Key provisions of the Law «On Cybersecurity» dated April 15, 2022

June 2022

EY
Building a better working world

Our team (1/2)

Dinara Tanasheva
Partner, Tax & Law Services Leader
for Kazakhstan and Central Asia

Tel.: +7 (727) 258 5960
E-mail: Dinara.Tanasheva@kz.ey.com

- Dinara is Head of Tax and Legal Services Practice for Kazakhstan and Central Asia.
- She is an active member of the following working groups:
  - Working group on digitalization of the Council of Foreign Investors under the President of the RK;
  - Working Group of the American Chamber of Commerce (AChC) in Kazakhstan on Foreign Investment, Technology and Innovation;
  - Working Group of the EUROBAK Committee on digitalization;
  - Working group on labor legislation, human capital development and attraction of foreign labor force of the Council of Foreign Investors chaired by the President of the RK, as well as the Council for Improving the Investment Climate in the RK, Chairman of the EUROBAK HR Committee.
- Dinara has extensive experience in leading the preparation of amendments to Kazakhstani legislation and participation in various working groups to improve Kazakhstani legislation, including amendments to the Labor Code, Customs Code, Tax Code, Code of Administrative Offenses, Civil Code, Civil Procedure Code , Criminal Code, Code "On Subsoil and Subsoil Use", Rules for Issuing Work Permits.
- Dinara participated and led projects in the field of cloud technology regulation. In particular, such projects included an analysis of the legislation of the RK regarding the current restrictions on the development of cloud computing, as well as in the field of personal data.

Nargiz Suleimenova
Manager, Tax and Law

Tel.: +7 (727) 258 5960
E-mail: Nargiz.Suleimenova@kz.ey.com

- Nargiz is a Senior Associate in Tax and Legal Services at EY Kazakhstan.
- Nargiz graduated from the High School of Law «Adilet» . She received her Master of Laws (LL.M.) from the China University of Political Science and Law (CUPL).
- Nargiz is a member of the Chamber of Legal Advisers "Kazