers (DPC and cloud services) are subject to quite stringent</p>

<p>for cross-border transfer of personal data. One of the conditions for cross-border transfer of personal data under the jurisdiction of the Kyrgyz Republic is an international treaty between the parties, under which the receiving party shall ensure adequate protection of rights and freedoms of subjects of personal data and protection of personal data established in the Kyrgyz Republic. However, the use of cloud services may be beyond the jurisdiction of any state. When transmitting personal data through the global information network (Internet, etc.), the holder (owner) of the personal data array, which transmits such data, is obliged to ensure the transfer with appropriate means of protection, while respecting information confidentiality. In this regard, provisions of the Law on the one hand allow for the personal data transfer through the Internet and their storage outside the territory of the Kyrgyz Republic, but the question of their potential storage in cloud services remains open, because in this case to protect the rights of personal data owners, the Law should explicitly provide for the possibility of storing personal data in the cloud services.</p>	<p>requirements for the protection of personal data. DPC and cloud service providers are obliged to follow basic principles set out in Article 5 of the GDPR, such as:</p> <ul style="list-style-type: none"> <li>- Legality, fairness and transparency - there must be legal grounds under the GDPR for the collection and use of data, non-breach of any laws, openness, integrity from the beginning to the end on the use of personal data;</li> <li>- Limitation by the purpose - processing should be limited to what has been stated to the data subject. All specific objectives must be stated in the confidentiality policy and strictly adhered to;</li> <li>- Data minimization - using the minimum amount of data necessary to achieve the stated purposes;</li> <li>- Accuracy - Personal data must be accurate and not misleading; erroneous data must be corrected;</li> <li>- Limitation of data storage - do not store data longer than necessary, periodically audit the data and delete unused data;</li> <li>- Integrity and confidentiality/security - store data in a secure location and pay sufficient attention to data security.</li> </ul> <p>As part of enforcing these principles, DPC service providers must also follow GDPR Article 28 regarding the rights and obligations of the data processor, as well as Article 32 on data protection when processing.</p> <p>In terms of flexibility in legal regulation, partially, best practices can also include the experience of US legal regulation. In the US, for example, cloud computing is not regulated by a specific "cloud law" and its services are not subject to direct regulation. Instead, the legal and regulatory framework consists of a matrix of different rules, as broad as the scope of the technology itself, covering several industries. At the same time, cloud computing in the US is not regulated by a specific "cloud law", and its services are not subject to direct regulation. There are, however, a number of regulations that apply to data protection, including the Gramm-Leach-Bliley Act (GLBA) and</p>
---	---

		<p>the Family Educational Rights and Privacy Act (FERPA). GLBA contains 2 key rules for "financial institutions" storing data in the cloud: the financial privacy rule and the safeguards rule. FERPA - protects student information collected by educational institutions and related vendors. Protecting student information under the FERPA rule is key when using cloud-based applications that process student records. IT administrators need to be aware of the information being transferred to the cloud network or application</p>
--	--	--

### Comments

Based on the analysis of the Kyrgyz Republic legislation and the review of the practices of other countries, it should be stated that the current legal regulation of cloud technology in the Kyrgyz Republic is clearly insufficient. In this regard, adequate legal regulation of cloud technology can be ensured following different models. One model is to regulate by adopting a special law, following the example of Korea and Ukraine. Another model may be the consolidation of the legal regulation of cloud technologies in different sectoral normative legal acts as in the United States, Germany, and France. Another option may be to leave the use of cloud technology at the discretion of users and cloud service providers, in other words, to implement these relationships on a contractual basis.

Taking into account the current realities and the experience of different countries, none of the above legal regulation options seems optimal in pure form for the Kyrgyz Republic. In this regard, given the specifics of the cloud technology, namely the fact that cloud storage facilities may be outside the jurisdiction of a particular state, it is necessary to enshrine in the legislation the conditions for using cloud technology, applying no methods of strict regulation of the entire range of cloud services and leaving the right of choice to users and cloud service providers to determine the options of interaction themselves. Legal regulation of the cloud services should focus more on creating conditions and opportunities for the use of the cloud services, following the example of the Korean legislation. However, we should not forget the protection of the rights and freedoms of the Kyrgyz Republic citizens in the use of various cloud services. On this basis, it is proposed to enshrine general conditions for the use of the cloud technology, namely, define the concepts of cloud, cloud services and other concepts related to cloud computing, the rights of citizens and legal entities to use cloud services, protection of personal data in cross-border transfer, cases and possibilities of personal data storage, issues of cybersecurity. At the same time at the subordinate level it is also important to establish requirements, procedures for cloud services provision, types, methods of cloud services provision, the use of cloud services, requirements for service providers, data processing centers, models of cloud services, models of their deployment, regulation of the public cloud services, etc.

We believe this option of ensuring legal regulation will allow successful implementation of the Cloud First policy in Kyrgyzstan, which will ensure the effective implementation of the national strategic documents to build a modern digital infrastructure.

## Section 25. Technical requirements for data processing centers (DPC)

### Content

- DPC (general provisions, technical requirements)
- DPC standards

### Current regulation (existing legislation):

1. E-Governance Law of the Kyrgyz Republic;
2. Law of the Kyrgyz Republic "On the fundamentals of technical regulation in the Kyrgyz Republic";
3. Decree of the Kyrgyz Republic President "On the National Development Program of the Kyrgyz Republic to 2026" dated October 12, 2021, UP No.435;
4. Decree of the Kyrgyz Republic President "On the National Development Strategy of the Kyrgyz Republic for 2018-2040" dated October 31, 2018, UP No. 221;
5. Resolution of the Kyrgyz Republic Government "On approval of the requirements for the State Data Processing Centers and their connecting communication channels" dated December 31, 2019, UP No.747;
6. Resolution of the Kyrgyz Republic Government "On approval of the requirements for protection of information contained in the databases of the state information systems" dated November 21, 2017, No.762;
7. Resolution of the Kyrgyz Republic Government "On certain issues related to the state information systems" dated December 31, 2019, No.744;
8. Resolution of the Kyrgyz Republic Cabinet of Ministers dated January 12, 2022, No.2-r;
9. Concept of Digital Transformation "Digital Kyrgyzstan 2019-2023" approved by the Decision of the Security Council dated December 14, 2018 No.2.

### Brief description of the identified shortcomings and international practice benchmarks

No.	Shortcomings	Type <sup>42</sup>	Best practices
25.1	<p>The E-Governance Law of the Kyrgyz Republic provides for the regulation of the state data processing centers only. So, according to Part 2 of Article 24, the data processing centers and their connecting communication channels, both built at the expense of the republican and local budgets and used on the basis of contracts of rent, services provision and other contractual basis can be used as part of the e-governance state infrastructure.</p> <p>In accordance with paragraph 10 of Part 2 of Article 6, the Government of the Kyrgyz Republic approves the requirements for the</p>	<b>G</b>	<p>In the context of the Kyrgyz Republic, the most acceptable seems to be general provisions on DPC, including DPC service providers. At the same time, the contractual nature of the relationship between users and providers, following the example of the Law "On Cloud Services" of Ukraine should be established.</p>

<sup>42</sup> The following types of regulatory shortcomings are listed in the Table:

- (G) regulatory gap (regulation is required, but it is missing)
- (O) obsolete provision (the existing provision should be changed)
- (N) non-functioning provision (the existing provision is non-functioning for the reasons described)
- (B) this provision is an unreasonable barrier to the implementation of activities

	state data processing centers and their connecting communication channels. At the same time, other DPCs, which are not part of the state e-governance infrastructure, are not mentioned at all.		
<b>25.2</b>	Resolutions of the Government of the Kyrgyz Republic dated December 31, 2019 No.747 and dated November 21, 2017 No. 762 establish fundamental basic requirements for SDPC, including more detailed requirements for the installed server rooms and the requirements for information systems. However, in general, the provisions of these normative legal acts do not establish any specific criteria for the parameters and engineering infrastructure of SDPC.	<b>G</b>	<p>The surveyed legislations of a number of countries (Russian Federation, Kazakhstan) and existing DPC standards (standards- EN 50600 Design of Data Centre Facilities and Infrastructures, Uptime Institute Standards, ISO27001 and ISO9001) show that DPC requirements generally include much more conditions and basic regulatory parameters than provided in the legislation of the Kyrgyz Republic. In general, the standards provide for similar requirements for DPC. For example, the TIA/EIA-942 standard outlines:</p> <ul style="list-style-type: none"> <li>- the requirements for the data processing center location and its structure;</li> <li>- the requirements for the cable infrastructure</li> <li>- the requirements for reliability specified by infrastructure layers</li> <li>- the requirements for the external environment.</li> </ul> <p>To date, of the standards used in DPC certification, TIA/EIA-942 is one of the most widely used guidance documents for professionals, who are directly involved in the design and creation of a structured cabling system in DPC. TIA/EIA-942 contains the requirements and recommendations that describe a number of subtleties and points to consider when designing a structured cabling system in a data center. In particular, this standard contains a detailed description of the functional subsystems and passive elements of the structured cabling systems, as well as the structured cabling system architecture.</p>
<b>25.3</b>	DPC standardization issues are not enshrined in the legislation. The legislation on technical regulation does not provide sufficient mechanisms for the adoption of international standards at the national level.	<b>G</b>	<p>One option to ensure standardization is the adoption of the national standards for telecommunications infrastructure harmonized with international standards by the levels of reliability of the DPC engineering infrastructure, following the example of the Republic of Kazakhstan.</p>

## Comments

The E-Governance Law of the Kyrgyz Republic entered into force on July 25, 2017, established the e-governance objectives and principles, as well as powers of certain state bodies in the field of e-governance. Article 24 of the Law defines the state data processing centers. Thus, according to this article of the Law, "the state data processing centers and their connecting communication channels are designed to host and operate state information systems. Data processing centers and their connecting communication channels both built at the expense of the national and local budgets and used on the basis of contracts of rent, services provision and other contractual basis can be used as part of the state infrastructure of e-governance. The requirements for the state data processing centers and their connecting communication channels, including the requirements for stability and security, as well as the procedure for incorporating the data processing centers and their connecting communication channels into the state infrastructure of e-governance shall be established by the Government of the Kyrgyz Republic.

According to paragraph 4, Part 3 of Article 18 of the Law, the data processing centers are part of the state infrastructure of e-governance. At the same time, in accordance with paragraph 10 of Article 6 of the Law, the requirements for the state data processing centers and their connecting communication channels, including the requirements for their security and stability, as well as the procedure for incorporating the data processing centers and their connecting communication channels into the state infrastructure of e-governance shall be approved by the Government of the Kyrgyz Republic.

Pursuant to this provision of the Law, the Government of the Kyrgyz Republic adopted the Resolution "On approval of the requirements for the state data processing centers and their connecting communication channels" dated December 31, 2019 No.747. The requirements establish goals and objectives of the state data processing centers (hereinafter - SDPC), their parameters and structure, and also determine the requirements for security and stability of SDPC and their connecting communication channels. According to this Resolution, the main parameters of SDPC are:

- a high request processing speed (the speed should not depend on the size of the data storage);
- parallel servicing of a given number of users without any noticeable performance degradation for the users.

As for the SDPC structure, it is established that it includes information, telecommunication and engineering infrastructure.

The information infrastructure includes highly reliable server hardware and software that ensure the main functions of SDPC - information processing and storage.

The telecommunications infrastructure ensures interconnection of the SDPC elements, as well as data transmission between SDPC and users.

The requirements for SDPC placement are regulated by the requirements for the protection of information contained in the databases of the state information systems approved by the Resolution of the Kyrgyz Republic Government dated November 21, 2017 No. 762 (hereinafter - Resolution 762). This Resolution establishes the Requirements for the systems of uninterrupted operation of technical means of the server equipment and for the server room of the state body, local self-government and organization.

Thus, the above Resolutions of the Government set fundamental basic requirements for SDPC, including more detailed requirements for server rooms established by the Resolution 762 and requirements for information systems approved by the Resolution 744. However, in general, the provisions of the above normative legal acts do not establish any specific criteria for SDPC parameters and engineering infrastructure.

Given the need to ensure sufficient legal regulation of the state data processing centers, attention should be paid to the legislation of the Kyrgyz Republic on technical regulation. Since May 22, 2004, the Law of the Kyrgyz Republic "On the fundamentals of technical regulation in the Kyrgyz Republic" is in force. The law establishes the legal framework in the area of:

- development, adoption, application and execution of mandatory requirements for products, including buildings and constructions, and/or product-related requirements for the design processes (including research), production, construction, installation, adjustment, storage, transportation, implementation, operation and utilization;
- development, adoption, application, and execution on a voluntary basis of the requirements for products or processes of design (including research), production, construction, installation, adjustment, storage, transportation, sale, operation, utilization, performance of works and provision of services.

According to Article 2, one of the technical regulation principles is uniformity of the rules that establish the requirements for products or processes of design (including research), production, construction, installation, commissioning, storage, transportation, sale, operation, utilization, performance of works or provision of services.

This law establishes the principles, objectives and procedures for the adoption of technical regulations, standardization and conformity assessment. In accordance with Article 14, the standardization aims to:

- stimulate scientific and technological progress;
- increase the competitiveness of products, works and services in accordance with the development of science, engineering and technology;
- improve facilities safety, taking into account the risk of the natural and man-made emergencies
- promote compliance with the requirements of the technical regulations;
- ensure energy efficiency and resource-saving;
- ensure technical and information compatibility;
- ensure uniformity of measurements, comparability of measurement and test results;
- ensure products interchangeability;
- increase the safety of life, health of individuals, life and health of animals and plants, as well as the property of individuals and legal entities, state and municipal property, and the environment.

According to Article 15, one of the principles of standardization is the voluntary application of the standards and the use of international, and regional standards and regulations as a basis for the national standards preparation. Article 16 establishes that "international, regional standards and national standards of other countries, as well as regional sets of rules and codes of rules of foreign countries are adopted in the Kyrgyz Republic as national standardization documents in accordance with the methodology established by the national standardization authority".

At the same time to date, there is no such methodology established by the national standardization authority.

Based on the above, it follows that the legislation of the Kyrgyz Republic establishes basic requirements for SDPC, while not covering the activities of other (private) DPCs. In this regard, the issue of legal regulation of non-state DPCs should be considered in terms of the right of participants in e-governance to use any information technology at their discretion, if their use meets the requirements of the E-Governance Law and other laws of the Kyrgyz Republic. However, there are no any requirements for private DPCs.

Based on the above, in the context of the Kyrgyz Republic, it seems inappropriate to apply any strict requirements for DPCs. Establishing the requirements for certification of the state data processing centers also poses certain questions, since certification according to generally recognized global standards needs a lot of financial resources.

Therefore, it is proposed to enshrine in the legislation a general concept of DPC and establish that DPC services are provided on a contractual basis (this provision should be applied separately from SDPC), as well as define mandatory terms and conditions of the contract. This will also apply to the cloud services application.

In terms of standardization and improvement of requirements for DPC, several options to improve legal regulation of both SDPC and DPC as a whole are proposed:

1) The current provisions of the normative legal acts of the Kyrgyz Republic should be supplemented with more specific parameters established in the generally recognized standards, and will be designed to ensure appropriate security, energy efficiency, fault-tolerance of DPC;

2) Adoption of the national standards for telecommunications infrastructure harmonized with the international standards by the levels of reliability of the DPC engineering infrastructure. At the same time, it is important to ensure that the main parameters of design, placement, operation, energy efficiency, fault-tolerance, etc. comply with these standards.

3) Adoption of the international standards or standards of foreign countries as the national ones. In this case, it is necessary to enshrine in the legislation the rules and procedure for adopting such standards as the national ones (possibly develop and approve a methodology in accordance with the legislation on technical regulation).

## Section 30. Cybersecurity

### Content:

- Criminal and administrative responsibility;
- Digital evidence in criminal proceedings;
- Digital evidence in civil proceedings;
- Information protection and cybersecurity.

### Current regulation (existing legislation)

1. Criminal Code of the Kyrgyz Republic;
2. Criminal Procedure Code of the Kyrgyz Republic;
3. Code of Offences of the Kyrgyz Republic;
4. Law of the Kyrgyz Republic “On Protection of State Secrets of the Kyrgyz Republic”;
5. E-Governance Law of the Kyrgyz Republic;
6. Law of the Kyrgyz Republic “On Personal Information”
7. Law of the Kyrgyz Republic “On Guarantees and Freedom of Access to Information”;
8. Law of the Kyrgyz Republic “On Telecommunications and Postal Service”;
9. Electronic Signature Law of the Kyrgyz Republic
10. Law of the Kyrgyz Republic “On Legal Protection of Softwares and Databases”;
11. Law of the Kyrgyz Republic “On the Fundamentals of Technical Regulation in the Kyrgyz Republic”;
12. Decree of the Kyrgyz Republic President “On the National Development Strategy of the Kyrgyz Republic 2018-2040” dated October 31, 2018, UP No. 221;
13. Decree of the Kyrgyz Republic President “On the National Security Concept of the Kyrgyz Republic” dated December 20, 2021 UP No. 570;
14. Resolution of the Kyrgyz Republic Government “On the Concept of Information Security of the Kyrgyz Republic for 2019-2023” dated May 3, 2019, No. 209;
15. Resolution of the Kyrgyz Republic Government “On the Cybersecurity Concept of the Kyrgyz Republic for 2019-2023” dated July 24, 2019, No. 369;
16. Resolution of the Kyrgyz Republic Government “On Approval of Requirements for the Protection of Information Contained in the State Information Systems Databases”, dated November 21, 2017, No. 762;
17. Resolution of the Kyrgyz Republic Government “On the Issues of Organization and Governance of State-owned Enterprises of the Kyrgyz Republic in the Digitalization Area” dated July 4, 2019, No. 340;
18. Digital transformation concept “Digital Kyrgyzstan 2019-2023”.

### Brief description of the identified shortcomings and international practice benchmarks

No.	Description of the deficiency	Type <sup>43</sup>	Best practice
30.1	<p>The existing Criminal Code articles do not fully respond to the current and potential threats in cyberspace.</p> <p>Lack of legislation that would form the criminal-legal basis for combating cybercrime, which does not meet the current law enforcement needs and prevents from:</p>	G/O/N	At present, the 2001 Budapest Computer Crime Convention is a key international document that can become the basis for forming the national criminal law framework for combating cybercrime and will harmonize the national legislation with international legislation.

<sup>43</sup> The following types of regulatory shortcomings are listed in the table:

- (G) regulatory gap (regulation is required, but it is missing)
- (O) obsolete provision (the existing provision should be changed)
- (N) non-working provision (the existing provision is non-working for the reasons described)
- (B) this provision is an unreasonable barrier to the implementation of activities

<p>suppressing cybercrimes successfully;          assessing objectively the extent of cybercrime;          building an effective legal framework for countering cybercrime.</p> <p>Specific terms used throughout the Criminal Code do not comply with the glossary of terms used in specific international legal acts and policy documents on cybersecurity and national legislation governing the communications and telecommunications sector.</p> <p>Some of the qualifying features of the offenses stipulated by Chapter 40 are already covered by other offenses' features.</p> <p>In addition to this Chapter, some offenses of other categories do not contain the qualifying signs of crimes using the Internet or computer technologies.</p>	<p>Given the cross-border nature of cybercrime, this approach to forming domestic legislation is essential to create conditions for effective cooperation with other countries worldwide.</p> <p>The Budapest Convention became open to signing more than 20 years ago, on November 23, 2001. Sixty-six countries have ratified the Convention, two have signed it, and ten have received invitations to join.</p> <p>More than 140 countries are working with the Council of Europe to strengthen their legislation and capacity to combat cybercrime.</p> <p>This Convention is the first international treaty on crimes committed through the Internet and other computer networks and deals with copyright violations, computer fraud, child pornography, and network security violations.</p> <p>One should also pay attention to the creation of a criminal law framework for bringing to justice persons who have committed acts related to illegal access, interception of data using technical devices, influence on information and the functioning of the system, illegal use of devices, fraud using information and communication technologies and etc.</p> <p>It is also necessary to ensure the implementation of the Law of the Kyrgyz Republic “On Personal Information”, which implies the liability for violations of the personal data legislation.</p> <p>Besides, to ensure the legal certainty principle, it is very important to bring terms and concepts in line with the Budapest Convention and the ITU glossary, international standards, the Cyber Security Strategy, and the Kyrgyz Republic communications and telecommunications legislation.</p> <p>It is necessary to distinguish clearly between the qualifying features of offenses.</p> <p>It is important to harmonize terms and concepts with the Budapest Convention, the ITU glossary, international standards, the Cyber Security Strategy,</p>
---	---

		<p>and the Kyrgyz Republic legislation on communications and telecommunications.</p> <p>In terms of qualifying signs of crimes committed using the Internet and computer technology, it is necessary to consider amending several articles of the Criminal Code. Particularly - Article 161 on the distribution of pornographic items; Article 204 on violation of copyright, related rights, and rights of patent holders - and other articles.</p> <p>Of course, it is necessary to study and consider setting a uniform qualification for cybercrimes as used by law enforcement, prosecutors, and courts.</p>
<p><b>30.2</b></p>	<p>Special provisions of the Code of Offences are not responsive to current and potential threats in cyberspace.</p> <p>There is competition between the legal provisions of the Criminal Code and the Code of Offences regarding prejudicial evidence.</p> <p>The terms used do not comply with the terminology of the current criminal law, international acts and requirements.</p> <p>A radical revision of Chapter 26 of the Code of Offences is required, also because of the need to create conditions for criminal law protection against the violation of existing legal requirements for personal information protection.</p>	<p><b>G/O/N</b></p> <p>The terms and concepts should be brought in line with the Budapest Convention, the ITU glossary, international standards, the Cybersecurity Strategy and the Kyrgyz Republic legislation on communications and telecommunications, including to ensure the legal certainty principle.</p> <p>It is also necessary to ensure the implementation of the Law of the Kyrgyz Republic “On Personal Information”, which implies the liability for violations of the personal data legislation.</p> <p>One of the methods for ensuring strict compliance with legal provisions by the parties to legal relations concerning the personal data processing, above all, is the existence of legal liability for breach of the law provisions. In the absence of legal grounds for holding persons liable for violating laws, the state bodies can not ensure the rule of law as an important component of the legal state, which implies guarantees of compliance with the prescriptions contained in the law provisions. It is the legislative establishment of the procedure for ensuring the rule of law that will be perceived by citizens as a consolidation of their real opportunities provided by the state.</p> <p>This is especially relevant when the state bodies use citizens' biometric data to ensure effective digital transformation of public administration and</p>

			<p>transparency of the electoral process. In the future, it is planned to actively use information and communication technologies to achieve the goals of modernizing public administration, the economy and the social sphere through innovative technologies, where the main citizen's identifier will be only his/her personal data. In such circumstances, it is important to ensure responsibility for:</p> <ul style="list-style-type: none"> <li>– processing of personal data without a legal basis;</li> <li>– unreasonable refusal to provide a personal data subject with information concerning personal data processing;</li> <li>– failure to comply with legal requirements of the authorized state body on personal data;</li> <li>– unreasonable refusal to the authorized state body on personal data or the Ombudsman (Akyikatchy) of the Kyrgyz Republic.</li> </ul>
<p><b>30.3</b></p>	<p>The current criminal procedural legislation does not provide a legal basis for the collection, storage, processing and presentation, and evaluation of the electronic (digital) data for subsequent proof.</p>	<p><b>G</b></p>	<p>At present, the 2001 Budapest Computer Crime Convention is a basic international document that can become the basis for forming a national criminal law framework for combating cybercrime and will harmonize the national legislation with the international legislation.</p> <p>Given the cross-border nature of cybercrime, this approach in forming domestic legislation is very important in terms of the need to create conditions for effective cooperation with other countries of the world.</p> <p>The Budapest Convention became open to signing more than 20 years ago, on November 23, 2001. To date, 66 countries have ratified the Convention, two have signed it, and 10 have received invitations to join. More than 140 countries are working with the Council of Europe to strengthen their legislation and capacity to combat cybercrime.</p>

			<p>This Convention contains a number of powers and procedures, such as the search of computer data, networks, and interception, defining the principles of international cooperation in investigating cybercrimes, and the exchange of technical information.</p> <p>Attention should also be paid to the creation of a criminal procedural framework for the collection of evidence and further prosecution of those who committed cybercrimes, including in other states of the world, including amendments to the CPC regarding the collection, storage and evaluation of electronic data (evidence).</p>
<p><b>30.4</b></p>	<p>The E-Governance Law contains a number of provisions relating to data protection and information security issues. Most of these provisions partly declare the fundamental information protection principles and directions, which should be taken into account and respected when building an e-governance system. But it should be recognized that these provisions have not lost their relevance today, correspond to existing paradigms in the field of data protection, and correlate with certain international principles and approaches in the field of cybersecurity, where the key role is played by human rights and freedoms.</p> <p>However, such regulation of cybersecurity is insufficient. Besides, these provisions can largely be characterized as non-working, although they are not relevant anymore. The information protection provisions in the Law have not been comprehensively implemented in practice. The regulatory enforcement mechanisms did not further support many conceptual provisions. For example, Article 3 stipulates that one of the e-governance is to ensure the information security of the Kyrgyz Republic. This task is universal and imposes obligations, including the protection of the critical information infrastructure facilities, both on the state and on the subjects</p>	<p>N</p>	<p>Today's cybersecurity trends have moved beyond the traditional approaches to protecting information. Today, the term “digital resilience” has emerged, which implies a systemic approach focused on prevention and adaptability, incorporating the risk management issues and consisting of prevention, reduction, preparedness, response, and recovery. Now this concept was also directed at governments. This is a more comprehensive approach, requiring the active participation of all stakeholders, including government, business, and civil society.</p> <p>Digital resilience today is a set of opportunities, methods and enabling environments that ensure the activity continuity of the government, business and society in the face of environmental changes, including man-made disasters and other crises.</p> <p>We must rethink cybersecurity as digital resilience - a set of strategies, practices and capabilities that help us anticipate, prepare, prevent and respond to the inevitable crises and disasters that will depend on and influence our increasingly digitally dependent society.</p> <p>The point is to recognize that digital transformation and digital resilience go hand in hand.</p> <p>At the application level, digital resilience consists of four key</p>

	<p>themselves - the information array holders, which involves detailed sub-legislative regulation of legal relations in this area.</p>		<p>pillars/components: continuity, cybersecurity, data and confidentiality, and digital citizenship.</p>
<p><b>30.5</b></p>	<p>In the Cybersecurity Strategy for 2019-2023, when building the key player architecture included in the state cybersecurity system and determining their areas of responsibility, a bias was made towards the system militarization. The role of civilian government agencies and private entities has not been taken into account, nor have the possible benefits of public-private partnerships in this area been considered.</p> <p>Many important provisions of the Strategy remain unimplemented. First of all, it concerns the principle of priority of cyber security of the critical information infrastructure. The Strategy identified the need to form a unified system of the critical information infrastructure security of the Kyrgyz Republic as the priority task. However, until now, legislatively:</p> <ul style="list-style-type: none"> <li>- the sectors, industries and areas of activity have not been defined where the critical information infrastructure facilities operate, including the government systems;</li> <li>- criteria and parameters determining whether objects belong to the critical information infrastructure have not been approved;</li> <li>- there are no mandatory requirements to ensure the security of their facilities for operators of critical information infrastructure.</li> </ul> <p>The following provisions of the Strategy have not been implemented relating to:</p> <ul style="list-style-type: none"> <li>- the criminalization of computer crimes in accordance with the international approaches to combating cybercrime;</li> <li>- methods and means of computer criminalistics, introduction of the digital evidence concept into the legal acts, description and presentation of its</li> </ul>	<p><b>B/O/N</b></p>	<p>It is necessary to take into account the recommendations of the Expert Group of the Commission on Crime Prevention and Criminal Justice of the UN General Assembly, which were set out in the Report of the Expert Group meeting to conduct a comprehensive study of cybercrime, held in Vienna on July 27-29, 2020. In particular, it is recommended to involve nongovernmental organizations and academia in efforts to prevent and counter cybercrime, because their participation allows for the broadest, most diverse and comprehensive view of the problem and, in particular, to guarantee the protection of human rights, freedom of speech and privacy.</p> <p>In addition, as mentioned above, current trends in cybersecurity have moved beyond traditional approaches to protecting information. Today it is necessary to take a prevention-oriented and adaptive approach, which includes risk management issues and consists of: prevention, reduction, preparedness, response and recovery - in other words, discuss digital resilience. This is a more comprehensive approach, requiring the active participation of all stakeholders, including government, business, and civil society. At the application level, digital resilience consists of four key pillars/components: continuity, cybersecurity, data and privacy, and digital citizenship.</p>

	<p>criteria, characteristics and capturing methods;</p> <ul style="list-style-type: none"> <li>- ensuring that digital evidence is recognized as having the same legal force as other evidence;</li> <li>- the harmonization of the KR legislation in terms of criminalization and investigation of computer crimes, cross-border extradition from the Kyrgyz Republic of persons suspected of committing computer crimes or convicted for committing them in foreign countries;</li> <li>- the consideration of engaging private companies to collect digital evidence and conduct forensic examinations of digital evidence for law enforcement agencies of the Kyrgyz Republic.</li> </ul>		
30.6	<p><u>Resolution</u> of the Kyrgyz Republic Government dated November 21, 2017, No. 762 approved the Requirements for the protection of information contained in the databases of state information systems, which define measures to protect information, as well as state information systems and ensure the security of information contained in their databases. In particular, it establishes requirements covering the use of information technology, the organization of cybersecurity, information systems, application software, technology platforms, hardware and software complexes, telecommunications networks, and systems of uninterrupted operation of server equipment and server rooms. That is, this resolution practically regulates all major practical aspects of data protection and cybersecurity in state information systems. However, in practice, these requirements in most cases are not implemented. To date, no cybersecurity positions have been introduced, let alone specialized units. There is a lack of workforce and funds, and there are no clear mechanisms for the compliance inspections.</p>	N/O	<p>Despite such circumstances, this Resolution is still relevant today, with the exception of certain organizational and technical provisions that require a natural revision. Since more than five years have passed since the resolution was adopted, cybersecurity paradigms have been replaced with the new, more effective and technologically advanced cybersecurity approaches and methods have been developed.</p> <p>In such context, it is possible to apply certain provisions and principles of the American National Institute of Standards and Technology (NIST), including the Minimum Security Requirements for Federal Information Systems and Information of Federal Importance. This standard defines the specification of minimum security requirements for the government information systems (organizational, operational and technical measures).</p>

	<p>In our opinion, the main reasons for non-compliance with these requirements are the lack of understanding by most heads of state bodies and enterprises, insufficient competence of the state bodies' employees, for the proper understanding of the requirements and their application in practice. Based on the results of interviews and discussions on this issue with experts and representatives of the competent government agencies, it is clear that in general, the civil service has no necessary level of understanding and competence, and there is not enough funding to meet these requirements, except for the Ministry of Digital Development of the Kyrgyz Republic and the State Committee for National Security of the Kyrgyz Republic.</p>		
--	--	--	--

### Comments

The widespread digitalization is irreversible because the opportunities it creates to reduce costs in the broadest sense, optimize value chains and generate economic and public goods are too great and cannot be achieved by any other means at this civilization stage. However, the irreversibility of these changes directly follows from the irreversibility and inevitability of the risks and security threats posed by the development of ICTs and the digital economy. First of all, they include:

- security and resilience risks of the critical infrastructure, which is increasingly closed to digital business processes. At the same time, the risks associated with the development of cross-border computer crime are increasing;
- activation of the terrorist and extremist activities performed through digital communications;
- the growing scale of government and corporate cyber espionage.

Kyrgyzstan lags far behind the global trends in cybersecurity. Today, the cybersecurity paradigm has begun to change, and more and more states and companies are coming to realize that building defenses that cannot be broken is inherently utopian. A few years ago, information technology was considered, to a greater extent, as a means of facilitating document management and automation of business processes<sup>44</sup>. In this regard, there was a growing demand for highly intelligent protection tools that can solve the problem of timely detection of attacks and incidents (security information and event management (SIEM), network traffic analysis (NTA), integrated anti-APT solutions<sup>45</sup>). Under such conditions, the main task of any security system was to detect an attack and the attacker in the system as quickly as possible, to reduce his window of opportunity so that he did not have time to do irreparable harm. It was enough to create the necessary security perimeter, which would be aimed at finding and detecting a security perimeter intruder. However, as processes move beyond the security perimeter, as technology continues to evolve, and as actors become more mobile, specific security perimeters blur. Under this set of circumstances, it becomes difficult to find a point of application of the above safety tools. We have to accept these risks and understand that it is almost impossible to prevent cybercrime.

<sup>44</sup> <https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/cybersecurity-2019-2020-rus.pdf>

<sup>45</sup> <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-2019-2020/>

Given these circumstances, in addition to information protection, in 2018-2020, the IT community is increasingly talking about **cyber resilience**, the essence of which is to ensure the smooth and sustainable functioning of the information infrastructure in the presence of constant cybersecurity risks. Thus, the main effort should be focused on the design of systems taking into account the requirements for their cyber resilience. At the same time, one of the main and important areas of cyber resilience is the resilience of international Internet connections. As the digital economy develops, the financial and business sectors are increasingly using the technological Internet opportunities for international transactions and other types of international interaction. As a result, most international experts conclude that in the realities of the XXI century, there is an urgent need to move toward cyber resilience, which implies the ability to quickly recover from cyber incidents.

Moreover, today's cybersecurity trends are already moving beyond traditional approaches to information protection, including cyber resilience. Today's cybersecurity trends have moved beyond the traditional approaches to protecting information. Today, the term "digital resilience" has emerged, which implies a systemic approach focused on prevention and adaptability, incorporating the risk management issues and consisting of: prevention, reduction, preparedness, response, and recovery. Now this concept was also directed at governments. This is a more comprehensive approach, requiring the active participation of all stakeholders, including government, business, and civil society.

Digital resilience today is a set of opportunities, methods and enabling environments that ensure the activity continuity of the government, business and society in the face of environmental changes, including man-made disasters and other crises.

We should rethink cybersecurity as digital resilience - a set of strategies, practices and capabilities that help us anticipate, prepare, prevent and respond to the inevitable crises and disasters that will depend on and influence our increasingly digitally dependent society.

One lesson is to recognize that digital transformation and digital resilience go hand in hand.

At the application level, digital resilience consists of four key pillars/components: continuity, cybersecurity, data and confidentiality, and digital citizenship.

**1) Cybersecurity:** consists of the standards, practices, and human resources necessary to keep digital systems running and ensure a secure digital ecosystem. It includes a risk management system that allows decision-makers to calculate the magnitude of risk associated with digital systems and regularly maintain sufficient capacity to anticipate and respond to incidents and emergencies on an ongoing basis.

**2) Continuity** - includes the crisis management and recovery planning and opportunities that are practiced to ensure that institutions and organizations can continue to function under adverse conditions. Continuity depends on the availability of appropriate rules and standards in place to ensure business and operations continuity, while ensuring rapid adaptation within a predictable and generally accepted set of rules and best practices.

**3) Data protection and confidentiality** include a robust data ecosystem of laws, institutions, and capabilities that define and regulate data collection, storage, and disposal. Functionally, this includes defining property rights and how data, including personal information is collected and used by governments, businesses and other third parties. Confidentiality and data protection are important to prevent harm, ensure the integrity of government and business operations, protect individuals from potential abuse or exploitation and ensure economic activity.

**4) Digital citizenship** means citizens' willingness to take advantage of the digital systems and infrastructure. Digital citizenship includes basic computer literacy, basic digital hygiene and skills for safe and secure use of the Internet, and awareness of the rights and responsibilities of using digital systems and data.

The Government's goal is creating an enabling (including regulatory and legal) environment and opportunities for all parties (the government itself, business, civil society) to achieve digital sustainability. The outcome should be the actual possibility of sustainability; data management and confidentiality; continuity of digital services. The following needs to be done at the government level:

- ensure the sustainability of national networks and digital assets, including critical information infrastructure;

- form a civil government body responsible for digital resilience - The Center for Digital Resilience, which is an important component. For a long time, we have been talking about the need for cyber-attack response teams - CERTs, today we already need a national body for digital resilience;
- inform and educate (everyone) about digital hygiene in a systematic way;
- train and educate specialists working in critical sectors of the economy and public administration;
- review legislation, develop standards.
- stimulate the expansion of broadband Internet access;
- provide access to national cloud resources for businesses;
- ensure the transfer of public services to online format (primarily, those important for business - taxation, licensing and registration).
- support digital education;
- provide reliable access to centralized online educational resources for teachers and students;
- provide access to hardware and software; and high-quality broadband;
- expand access to health services (development of telemedicine);
- accelerate access to digital transactions (fintech, “sandboxes”, e-commerce).

In global cybersecurity practice, there is another trend to use the **supply chain security** approaches, which aims at securing the entire supply chain (of goods, services, works, etc.). Today's supply chain is becoming transnational and global, and supply chain security is becoming increasingly important. The presence of a wide range of cybersecurity risks, including those related to human factors, for one participant can cause difficulties for all other partners interconnected by the information and communication technologies. In most cases, we encounter problems when the supplied information and telecommunications equipment or software products are deliberately or unknowingly supplied with unlicensed software or with malware already installed. That is, because of the supply chain's interconnectedness, poor security in one link can jeopardize the functionality of the entire supply chain. An attack on the supply chain can occur in any industry, whether in the financial, public or private sector.

Attacks on supply chains are especially dangerous because if successful, it opens up access to hundreds or even thousands of companies. For example, according to a recent analysis, [the average cost of a data breach is \\$3.86 mln, and the cost of a mega-leak \(the theft of 50 mln records or more\) reaches \\$392 mln<sup>46</sup>](#). One of the most recent cyber attacks on the supply chain was against SolarWind, an IT infrastructure company with about 33,000 customers worldwide. In this attack, about 18,000 of the company's SolarWind Orion software upgrade platform customers became vulnerable.

In addition to the above trends in cybersecurity, many countries have begun to pay special attention to **the security of the critical information infrastructure (hereinafter - CII)**. In international practice, there are different approaches to regulating CII security. Based on the results of a comparative legal review of such methods, it is possible to distinguish two basic models of the CII regulation, depending on the direct regulation subject: the “object” (RF, Kazakhstan, Germany) and the “subject-activity” (EU except Germany, Georgia, Singapore, China, Japan).

In a number of jurisdictions of the selected models, one can find the presence of similar terms, similar duties of the CII subjects, identical powers of competent authorities in the field of CII security, the establishment of administrative and criminal liability for CII violations. This can be explained by the overall objective of the relevant regulation - to ensure CII safety.

The “object” model has the following features - the focus of regulation directly on the CII objects, the presence of a hierarchically structured regulation system, building the terminology based on the definition of CII and its objects, establishment of clear categorization criteria by establishing the “threshold values”, the precise and transparent definition of the subjects’ duties, with the main duties contained in the Law and the limited number of authorized bodies with clearly defined competence.

---

<sup>46</sup> <https://www.ibm.com/blogs/supply-chain/what-is-supply-chain-security/>

This approach allows, on the one hand, to streamline civil turnover (the new object owner understands which category it belongs to and what obligations will be imposed on them). On the other hand, it simplifies the state authorities' task to exercise control over the objects' owners even in cases where the latter have incorrectly performed categorization.

However, this approach lacks flexibility in terms of establishing site-specific safety requirements.

In contrast to the above model, the "subject-activity" model has different features, which are the regulation of subjects' activities in the field of CII, fragmentation of the legal regulation, building the terminology based on the definition of vital services, flexibility in categorization, risk-based approach, and multiple regulators in different areas of CII.

The subject-activity model of determining the regulation subject is more flexible. Thus, a particular object may be owned by a particular person but not used; therefore, damage to the object will not have a significant impact.

What matters in this model is the subject's economic activity in this or that area and the possible damage from a computer incident to such significant activity. This model provides for a greater degree of autonomy of subjects and generally involves a risk-based approach (in each specific case, the subject decides on the proportionality of measures taken to the existing cyber threats).

At the same time, this model is less structured and insufficiently transparent. This conclusion is particularly characteristic of the USA<sup>47</sup>.

In recent years, many countries have come to understand the need for the **public-private cooperation**, and cooperation between the international and regional communities, to ensure the adoption of effective ICT risk management and resilience strategies, and the commitment to develop the necessary national capacity to improve ICT confidence and security, address gaps and respond to significant cybersecurity risks<sup>48</sup>.

### **Brief Conclusions and Recommendations**

In the legal field, despite the abundance of normative legal acts in the field of information, there are no contradictions in cybersecurity matters. Overall, an analysis of the current information and cybersecurity legislation, with the exception of the 2019-2023 Cybersecurity Strategy, which was approved by Resolution of the Kyrgyz Republic Government dated July 23, 2019, suggests that it:

- does not define a legal framework, fundamental principles and unified approaches in cybersecurity of the Kyrgyz Republic, allowing to build a unified "system of coordinates" for the state cybersecurity policy;
  - represents an incomplete and outdated regulatory framework, most of the laws were formed in a fundamentally different technological and social environment, and therefore, are not compliant with current trends in cybersecurity;
  - does not include terms and definitions relating to the critical information infrastructure, etc;
  - does not provide effective control over ensuring the rights of the legal relations subjects in cybersecurity.
- At the same time, the Kyrgyz Republic does not currently have a number of basic conditions, and reference points, without which it is impossible to ensure the digital transformation security, in particular, and the development of the national IT and communications industry as a whole. Including the following:
- there are significant gaps in the regulations and policies to ensure cybersecurity (lack of concepts and approaches to respond to computer incidents, security of critical infrastructure and automated technological process management systems, international cooperation in the field of cybersecurity);

---

<sup>47</sup> Comparative analysis of approaches to the CII regulation, <https://internetpolicy.kg/2020/03/04/sravnitelnyj-analiz-podhodov-k-regulirovaniju-kii/>

<sup>48</sup> Managing National Cyber Risks, Melissa Hathaway

- in those government policy niches and areas, where a system of normative legal acts and their defined approaches is present, there is incompleteness and lagging behind current trends in ICT development and cybersecurity (countering computer crime, information protection regulation, technical standardization in the IT field);
- there is no approach to improving computer hygiene and digital literacy, and overall capacity building and the use of human resources in the government cybersecurity policy.
- The existing criminal legislation does not contain elements of cybercrimes committed today, and the procedural legislation does not contain methods for searching, recording and evaluating the digital evidence.

Since the Kyrgyz Republic has not yet experienced a large number of cybercrime prosecutions, the limited capacity of law enforcement and judicial officials in this area could potentially result in ineffective investigations, prosecutions, and convictions, allowing cybercriminals to stay unpunished and continue their criminal activities.

The problem of criminal evaluation of cybercrimes results from the weak legislative framework, the complexity of collecting evidence and the process of proof itself, the lack of competent persons in information technology in the state authorities, the lack of a generalized judicial system and other factors affecting the development of counteraction to cybercrime.

Therefore, in addition to strengthening the legal framework, it is important to improve the capacity of the criminal justice system to successfully combat and prevent cybercrime.

With the digital transformation of many sectors of social relations, there is still an outstanding issue of civil dispute resolution. The civil procedure law has no basis for collecting electronic (digital) evidence.

Besides, the abundance of normative legal acts in communications, digitalization, and telecommunications leads to ambiguous interpretation of many terms and definitions, and the fragmentation of the information market subjects, responsible for information security, prevents a clear policy in this area.

**In this regard, it seems necessary to:**

Legislatively define the legal and organizational framework, goals, directions and principles, and of state policy in the sphere of cybersecurity in the Kyrgyz Republic. This can be done by introducing a separate provision on cybersecurity. At the same time, it is advisable to disclose the basic cybersecurity concepts.

It is necessary to start reviewing legislation in the field of combating cybercrime and the use of electronic evidence, focusing on positive examples and successful world experience in implementing reforms. It is also essential to develop a unified methodology for identification, collection, receipt and storage of evidence presented in digital form for both criminal and civil proceedings. When developing such a document, it is advisable to base on the international standard ISO/IEC 27037:2012 “Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence”).

This standard was adopted by the ISO - International Organization for Standardization in 2012 and provides guidance on specific processes when handling the potential evidence presented in digital form (hereinafter digital evidence); these processes include: identification, collection, receipt, and preservation of potential digital evidence. These processes are necessary in an investigation and are designed to support the integrity of digital evidence, i.e., an acceptable methodology for obtaining digital evidence that will contribute to its admissibility for legal and disciplinary actions, and for another case as needed. This standard also provides general guidelines for collecting digital evidence that may be useful at the stage of analysis of such evidence.

This standard is intended to provide guidance to those responsible for the identification, collection, retrieval, and preservation of the potential digital evidence. These individuals include “first responders” for digital evidence, incident responders, and forensic laboratory managers. This standard provides assurance that responsible individuals manage the potential digital evidence in a rational and

generally recognized manner to systematically and impartially facilitate investigations that use digital devices and digital evidence while preserving their integrity and authenticity.

Another reason to use this standard is that some EEU countries have already implemented them in their standards and are widely using them in practice, which will allow the use of compatible technical standards for digital forensics and cross-border search of electronic evidence.

In addition, another basic international document is the Budapest Convention on Cybercrime of 2001, which can also become the basis for a national criminal and procedural framework for combating cybercrime and will harmonize the national legislation with international law.

Given the cross-border nature of cybercrime, this approach in the formation of domestic legislation is very important in terms of the need to create conditions for effective cooperation with other countries of the world.

The Budapest Convention became open to signing more than 20 years ago, on November 23, 2001. To date, 66 countries have ratified the Convention, two have signed it, and 10 have received invitations to join. More than 140 countries are working with the Council of Europe to strengthen their legislation and capacity to combat cybercrime.

This Convention contains several powers and procedures, such as the search of computer data, networks, and interception, defining the principles of international cooperation in the investigation of cybercrimes, and the exchange of technical information.

Ensure the implementation of paragraph 4.5 of the National Development Strategy of the Kyrgyz Republic for 2018-2040, and provisions of the Digital Transformation Concept “Digital Kyrgyzstan 2019-2023” related to cybersecurity, through the development and adoption of the Law on the Critical Information Infrastructure Security and several acts of the Government to ensure its implementation. As noted above, a thorough comparative analysis of the legislation and practices of the European Union, the United Kingdom, Asian countries, including China, Japan, Singapore, as well as the Russian Federation, Kazakhstan and Georgia identified two main models of CII security regulation, depending on the direct regulation subject: the “object” (RF, Kazakhstan, Germany) and the “subject-activity” (EU, except for Germany, Georgia, Singapore, China, Japan).

The analysis showed that in the early stages of legal regulation in the field of CII security, it is advisable to use the object approach. It should be borne in mind that without the establishment of clear criteria for categorization, leaving the object category definition to discretion of the state body or the person - the CII object owner itself, it is difficult to ensure uniformity in the protection of CII objects from potential threats.

Since the Russian approach to CII protection has been elaborated in details, the Russian Federation experience in CII regulation may be most useful in developing the approach of the Kyrgyz Republic, both in general, in defining the legislative model (due to the proximity of the legal order of the two countries) and in specific aspects of regulation (for example, in terms of categorizing the CII objects). Besides, the Russian approach also implies an identification of categories of significant CII objects. Referring to a certain category of significance means a greater likelihood of negative consequences in a certain area and increased requirements for the title holders of such objects.

A specific list of areas, depending on the importance of certain industries from an economic and social point of view for the state, should be determined in accordance with the subsequent categorization of the critical information infrastructure objects.

The Russian approach can also be considered as a possible model for CII terminology, taking into account features of the existing legislation of Kyrgyzstan on information and information technology.

Thus, analysis of the critical information infrastructure security models has shown that the Russian approach and the current mechanism for ensuring the critical information infrastructure security in the Russian Federation, compared to other systems established in other countries, is most consistent with the situation in the Kyrgyz Republic on the regulation of the information infrastructure use.

Provide additional criminalization of acts related to cybercrime. When implementing this approach, it is advisable to consider the law enforcement practices of other countries and use the

provisions of international cybersecurity acts. To harmonize the national legislation with international approaches, one may consider the provisions of the Budapest Convention on Cybercrime of 2001.

This Convention is the very first international treaty on crimes committed through the Internet and other computer networks, and in particular, deals with copyright violations, computer fraud, child pornography, and network security violations, among others.

Attention should also be paid to the creation of a criminal law framework for bringing to justice persons who have committed acts related to illegal access, interception of data using technical devices, influence on information and the functioning of the system, illegal use of devices, fraud using information and communication technologies and etc.

It is also necessary to ensure implementation of the Law of the Kyrgyz Republic “On Personal Information”, which implies the liability for violations of the personal data legislation, including liability for:

- processing of personal data without a legal basis;
- unreasonable refusal to provide the personal data subject with information concerning the personal data processing;
- failure to comply with legal requirements of the authorized state body on personal data;
- unreasonable refusal to the authorized state body on personal data or the Ombudsman (Akyikatchy) of the Kyrgyz Republic.

Besides, it is very important to bring terms and concepts in line not only with the Budapest Convention, but also with the ITU glossary, international standards, the Cyber Security Strategy, and the Kyrgyz Republic communications and telecommunications legislation, in order to ensure the legal certainty principle.

Develop and adopt acts relating to the procedural powers in pre-trial proceedings for cybercrimes and crimes involving electronic evidence.

It is necessary to consider recommendations set in the Report of the UN General Assembly Expert Group, which was prepared based on a comprehensive study of cybercrime in 2020, concerning the issues of legislative provisions on international cooperation in the field of cybersecurity.

Given the weak capacity of law enforcement and the judiciary bodies in the investigation and handling of cases involving digital evidence, it is necessary to systematically carry out activities to improve their skills. In doing so, it is very important to inform of the international practices and international trends in cybersecurity.

Consider joining regional and international initiatives, coordinating movements, and capacity building programs on combating cybercrimes to strengthen international cooperation in this area.

For lack of cybersecurity risk analyses, there is a need for state standardization of information security, including in the area of interagency interaction. To maintain the interoperability of information systems, standards must be open and meet the following criteria:

- adoption and further development of the standard should be based on an open decision-making procedure accessible to all stakeholders;
- documents describing the standard should be freely available;
- the patent requirements to use the standard should not include the royalty payment;
- the standard should be technology-neutral;
- the standard should support localization where appropriate.

Consider simplifying or putting into separate provisions the Requirements for the protection of information contained in the state information systems database. At the same time, make adjustments in terms of existing standards and current trends in ICT and cybersecurity. In this context, it is possible to apply certain provisions and principles of the American National Institute of Standards and Technology (NIST), including the Minimum Security Requirements for the Federal Information Systems and Information. This standard defines the specification of minimum security requirements for government information systems (organizational, operational, and technical measures).

## Section 31. Experimental legal regimes (regulatory sandboxes)

### Content

- legislation on experimental legal regimes

#### Current regulation (existing legislation):

1. E-Governance Law of the Kyrgyz Republic
2. Innovation Activities Law of the Kyrgyz Republic
3. Law of the Kyrgyz Republic “On the National Bank of the Kyrgyz Republic, Banks and Banking Activities”
4. Decree of the Kyrgyz Republic President “On Measures to Develop the Creative Economy and Create Conditions for the Progressive Development of the Kyrgyz Republic” dated April 21, 2022 UP No. 123
5. Resolution of the Board of the National Bank of the Kyrgyz Republic “On Approval of the Regulation “On the Special Regulatory Regime” dated August 12, 2020, No. 2020-P-12\45-3-(NLA)

#### Brief description of the identified shortcomings and international practice benchmarks

No.	Description of the shortcoming	Type <sup>49</sup>	Best practice
33.1	There is no "regulatory sandbox" law. This prohibits the possibility of using the "regulatory sandbox" in testing new legal relations, support for the ICT innovations, there are no partnership mechanisms, state support for technology startups.	G	Today, about 50 countries use the regulatory sandboxes. In 13 of them, legislation on special legal regimes has proven to be the most effective tool. For example, regulatory sandboxes have been successfully implemented in the United States, Australia, Singapore, UAE, Hong Kong, Malaysia, Thailand, Indonesia, Bahrain, Switzerland and Canada. The USA was the first country to resort to such mechanisms, it launched the Financial Conduct Authority (FCA) sandbox back in 2016. When piloting, regulators approved 50 of 146 applications submitted for piloting in the sandbox; 75 percent of the accepted companies were successful. The sandbox functions well; many startups get there and become attractive for investments at the first stage. Today, the FCA is one of the largest sandboxes in the world in terms of investment raised. After London, Singapore, where the monetary authority is the regulator, became interested in sandboxes. The criteria for evaluating startups here are similar to the British model, but there is no uniform timeframe for evaluating a

<sup>49</sup> The following types of regulatory deficiencies are listed in the table:

- (G) regulatory gap (regulation is required, but it is missing)
- (O) obsolete provision (the existing provision should be changed)
- (N) non-working provision (the existing provision is non-working for the reasons described)
- (B) this provision is an unreasonable barrier to the implementation of activities

		<p>company. It depends on the project area, so it is chosen individually. According to public sources, four projects are currently being piloted in Singapore's sandbox.</p> <p>In the post-Soviet area, Belarus became the first country to create a sandbox analog. In 2018, the Decree “On the Digital Economy Economy” was adopted there, according to which a special regime of the High-Tech Park was established. As part of it, the officials legalized the mining and circulation of cryptocurrencies. Thanks to this, the Park residents can freely engage in the creation of cryptocurrency exchanges, cryptocurrency trading, and other assets.</p> <p>In Russia, the Federal Law “On Experimental Legal Regimes in Digital Innovation in the Russian Federation” came into force in January 2021. It allows a zone in a particular region, in which an exemption from general legal regulation is provided. That is, in this territory, for three years, companies will be able to test their products without a license and without the risk of violating the existing law. If the innovation proves to be safe and effective, the experiment can be scaled up nationwide. As of January 2022, the experimental legal regimes have been approved for 5 projects: heavy unmanned transportation of goods in the Tomsk oblast (region), experiments related to unmanned taxis in certain cities, analysis of drugs efficiency based on big data, remote drug trade, delivery of goods up to 500 kg by drones. It is noted that preparation of the initial application for the creation of a “regulatory sandbox” requires a very large and serious preparation. Also, investors do not understand how they should act if three years of the “regulatory sandbox” expire, and amendments to the main legislation enshrining the successful “experimental” legal experience is not adopted.</p>
--	--	---

### Comments

As of April 2022, the KR existing legislation does not contain a special law or a direct indication in the laws of the admissibility of the “digital sand” application in the country, which would imply the establishment of an advanced experimental legal regime. Nevertheless, a minimal experience as an attempt to introduce a prototype of an experimental legal regime did take place.

In April 2020, amendments were made to the Kyrgyz Republic Law “On Innovation Activities” dated November 26, 1999, No. 128, which stipulated that the legal relations and conditions for testing innovative services/technologies in the banking, payment services under special regulatory regimes should be regulated by the Kyrgyz Republic Law "On the National Bank of the Kyrgyz Republic, Banks and Banking Activities" dated December 16, 2016, No. 206. In turn, this law was also supplemented by Chapter 11 “Special Regulatory Regimes”, providing that the National Bank has the right to establish for a certain period of time pilot the regulation within the special regulatory regime in order to test the legal regulation of social relations in the provision of banking, payment services related to the introduction of innovative services / technologies, on a particular or the entire territory of the Kyrgyz Republic. Special regulatory regime means a set of rules that allow participants engaged in the implementation of innovative services/technologies in the banking and payment services market, to test them in a limited controlled environment (by territory, time, number and volume of transactions and users, etc.). Such activity is aimed at accelerating the introduction of innovative banking operations and services into the market, and is based on a license. According to the Regulations “On Special Regulatory Regime” approved by Resolution of the KR National Bank dated August 12, 2020, No. 2020-P-12(45-3-(NPA), such license entitles its holder to a limited list of operations and services, which are fundamentally new, have not been applied previously or were limited, and are not regulated by normative legal acts and there is no direct prohibition and regulatory norms on them. According to the register of special regulatory regimes posted on the website<sup>50</sup> of the KR National Bank currently out of 3 of 4 issued are valid and one license was revoked.

In 2021, one of the Parliament members raised the fintech<sup>51</sup> issue. One of the main rationales for the law was the fact that today, not a single legal act provides for the development of the country's financial sector. The rationale statement of the law stated that “the goals and objectives set for the National Bank include stability, security, reliability, but not development”. At the same time, according to the developers, the reliability of such companies should be achieved by storing assets in the vault of the National Bank of Kyrgyzstan. The National Bank has the right to establish a pilot regulation of such companies for a certain period, on a particular or the whole territory of the Kyrgyz Republic. The bill caused considerable controversy and was eventually rejected by the Parliament Committee in October 2021. The main subject of heated debate was the provision allowing the fintech companies to open correspondent accounts in the National Bank. Thus, the National Bank would be transformed from the financial market regulator into its participant. This approach was opposed by the then chairman of the National Bank and some PMs. Finally, the bill was rejected, but the committee members appreciated the very attempts to establish experimental legal regimes, provided that the relevant legislative initiatives were strongly grounded and that the proposals contain convincing arguments for leveling the risks that accompany any attempts to introduce special or experimental legal regimes in the state. Such attempts, if insufficiently thought through, may not only create opportunities for abuse of a privileged position by individual participants in the civil-law relations, but also carry the key risks of harm to the population, in all good faith decisions and actions. Thus, the subsequent initiatives are still in a maturing stage.

Along with this, attempts are being made to introduce the digital sandboxes institution at the Eurasian Union level. Thus, the Supreme Eurasian Economic Council’s decision of October 11, 2017 No. 12 “On the Main Directions of Implementation of the Digital Agenda of the Eurasian Economic Union to 2025”<sup>52</sup> states that the regulatory sandbox is a special coordinated mode for the development and piloting of solutions, including the regulatory ones, to identify an effective model of interaction and building the business processes. In accordance with the Main Directions of Implementation of the Digital Agenda of the Eurasian Economic Union (hereinafter - EEU) to 2025, the “regulatory sandboxes” system is one of the priority development of initiatives and their application is declared as one of the mechanisms for the successful implementation of the EEU digital agenda. The expert platform for creation of the “regulatory sandboxes” system, which was attended by representatives of the business community,

---

<sup>50</sup> [www.nbkr.kg](http://www.nbkr.kg)

<sup>51</sup> <https://economist.kg/novosti/ekonomika/2021/09/23/skandalnyj-zakonoproekt-o-finteh-ili-pri-chem-tut-biznes-sestry-deputata/>

<sup>52</sup> <https://www.alta.ru/tamdoc/17vr0012/>

experts and specialists from state bodies of the EEU member states, research organizations and educational institutions of the Union member states, and experts from the functional blocks of the Commission, prepared report on the use of the “regulatory sandboxes” in the EEU and initiated a draft decree “On the development of a concept for the use of special regimes (the “regulatory sandboxes”) as part of the implementation of the digital agenda of the Eurasian Economic Union.” It describes the key challenges to implementing the digital agenda (including the limitations of the current process of developing initiatives and implementing projects), the goals, principles and proposed process of applying special regimes, the benefits for stakeholders and integration effects, provides an overview of alternative models with their advantages and disadvantages, and analyzes cases of possible application of “regulatory sandboxes”<sup>53</sup>. Currently, the Commission is striving to fulfill the assignment to develop, together with the EEU member states governments, a draft concept for the application of special regimes. No further details on the current status of this issue are available in the open sources.

Thus, the need to introduce special legal regimes in the Kyrgyz Republic is in a sense predetermined by the participation of the KR Cabinet of Ministers in the development of collective decisions in this area at the EEU level.

The experience of other countries already applying the experimental legal regimes in the digital sphere shows the continued distribution of regulatory sandboxes, which can be reduced to the following general definition:

Regulatory sandboxes, or experimental legal regimes, are applied in the area of innovation activities when general regulation of the relevant area is absent or creates obstacles in the implementation of innovative projects that may pose a threat to their implementation. Accordingly, the regulatory sandbox, first of all, makes it possible to fill, taking into account the needs of a rapidly developing digital economy, the legal regulation, which often lags behind the innovation sphere. In addition, the regulatory sandbox allows entrepreneurs to test new technologies on favorable legal terms. Regulatory sandboxing is a progressive and forward-looking regulation and is quite widely used in world practice. This tool is actively implemented in the United Kingdom, USA, Singapore, and Canada, among others. In 2021, the Federal Law “On Experimental Legal Regimes in Digital Innovation in the Russian Federation” dated July 31, 2020, N 258-FZ came into force in the Russian Federation with an essentially open list of areas and fields of activity where the digital sandbox can be applied. According to the generalizing publications, the Regulatory Sandbox is a special legal regime of regulation, development and piloting of solutions, including the regulatory ones, to identify the most effective model of interaction and building of business processes in any new area.

Regulatory “sandboxes” are appropriate for the development of mechanisms and rules for the regulation of economic processes within digital initiatives and projects. Conditionally regulatory “sandboxes” in world practice can be divided into two types: “fintech sandboxes” and universal “sandboxes”. The former work with digital innovations in the financial sector - new mechanisms for insurance, credit, financial counseling, crowdfunding, “digital” and “mobile” banks, microfinance activities. The latter in turn, target a broader range of digital innovations applied to the real economy - big data technologies, neurotechnology and artificial intelligence, distributed registry systems, quantum technologies, new manufacturing technologies, industrial Internet, robotics and sensorics components, wireless communication technologies, virtual and augmented reality technologies. Currently, the most common type is “fintech sandboxes”. This is explained both by the features of the regulation subject (the financial sector is traditionally the most “regulated” area of economy) and by the dynamics of financial technology development with significant marginality of fintech technologies.

Undoubtedly, there are specific conditions for the implementation of experimental legal regimes for countries with a developed legal system, established legal culture, and traditionally partnership-based relations between the regulatory authorities and business in comparison with developing countries, which objectively lag far behind in the development of state institutions designed to ensure fair

---

<sup>53</sup> <https://docs.cntd.ru/document/551782135>

regulatory policies and restrictions, and the weak participation of civil society institutions in ensuring public control over the reform processes.

One paper<sup>54</sup> summarizes the conclusions that regulatory capacity problems in developing countries have peculiarities.

When drafting the normative legal acts on the digital sandbox in Kyrgyzstan, it seems necessary to pay attention to the following features and risks that will accompany both the processes of development, consideration and adoption of the relevant drafts, and their subsequent implementation in practice.

1. Regulatory sandboxes can require time and skill level of regulators needed to determine testing plans and performance indicators, assess complex innovations and innovator challengers during individual assessments.

2. It is also necessary to identify resources to control the participants in their own sandbox. This will require additional staff and time commitments that regulators, especially in countries with limited resources such as Kyrgyzstan, may not have and may be otherwise occupied (or diverted) from other core responsibilities as a regulator. In some countries, regulatory agencies establish full-time staff dedicated to working with the sandbox. Forming a dedicated cross-functional team for sandboxes is especially difficult in developing countries, which have much less financial and human resources.

3. Sandboxes are designed to promote more open communication between regulators and innovators, which can produce mutually beneficial learning experiences. But regulators may simply not have the resources or the necessary expertise to understand and appreciate the complex nature of the innovation (especially given Kyrgyzstan's lower level of market sophistication) and stay abreast of its rapid pace and make changes. Ideally, regulators' actions should take into account the regulation goals while taking into account and respecting the legal boundaries. Regulators with insufficient capacity to fully understand and evaluate what may be a new, complex, breakthrough innovation may resist approval, evade choosing to protect against the risk of failure and personal impact by maintaining the status quo. At the other extreme, an overzealous program to encourage innovation can result in excessive deregulation with unnecessary risks introduced into the testing system, leading to possible failures. The ultimate success of the sandbox can be affected by a variety of unanticipated circumstances, which in doing so can undermine existing conditions and restrictions and damage the legal system.

4. While sandboxes have generated considerable interest and enthusiasm, they are only one of several approaches to regulation and are not always the best solution. Regulatory reform may be needed to eliminate regulatory inflexibility and incompatibilities that can hinder the effectiveness and success of the “sandbox”.

5. Smaller and less developed markets, i.e., the developing countries markets, often pose fundamental problems. These may include limited local resources (such as availability of capital and human resources), remoteness from resources and insufficient manpower reserves, limited infrastructure, and suboptimal market conditions.

6. The business operations of local sandboxes are also limited by internal boundaries and achieving sufficient economies of scale for long-term viability can be a challenge. Such risks reduce the attractiveness of innovation and opportunities for local and foreign direct investment. In addition, a structure and regulation that limits transactions to physical boundaries can stifle the creation of cross-border activity and the borderless nature of financial technology, which can provide necessary and profitable economies of scale.

7. There are also problems with limited transparency. Since the details of sandbox participation agreements are generally not made public and are often subject to confidentiality agreements, care should be taken not to provoke negative public opinion, in Kyrgyzstan, where there is a high level of corruption, especially. Participants admitted to the sandbox can benefit from a special status over others through the relaxed rules and communicating with the regulator. Certain candidates can be admitted to the sandbox through improper lobbying. The likelihood of such lobbying in the KR is extremely high.

---

<sup>54</sup> <https://deliverypdf.ssrn.com/delivery>

8. Risk mitigation should be sought: sandbox participants are responsible for managing their own affairs, such as ensuring sufficient funding, financial accounts with banks and financial institutions, and gaining access to data. These challenges can be difficult for innovators, including those who serve or work in Kyrgyzstan.

Thus, it is necessary to take into account the already, albeit little, practice in the KR banking sector on special regulatory regimes and the involvement of Kyrgyzstan in the development of solutions to prepare proposals for regulatory sandboxes on the EEU sites. We should also take into account the Decree of the KR President “On Measures to Develop Creative Economy and Create Conditions for Progressive Development of the Kyrgyz Republic” dated April 21, 2022, No. UP 123. According to it the Cabinet of Ministers approved the Concept for Development of Creative Economy in the Kyrgyz Republic for 2022-2026 (Resolution of the KR Cabinet of Ministers dated April 25, 2022, because its purpose is to create favorable conditions for the creative economy and to increase the contribution of creative industries to the domestic economy under a comprehensive state policy. According to the Concept, the creative industries sector in the country is designed to become an accelerator of entrepreneurial activity with high added value and high economic impact, and this will rationalize capital investments, expand export opportunities and provide employment growth. It should be assumed that efforts in this direction will inevitably bring the law of experimental legal regimes onto the agenda. According to the decree of the Head of the State and the executive branch, the creative economy should become in the future a stimulus for innovation, increase investment attractiveness and reduce the “dependence of the national economy on the mining sector and migrants’ remittances”.

However, when drafting specific normative legal acts, risks should be assessed with extreme caution and prudence, taking into account the specificity of the normative and legal system and the socio-economic realities of the Kyrgyz Republic.

## Section 33. Tax regulation

### Content

- effective tax policy as part of the Kyrgyz Republic's transition to the digital economy;
- modernization of the instrumental and methodological apparatus of the tax policy;
- synchronization of the legal tools used in the tax legislation.

### Current regulation (existing legislation):

1. Tax Code of the Kyrgyz Republic;
2. E-Commerce Law of the Kyrgyz Republic;
3. E-Government Law of the Kyrgyz Republic
4. Electronic Signature Law of the Kyrgyz Republic;
5. The Law of the Kyrgyz Republic “On Innovation Activities”;
6. Virtual Assets Law of the Kyrgyz Republic;
7. E-Commerce Law of the Kyrgyz Republic.

### Summary of the identified deficiencies and benchmarks from the global practice

No.	Description of the shortcoming	Type <sup>55</sup>	Best practice
33.1	The basic principles, specific tasks and urgent priorities of tax policy in the transition to the digital economy are not defined, nor are basic concepts such as “joint economy”, “digital platform”, etc. defined.	G	Globally there is no single codified legislation regulating the legal relations on the Internet, and there are absolutely objective problems of taxation of the digital economy (joint economy) subjects, which have not yet been solved. Taxation rules cannot keep pace with the digital business models development. Foreign IT giants, making money from users worldwide, pay profit tax only at the place of their HQ registration. As a result, countries not only lose tax revenues, but also violate the fair competition principles - national digital companies pay more taxes and, accordingly, work in less favorable conditions than foreign ones. Since 2015, the OECD has been trying to find a unified international approach and solve the problem of unfair tax distribution of IT giants. It has not yet been possible to develop a mechanism that would be acceptable for all countries. The main difficulty is how to calculate which share of the profits of a multinational corporation goes to one country or another. Only the corporations themselves know how much profit users in a particular country generate, but they do not disclose detailed information.

<sup>55</sup> The following types of regulatory deficiencies are listed in the table:

- (G) regulatory gap (regulation is required, but it is missing)
- (O) obsolete provision (the existing provision should be changed)
- (N) non-working provision (the existing provision is non-working for the reasons described)
- (B) this provision is an unreasonable barrier to the implementation of activities

33.2	Under the “digital tax” there are no criteria (not only domain name and IP-address) for the formation of a permanent establishment of a foreign Internet company in order to establish the obligation of tax registration and income taxation in the Kyrgyz Republic.	G	<p>In the BEPS Final Report dated October 5, 2015, the OECD discussed three measures that could improve the e-commerce taxation:</p> <ul style="list-style-type: none"> <li>- accounting communication based on the concept of a significant economic presence within the jurisdiction indicating the tax payment location;</li> <li>- digital transaction tax;</li> <li>- equalization levy, which involves taxing the turnover (not profits) of companies in the digital economy.</li> </ul> <p>Without waiting for the OECD global consensus, a number of states, including the UK, France, Italy, and Turkey, have unilaterally introduced their own digital taxes and established their own taxation practices, allowing them to charge VAT or tax on goods and services delivered directly to consumers in their territory for online advertising and digital intermediation services.</p> <p>Pursuing their own interest in collecting taxes, the European countries moved from the principle of origin to the principle of destination and aligned their tax conditions with this principle. Further, they established a threshold for the sales amount, at which the seller is taxed in the destination country.</p> <p>France became the first European country to announce a digital tax in 2019, which includes cloud services. Payments at 3% are made by digital companies with total revenues worldwide of €750 mln, more than €25 mln of which came from the French users. The tax applies to the income that technology giants earn in the country.</p>
33.3	The terms related to the taxation objects in the digital economy, such as “mining” or “virtual asset” are not clearly defined, which will result in difficulties in applying the digital tax provisions in practice.	N	This problem needs to be addressed as part of the glossary, since the terms mentioned are not only relevant for taxation purposes.
33.4	Different approaches to the application of value-added tax on international telecommunication services, established by the ITU and the EEU Agreement, allow concluding that there is a legal discrepancy between the approaches to	B	The International Telecommunication Regulations, in Article “Tariffing and Settlement” (paragraph 6.3.1), establish the rule “If the national legislation of any country provides for a tax on the charging fees for the international

charging VAT for international communication services, which should be resolved in accordance with international law and be reflected in the legislation of the Kyrgyz Republic, for the clarity purposes.

telecommunication services, and such tax is imposed only on those international services that paid for by customers of that country, unless other agreements are concluded for specific special cases”. The established global practice interprets this rule as the impossibility of applying value-added tax in the Kyrgyz Republic for international telecommunication services, such as roaming services, interconnection and international transit traffic services, in settlements between operators, since such services are paid by customers of a foreign telecommunications operator ordering such services. The Regional Commonwealth of Communications Commission by its Decision dated March 19-20, 2009, No. 23/10 recommended that the communications administrations and telecommunication operators of the RCC member countries to be guided by clarification of the RCC Executive Committee to the international rules on exemption of communication administrations (operators) from value-added tax in mutual settlements with administrations (operators) of other countries for international communication services provided.

The clarification refers to the International Telecommunication Regulations. It is pointed out that in CIS countries, the value-added tax is paid by customers when using international communication services, but cannot be paid by telecom operators of other countries when making mutual settlements with them. It is proposed that telecommunications operators of the RCC member countries make mutual settlements with each other and with telecommunications operators of non-CIS countries for international communication services without charging value-added tax.

However, as the practice has shown, the provisions of the Regulations of the International Telecommunication Union for charging the value-added tax and implementation at the legislative level of

		<p>the RCC Commission recommendations, are not reflected in the tax legislation of the Kyrgyz Republic as special norms. Telecom operator services provided to a foreign telecom operator shall be subject to value-added tax at the place of provision of such services (place of sale of the services).</p> <p>Protocol 18 to the EEU Agreement, the place of sale of communication services and, accordingly, the place of VAT payment, determined the territory of a member state if the services are provided by the taxpayer of this member state.</p> <p>Administrative Regulations of the International Telecommunication Union, provides for the VAT collection in the country in which services are paid for by the consumer (subscriber), in other words, at the place of payment for services.</p>
--	--	--

### Comments

Economic transformation is characterized by widespread processes of implementing the information and production technologies in business entities: the use of cloud storage, transition to digital money, implementation of biometric authentication systems, and use of artificial intelligence functions. The tax system is an integral part of this picture, stimulating the introduction of digital technologies in the interaction between tax authorities and taxpayers. Informatization of technological and production processes is becoming most in meeting the needs of both citizens and state authorities. Accelerated development and the global digitalization process generate new opportunities for the state budget, which are still at the stage of comprehension and formation in the Kyrgyz Republic.

At the state level, the principles of taxation in the field of Internet economy and e-commerce have not yet been defined. Therefore, the reforms and harmonization of tax legislation through the widespread introduction of new taxation tools, including the development of digital business tax architecture, are urgently needed and should be implemented as soon as possible, based on the already established international practice and the OECD recommendations.

Despite the new taxation tools introduced on January 1, 2022, the government still faces two major challenges in improving the tax administration practices:

- modernization of the instrumental and methodological apparatus of the existing tax policy, and
- introduction of digital technologies and digital platforms into the economy.

Measures required for the implementation of these tasks include:

- creating a digital identification system, including at the international level;
- application of tools for interaction with taxpayers, embedded in the natural environment and nationwide services;
- improving the data management standards, ensuring the availability of information necessary for administration;
- implementation and development of the automated algorithms for calculating tax liabilities, with the implementation of the function of preliminary notifying the taxpayer;

- application of artificial intelligence and predictive analytics for tax administration, development of new competencies of tax officers;
- building a convenient mechanism for international interaction between tax administrations.

From January 1, 2022, the tax legislation introduced electronic tax reporting and social insurance reporting, labeling of goods for their traceability, and established special tax regimes: “mining tax”, “tax on e-commerce activities” and “tax regime in the High Tech Park”, and established special terms - “Electronic service”, “Mining”, “Virtual asset”, expanded the concepts of “Permanent establishment” and “Place of service”, and determining conditions for tax registration of foreign legal entities.

It should be noted that there is no unified codified legislation regulating the legal relations on the Internet, and there are absolutely objective problems with the taxation of the digital economy subjects (shared economy), which have not yet been solved. Taxation rules cannot keep pace with digital business model development. Foreign IT giants, making money from users around the world, pay profit tax only at the place of their HQ registration. As a result, countries not only lose tax revenues, but also violate the fair competition principles - national digital companies pay more taxes and, accordingly, work in less favorable conditions than foreign ones. Since 2015, the OECD has been trying to find a unified international approach and solve the problem of unfair tax distribution of IT giants. It has not yet been possible to develop a mechanism that would be acceptable for all countries. The main difficulty is how to calculate which share of the profits of a multinational corporation goes to one country or another. Only the corporations themselves know how much profit users in a particular country generate, but they do not disclose detailed information.

Marketplaces are the most popular business model in e-commerce. While it does not own the goods, it provides the technology and infrastructure for online commerce (the “digital platform”) to goods owners - manufacturers, distributors, and retailers. Today, the largest marketplaces in the world are Alibaba, JD.com, Amazon, and Pinduoduo.

Effective taxation of sellers who use digital platforms in their economic activities, i.e., individuals who sell goods or services through digital platforms, is a common challenge for many tax administrations in light of their continued rapid growth. Two key principles of the platform business - the service product format and flexible payment format - provide positive and productive experience for many consumers, but have proven to be virtually beyond the reach of tax administration. Until January 1, 2022, there was rapid growth of e-commerce trade in Kyrgyzstan without any serious government regulation, in particular the “digital tax”, which was successfully introduced in 130 countries that have joined the OECD global digital tax pact.

In the BEPS Final Report dated October 5, 2015, the OECD discussed three measures that could improve the e-commerce taxation:

- accounting communication based on the concept of a significant economic presence within the jurisdiction indicating the tax payment location;
- digital transaction tax;
- equalization levy, which involves taxing the turnover (not profits) of companies in the digital economy.

Without waiting for the OECD global consensus, a number of states, including the UK, France, Italy, and Turkey have unilaterally introduced their own digital taxes and established their own taxation practices, allowing them to charge VAT or tax on goods and services delivered directly to consumers in their territory for online advertising and digital intermediation services.

Pursuing their own interest in collecting taxes, the European countries moved from the principle of origin to the principle of destination and aligned their tax conditions with this principle. Further, they established a threshold for the sales amount, at which the seller is taxed in the destination country.

France became the first European country to announce a digital tax in 2019, which includes cloud services. Payments at 3% are made by digital companies with total revenues worldwide of €750 mln, more than €25 mln of which came from the French users. The tax applies to the income that technology

giants earn in the country. The digital tax affected about 30 global corporations, including Google, Amazon and Facebook. The taxation object is “the provision of digital interface that allows users to come into contact and interact with each other, involving the delivery of goods or services directly between such users” and “the placement of targeted advertising messages in the digital interface, taking into account the users data received when they use the digital interface.” France is considered to be the sale place if the user devices involved in the digital services are located in France. In this case, the tax base is the income from the sale of digital services (excluding VAT). The amount of revenue is defined as the proportion of the company's total revenue from the relevant service proportional to the volume of deliveries to users in France, or the number of accounts in France, or the number of ad views in France, or the number of French users whose data has been processed, in the total volume of these transactions.

Turkey began levying a digital tax at a rate of 7.5%, on March 1, 2020.

The UK began levying a digital tax on the technology giants' revenue at a rate of 2%, from April 2020.

In January 2020, Italy imposed a 3% tax on digital service providers (including cloud services) that generate more than \$831 mln in revenue worldwide and at least \$6 mln in Italy.

Spain has imposed a 3% tax on foreign IT companies with global revenues of more than 750 mln Euros per year and more than 3 mln Euros in Spain.

In 2019, the Czech government approved the introduction of a 7% digital tax. It was imposed on large international companies with a turnover of 750 mln Euros in the world and 100 mln crowns (3.91 mln Euros) in the Czech Republic, and on a user audience of over 200 thousand people. Facebook and Google are among them. The new tax is levied on income from sales of targeted advertising on digital platforms, and the user data. The initiative applies to services provided to Czech users.

Brazil launched a similar initiative in 2020, where a law was submitted to the House of Representatives to create a digital tax on legal entities registered in Brazil or abroad, and members of international groups whose income in the previous year exceeds 3 billion Brazilian reals (\$600 mln). In addition, taxpayers should have gross income in Brazil in excess of 100 mln Brazilian reals (\$20 mln). The tax rate is differentiated from the gross income from 1% to 5%.

The procedure for establishing a digital tax has been implemented in some countries in Asia and Latin America, and in post-Soviet countries, which have delegated charging VAT (Goods and Services Tax) on all purchases (for all paid content purchased by users) made by users in the Google Play Market to local and/or foreign developers, setting the applicable tax rates. This practice applies to Australia, Bahrain, Belarus, India, Chile, Japan, Saudi Arabia, Russia, South Korea, New Zealand, Singapore, Indonesia, Kazakhstan, etc.

Since 2016, India has imposed a 6% levy on foreign companies' B2B digital advertising revenue.

In 2020, Thailand approved a bill requiring foreign providers of cloud and other digital services to pay 7% VAT on sales. The law requires non-resident companies or digital platforms that earn more than 1.8 mln baht (\$82, 831) a year from providing digital services to pay VAT.

In May 2020, Indonesia adopted a law requiring large Internet companies to pay VAT on sales of digital products and services, and in the Philippines, a legislator submitted a similar bill in parliament, to tax digital services.

On January 1, 2020, Google will begin charging a 6% tax on its cloud and other digital services in Malaysia. The service tax amount will be charged on the purchase and will appear on a separate line in transactions under Bills & Payments.

From April 2020, Google began paying taxes for online services in Uzbekistan. The country's tax code has been amended to include a “Google tax” on companies that provide digital services. The tax obliges foreign companies providing paid services to Internet users in Uzbekistan to pay 15% VAT. The Tax Committee created a special online resource - the VAT office, at tax.uz, to register foreign Internet companies in Uzbekistan. According to the innovations, foreign legal entities selling services and goods electronically, which sale place in Uzbekistan, are recognized as taxpayers of such services rendered to individuals.

On January 1, 2022, Kazakhstan officially introduced into the Tax Code the 25th section called "Characteristics of taxation of foreign companies in carrying out electronic commerce in goods, and

delivering e-services to individuals”. Since January 1, 2022, foreign Internet companies operating in Kazakhstan without establishing a legal entity will have a tax obligation to pay VAT at a rate of 12%, when they engage in e-commerce in goods or deliver e-services to individuals - customers. It is expected that the potential digital taxpayers will be major technology companies such as Facebook, Amazon, Apple, Netflix, Alibaba and Google, for which there are a number of facilitated procedures for tax registration in the form of conditional registration as a VAT payer. It is sufficient to send a letter of confirmation by mail to the tax authority of Kazakhstan on paper. Tax is paid without issuing electronic invoices. Filing tax reports is not stipulated. Opening of settlement accounts in banks of the Republic of Kazakhstan is not required, as the foreign company pays tax from its settlement bank accounts abroad.

All countries that have enacted digital tax laws have provided special methodologies for determining the portion of gross income subject to taxation in their country, as well as special tax registration procedures. Depending on the underlying tax regime and the nature of the payments, withholding can range from a simple system with a universal set rate, to a more complex system that takes into account broader circumstances.

**The main problems** faced by countries that have enacted an Internet tax at the legislative level include:

- a. lack of appropriate (generally applicable) terminology in the law;
- b. inability to comprehensively implement controls on profits derived from electronic commerce (especially those conducted through anonymous payment systems), making digital tax evasion seem limitless;
- c. predominance of intangible assets over tangible assets and their transnational mobility create additional barriers;
- d. issues of revising the national tax doctrines and double taxation avoidance agreements to balance the source with the tax at the company's place of incorporation have not been resolved;
- e. lack of information on the number of digital assets and services provided by foreign IT companies.

Realizing its need for effective taxation of e-commerce, the Kyrgyz Republic proposed its own model of digital tax application from January 01, 2022, which was to take into account the existing positive experience and allow resolving the above-mentioned problems. However, this decision has some shortcomings, in particular:

- under the “digital tax” there are no criteria (not only domain name and IP-address) for the formation of a permanent establishment of a foreign Internet company in order to establish the obligation of tax registration and income taxation in the Kyrgyz Republic;
- The terms related to the taxation objects in the digital economy, such as "mining" or "virtual asset" are not clearly defined, which will result in difficulties in applying the digital tax provisions in practice.

These problems go beyond the tax legislation itself and need to be addressed in the process of defining the boundaries of sovereignty of the Kyrgyz Republic in cyberspace and compiling a glossary, because the terms listed are important not only for tax purposes.

In addition, there are tax discrepancies in the field of taxation of international telecommunications services. Different approaches to the application of value-added tax on international telecommunication services, established by the ITU and the EEU Agreement, allow concluding that there is a legal discrepancy between the approaches to charging VAT for international communication services, which should be resolved in accordance with international law and be reflected in the legislation of the Kyrgyz Republic, for the clarity purposes.

The International Telecommunication Regulations, in Article “Tariffing and Settlement” (paragraph 6.3.1), establish the rule “If the national legislation of any country provides for a tax on the charging fees for the international telecommunication services, and such tax is imposed only on those international services that paid for by customers of that country, unless other agreements are concluded for specific special cases”. The established global practice interprets this rule as the impossibility of applying value-added tax in the Kyrgyz Republic for international telecommunication services, such as roaming services, interconnection and international transit traffic services, in settlements between

operators, since such services are paid by customers of a foreign telecommunications operator ordering such services. The Regional Commonwealth of Communications Commission by its Decision dated March 19-20, 2009, No. 23/10 recommended that the communications administrations and telecommunication operators of the RCC member countries to be guided by clarification of the RCC Executive Committee to the international rules on exemption of communication administrations (operators) from value-added tax in mutual settlements with administrations (operators) of other countries for international communication services provided.

The clarification refers to the International Telecommunication Regulations. It is pointed out that in CIS countries, the value-added tax is paid by customers when using international communication services, but cannot be paid by telecom operators of other countries when making mutual settlements with them. It is proposed that telecommunications operators of the RCC member countries make mutual settlements with each other and with telecommunications operators of non-CIS countries for international communication services without charging value-added tax.

However, as the practice has shown, the provisions of the Regulations of the International Telecommunication Union for charging the value-added tax and implementation at the legislative level of the RCC Commission recommendations, are not reflected in the tax legislation of the Kyrgyz Republic as special norms. Telecom operator services provided to a foreign telecom operator shall be subject to value-added tax at the place of provision of such services (place of sale of the services).

Protocol 18 to the EEU Agreement, the place of sale of communication services and, accordingly, the place of VAT payment, determined the territory of a member state if the services are provided by the taxpayer of this member state. Administrative Regulations of the International Telecommunication Union, provide for the VAT collection in the country in which services are paid for by the consumer (subscriber), in other words, at the place of payment for services.

## Section 34. Customs regulation

### Content

- issues of customs clearance and control using digital means,  
customs control of intellectual property

### Current regulation (existing legislation):

1. Treaty on the Customs Code of the Eurasian Economic Union dated April 11, 2017.
2. Customs Code of the Eurasian Economic Union (Annex No. 1 to the Treaty on the Customs Code of the Eurasian Economic Union dated April 11, 2017).
3. Customs Regulation Law of the Kyrgyz Republic dated April 24, 2019, p 52
4. Tax Code of the Kyrgyz Republic dated January 18, 2022, No. 3.
5. Law “On State Regulation of Foreign Trade Activities in the Kyrgyz Republic” dated July 2, 1997, No. 41.
6. Law of the Kyrgyz Republic “On Export Control” dated January 23, 2003, No. 30.
7. Law of the Kyrgyz Republic "On Trademarks, Service Marks and Appellations of Origin of Goods" dated January 14, 1998, No. 7.
8. Law “On the Customs Tariff of the Kyrgyz Republic” dated December 30, 2014, No. 173.
9. Resolution of the KR Government “On Some Issues of Customs Affairs” dated February 13, 2020, No 79.
10. Resolution of the KR Government “On Approval of the Regulations on the Procedure of Customs Control of Goods Containing Intellectual Property Objects” dated November 27, 2000, No. 694.
11. Resolution of the KR Government “On Measures to Introduce a National Export Control System in the Kyrgyz Republic” dated May 4, 2004, No. 330.
12. Resolution of the Kyrgyz Republic Government “On Approval of the National Control List of Controlled Products of the Kyrgyz Republic” dated April 2, 2014, No. 197.
13. Resolution of KR Government “On Measures to Implement the Requirements of the Law of the Kyrgyz Republic “On Customs Regulation in the Kyrgyz Republic” dated August 6, 2015, No. 563.
14. Resolution of the KR Government “On Measures to Implement the Requirements of Articles 95, 101, 102, 105, 128, 135, 148, 153, 157, 158, 163, 176, 180, 213, 229, 232 of the Law of the Kyrgyz Republic “On Customs Regulation in the Kyrgyz Republic”, dated August 10, 2015, No. 564 .
15. Resolution of the KR Government “On Reorganization of the State Enterprise “Customs Infrastructure” under the State Customs Service under the Kyrgyz Republic Government” dated June 23, 2016, No. 353.

Brief description of the identified shortcomings and international practice benchmarks

No.	Description of the shortcoming	Type <sup>56</sup>	Best practice
34.1	Incomplete use of the potential of the institution of electronic preliminary information.	G	<p>The World Customs Organization (WCO) considers the use of advance information to be an indicator of a high level of customs development. The International Convention on the Simplification and Harmonization of Customs Procedures (Kyoto Convention) stipulates the need to use advance information when developing customs procedures and to ensure that it is transmitted electronically.</p> <p>Along with other mechanisms and tools, the advance information and advance declaration is the basis for the implementation of the Framework Standards of Trade Security and Facilitation, and the implementation of Integrated Supply Chain Management Guidelines (WCO, June 2004).</p> <p>Advance notice is actively developing in the face of the danger of international terrorism growth. In particular, a number of governments have adopted regulations and entered into agreements with the business community to ensure the necessary level of security based on the results of risk assessments conducted prior to the arrival of goods in the customs territory: Canada Customs' Partners in Protection (PIP) program, Australia Customs' Front Line and Accredited Customer program, USA Customs' C-TPAT program, New Zealand Customs' SEP and FrontLine program</p> <p>Chapter 6 "Customs Control" of the Guidelines to the General Annex of the International Convention on the Simplification and Harmonization of Customs Procedures (Kyoto Convention):</p> <p>Customs administrations should develop customs procedures for the implementation of customs control methods to ensure uniform application throughout the customs territory. In developing these procedures, the customs administration should shift its focus from the executive application of customs movement controls to the customs controls based on audits, taking into account the following:</p> <ul style="list-style-type: none"> <li>• reducing the delay time during the movement of goods/persons,</li> </ul>

<sup>56</sup> The following types of regulatory deficiencies are listed in the table:

- (G) regulatory gap (regulation is required, but it is missing)
- (O) obsolete provision (the existing provision should be changed)
- (N) non-working provision (the existing provision is non-working for the reasons described)
- (B) this provision is an unreasonable barrier to the implementation of activities

			<ul style="list-style-type: none"> <li>• increasing use of periodic filing of customs declarations,</li> <li>• encouraging the trader to hold self-assessment,</li> <li>• enabling traders (not the customs authority) to delay providing the supporting official and commercial documents,</li> <li>• increasing the use of advance information and its electronic transmission,</li> <li>• increasing the use of the commercial system of traders and accounting instead of the need to store customs documents</li> <li>• encouraging compliance with customs legislation by sharing more and more responsibility with the trade community while partnering with the customs authority to reduce risk.</li> </ul> <p>To optimize the use of advance methods of customs control, the use of automation is recommended.</p> <p>The customs administration should use on-site analysis and consider mechanisms to ensure the effectiveness of customs control procedures applied throughout the customs territory. Procedures can be revised and adjusted as needed to meet certain requirements.</p>
34.2	Multiple controls and duplication of state controls at the border	G	<p>“Customs control” is defined in the World Customs Organization's Glossary of Customs Terms as “measures applied to ensure compliance with laws and regulations, the enforcement of which is entrusted to the customs authorities.” To ensure the proper application of customs laws and regulations, it is essential that all international movements be declared for processing or use that are authorized by the customs authority.</p> <p>To fulfill the obligations of collecting public revenue, implementing trade policies and protecting the population, while regulating the increase in international trade and tourism, which manifests itself together with the reduction of the customs staff, and to facilitate trade by strengthening the law compliance of traders, travelers and carriers, the customs administration should apply customs control methods effectively and efficiently by implementing risk management methods. Continuous review of these controls to ensure that they are continually updated will help the customs administration perform these complex tasks despite the strong influence of intense international trade development and continuous changes in the trade and transport system. Social problems cause at least equally</p>

			<p>important changes in customs control requirements. Promoting legitimate trade in the risk management process plays a very important role. A memorandum of understanding with individual companies (as recommended in the World Customs Organization ACTION /DEFIS program) can formalize such cooperation as customs-trade.</p> <p>There are many ways to respond to such changes by raising the level of facilitation and customs control following the best customs practices. One way to combine the facilitation and customs controls measures is to use a single competent unit to perform a wide range of tasks, such as phytosanitary, veterinary or dangerous goods control, currently performed by different agencies, possibly located in different places. Customs authorities, already existing at all borders and with extensive experience in the operational fulfillment of the international trade and transport requirements, provide logical and economically sound consideration to fulfilling such duties.</p> <p>One of the solutions for rational and optimal construction of the border crossing process is the application of the "Single Window" principle. The most common definition of "Single Window" is found in UNECE Recommendation No. 33. According to this definition, an SW is "a facility that allows parties involved in trade and transport to lodge standardized information and documents with a single entry point to fulfill all import, export, and transit-related regulatory requirements. If information is electronic, then individual data elements should only be submitted once."</p> <p>A single window is created for the exchange of information between traders and government agencies, and among government agencies themselves on procedures related to foreign trade, such as obtaining relevant permits, licenses, certificates and approvals, passing through customs clearance and release from the port.</p> <p>The Single Window system allows traders to submit foreign trade information once in one place and provides for more efficient and faster processing of information if it is submitted electronically.</p>
34.3	Simplification and optimization of goods delivery control	G, O	<p><b>In the Republic of Azerbaijan</b>, when importing goods from the external border to the internal customs authorities, only customs operations on primary registration of goods and vehicles at the</p>

			<p>border crossing points are applied, without customs declaration and placement under the transit customs procedure.</p> <p>In this case, goods are delivered to the internal customs authorities with the use of GPS locks and navigation seals.</p> <p>As a result, in the Republic of Azerbaijan, the average time to pass through the BCPs is 15-20 minutes, since there is no need to form documents. It should be noted that the information system (Unified Automated Management System) of the State Customs Committee of the Republic of Azerbaijan is considered one of the most successful models of customs administration, according to the world community.</p> <p>The World Customs Organization (WCO) recommends this system as the “best practice” platform.</p>
34.4	Implementation of the national authorized economic operators system	B	<p>As defined <a href="#">in the WCO SAFE Framework of Standards</a>, an Authorized Economic Operator (AEO) is a party involved in the international movement of goods in whatever function that has been approved by or on behalf of a national Customs administration as complying with WCO or equivalent supply chain security standards. AEOs may include manufacturers, importers, exporters, brokers, carriers, consolidators, intermediaries, ports, airports, terminal operators, integrated operators, warehouses, distributors and freight forwarders.</p> <p>For many years, and in some cases as far back as the 1970s, customs has been carefully focusing on security in the international supply chain, with a number of special programs developed more recently for this purpose, aimed at strengthening trade security globally. The AEO concept is part of these programs, and in 2005, the WCO developed a separate standard for AEOs, the WCO SAFE Framework of Standards. Since then, traders have to make much effort to achieve AEO status in certain cases, but even after becoming an AEO, trade organization should continuously maintain it. At the same time, customs authorities often do not provide AEO holders with any significant benefits in terms of trade facilitation, which, naturally, increases trade costs. Therefore, the AEO programs are implemented in the world quite slowly.</p> <p>Under the AEO program, customs authorities should provide a number of benefits to</p>

			<p>organizations that have received this status, and all work should be performed in close cooperation with trade representatives. Standard 6 of Section II of the WCO SAFE Framework of Standards encourages cooperation between customs and traders to ensure the highest level of security and simplicity. However, this standard prioritizes safety over simplicity, which creates a dilemma. Therefore, the WCO has developed specific AEO Guidelines (outlined in Chapter 5 of the WCO Safety Standards Framework), as well as an AEO Benefits Plan drafted by private sector efforts. These benefits include reduced inspections and priority inspections, mutual recognition of foreign AEO programs, relaxed security and safeguards requirements for expedited release of goods, and pre-clearance, simplified procedures, priority service for emergencies, etc.</p>
<b>34.5</b>	On the need to develop technologies for simplified, accelerated operations for certain categories of goods	<b>G</b>	<p>It is recommended to develop and approve in the Kyrgyz Republic the customs operations technologies for certain categories of goods requiring special transportation conditions, such as perishable products, which would provide a standardized and simplified procedure for their border crossing and customs clearance. In particular, Article 7.9 of the Trade Facilitation Agreement of the World Trade Organization states that, during clearance and inspection, WTO members must ensure priority for perishable goods and allow the transportation and storage of perishable goods in approved storage facilities (public or private), as well as provide the opportunity to clear in the same storage facilities.</p>
<b>34.6</b>	Making a preliminary decision on the methods for determining the customs value of imported goods	<b>G</b>	<p>The General Agreement on Tariffs and Trade 1994 (GATT 1994) is a multilateral interstate agreement that is central to the legal regulation of international trade in goods. The national trade and political systems of the GATT member states and now the WTO have contributed to forming a uniform legal framework for global trade. Article VII, “Valuation for Customs Purposes”, of this Agreement, defines the general principles of valuation and requires that these principles be applied to all products subject to duties or other charges or restrictions on importation and exportation based upon or regulated in any manner by value. At the same time, Article 22 of the Agreement on the Implementation of Article VII of the General Agreement on Tariffs and Trade 1994 states that each member shall ensure, not later than the date of application of the provisions of this Agreement</p>

			for it, the conformity of its laws, regulations and administrative procedures with the provisions of this Agreement.
--	--	--	--

### Comments

According to Article 11 of the Customs Code of the Eurasian Economic Union, a participant in foreign economic activity has an obligation to provide preliminary information on the goods planned to be moved across the customs border of the Union, vehicles for international transportation carrying such goods, time and place of arrival of goods in the customs territory of the Union, passengers arriving in the customs territory of the Union, prior to the actual arrival at the EEU customs border.

In case of failure to present preliminary information which must be submitted on a mandatory basis, or in case of failure to comply with the time period for its presentation, the measures shall apply established in accordance with the legislation of the Member State on customs regulation to whose customs authority such preliminary information must be presented.

The legislation of member states may provide for liability for failure to present preliminary information to the customs authorities or failure to comply with the time period for the presentation thereof.

However, the Kyrgyz Republic legislation does not provide for the application of liability for failure to provide preliminary information or failure to comply with the timer period for its presentation.

Thus, the potential of the preliminary information is not properly used, because even though the EEU law obliges participants of foreign economic activities to provide preliminary information, **the KR national legislation does not set forth liability both for failure to submit preliminary information in general, and for failure to comply with the time period for its presentation.**

According to the Resolution of the Kyrgyz Republic Government "On Measures to Streamline the Functioning of Checkpoints Across the State border of the Kyrgyz Republic, intended for International Road, Air and Rail Traffic, and Internal Stationary Posts on the Roads of the Kyrgyz Republic" dated November 19, 2007 No. 556, at checkpoints across the state border of the Kyrgyz Republic, the following types of state control are carried out:

- border;
- radiation control;
- sanitary and quarantine control;
- veterinary control (surveillance);
- quarantine phytosanitary control (surveillance);
- transport (automobile) control;
- customs control.

In its turn, the sequence of actions when carrying out border, customs and other controls at automobile checkpoints across the EEU customs border in the Kyrgyz Republic is determined by the Procedure of interaction of authorized state bodies of the Kyrgyz Republic at automobile checkpoints across the customs border of the Eurasian Economic Union in the Kyrgyz Republic (hereinafter - the Procedure), approved by Resolution of the Kyrgyz Republic Government dated November 19, 2020.

In particular, chapters 3, 4, 5, and 6 of the Procedure describe the sequence of control actions by the state authorities upon arrival/departure of various categories of goods and vehicles.

At the same time, each type of state control provides for the same control actions, which are often duplicated.

**In this regard, it is proposed to revise** this Procedure, in order to eliminate the duplication of control forms and methods through the introduction of a single interagency information system.

Currently, when goods are moved from entry points into the EEU customs territory in the Kyrgyz Republic, regardless of the delivery point, the Kyrgyz Republic customs authorities apply the customs procedure of customs transit to control the delivery of goods.

Moreover, the customs transit procedure also applies when goods are delivered under customs control from an internal customs authority both to another internal customs authority and to the point of departure from the EEU customs territory in the Kyrgyz Republic.

At the same time, it should be noted that, according to the EEU Customs Code, to place goods under the customs transit procedure, it is necessary to comply with the conditions of placement of goods under this procedure.

Thus, under paragraph 1 of Art. 142 of the Customs Code, the customs procedure for transit is a customs procedure when the goods are transported (shipped) from the customs authority of departure to the customs authority of destination without payment of customs duties and taxes, safeguard, anti-dumping and countervailing duties, provided that the terms and conditions of the placement of those goods under this customs procedure were complied with.

The terms of placement of goods under the customs procedure for transit are in turn described in Article 143 of the EEU Customs Code:

“1) ensuring the fulfillment of obligation for payment of import customs duties and taxes in accordance with Article 146 of this Code for foreign goods;

2) ensuring the fulfillment of obligation for payment of safeguard, anti-dumping, countervailing duties in accordance with Article 146 of this Code for foreign goods in cases stipulated by the Commission;

3) facilitation of identification of the goods by the methods stipulated by Article 341 of this Code;

4) compliance conformity of a vehicle for international transportation with the requirements specified in Article 364 of this Code, provided that the goods are transported in cargo holds (compartments) of a vehicle with the customs seals and stamp attached to them;

5) compliance with prohibitions and restrictions in accordance with Article 7 of this Code.

In addition, there are a number of features when placing certain categories of goods, such as goods for personal use, international mail, goods transported by pipeline, etc., under the customs transit procedure.

However, in accordance with paragraph 10 of Article 142 of the Customs Code of the EEU, the features of application of the customs procedure for transit to the goods transported within the territory of one Member State only may be stipulated by the customs legislation of that State.

It should be noted that in the national legislation the features of the customs procedure for transit are regulated by the Instruction on features of customs operations when placing goods under the customs procedure for transit, approved by the Kyrgyz Government Resolution On measures to implement the requirements of Articles 95, 101, 102, 105, 128, 135, 148, 153, 157, 158, 158, 163, 176, 180, 213, 229, 232 of the Kyrgyz Republic Law “On Customs Regulation in the Kyrgyz Republic” dated August 10, 2015, No. 564 (hereinafter - Instruction).

This Instruction was adopted in implementing the Kyrgyz Republic Law “On Customs Regulation in the Kyrgyz Republic” dated December 31, 2014 No. 184, which became void with the adoption of the current Kyrgyz Republic Law “On Customs Regulation” dated April 24, 2019 No. 52.

At the same time, the Instruction does not establish specifics for the application of customs transit, but only determines the procedure for customs operations on the submission, registration of the transit declaration and completion of the customs procedure for transit in the Kyrgyz Republic.

At the same time, the customs legislation of the Kyrgyz Republic does not use the potential of applying the features of the customs procedure for transit in order to simplify and optimize customs processes.

In particular, when transporting goods under customs control for short distances, the customs authorities are forced to apply the customs transit procedure, while requiring mandatory compliance with all conditions and provisions established by the EEU Customs Code, regardless of whether they are redundant or not.

**In this regard, it is recommended** to develop a simplified mechanism for controlling the delivery of goods under customs control within the Kyrgyz Republic, including the development of new instructions related to the regulation of features of the customs transit procedure in the Kyrgyz Republic.

With the adoption of the EEU Customs Code and adoption of the revised law “On Customs Regulation” in January 2018, the Authorized Economic Operator (AEO) program in the Kyrgyz Republic began to be implemented. As such, it is still in the early stages of development and an awareness campaign should be organized to raise general awareness of the opportunities and benefits among the trading community.

One of the criteria for obtaining the AEO status under the EEU Code is the placement of a guarantee of at least 1 mln, 700,000 and 500,000 euros, depending on the three different types of certificates. For many local companies, this amount is a too high threshold. There is a need to explore other options regulated by own national legislation to provide trade facilitation measures for local companies by establishing more reasonable and appropriate criteria.

While there is currently only one company with AEO status, as they understand the benefits of this status and their number grows, it is necessary to ensure that a system of validation/verification, compliance monitoring and other commitment criteria is in place. An official decision-making body is also needed in terms of granting, revoking, and reinstating AEO status, as well as to ensure that AEOs are properly accorded the benefits of facilitation. **It is recommended that the SCS explore a more inclusive structure outside of the EEO program with more realistic and achievable criteria for local companies with high levels of compliance.**

Art. 81 of the EEU Customs Code provides for a special priority procedure for customs operations in respect of the goods required for mitigation of impact of natural disasters and natural and man-made emergency situations, the military products required for peacekeeping actions or military exercise, the perishable goods, and in respect of animals, radioactive materials, explosives, international postal items, urgent cargo, the goods to be exhibited at international exhibition events, humanitarian and technical aid, messages and materials for mass media, spare parts, engines, consumables, equipment and tools required for repair and/or maintenance of the safe operation of vehicles for international transportation, currency of the Member States, foreign currency and other currency assets, precious metals, including gold, imported by national/central banks of the Member States and the branches thereof and other similar goods shall be carried out using priority procedure.

At the same time, according to Article 78 of the EEU Customs Code “Customs operations and the procedure for their performance shall be established in this Code and other treaties and acts on customs regulation, and where not covered by this Code, in other treaties and acts on customs regulation, or, if so provided in the treaties and acts on customs regulation, in accordance with the legislation of the Member States on customs regulation.

The technology for performance of customs operations shall be established in accordance with the legislation of member states on customs regulation.

Thus, the EEU Customs Code provides an opportunity to determine customs operations and the procedure for their performance not regulated by the EEU Customs Code and international treaties, and in general the technologies for performing these operations by the laws of the EEU member states.

However, despite this, **there are no provisions in the normative legal acts governing the issues that establish the priority procedure for certain categories of goods, in particular those listed in Article 81 of the EEU Customs Code.**

In accordance with provisions of Article 38 of the Customs Code of the Eurasian Economic Union, Preliminary decisions on the application of methods for determining the customs value of imported goods may be taken in cases where this is established by the legislation of member states on customs regulation. The procedure and terms for issuance by the authorized body of the Member State of a preliminary decision on the application of methods for determining the customs value of imported goods, and the procedure and terms for the application of such a preliminary decision shall be established by the legislation of the Member State on customs regulation.

However, the **Kyrgyz Republic legislation does not provide a procedure for taking a preliminary decision on the application of methods to determine the customs value of goods imported into the Kyrgyz Republic prior to the customs declaration of imported goods.**

Implementation of the Preliminary decision mechanism will not only speed up the release of goods, but also help to eliminate false declarations, which in turn will allow foreign traders to better predict and plan their foreign economic activity.



ГРАЖДАНСКАЯ ИНИЦИАТИВА  
ИНТЕРНЕТ ПОЛИТИКИ

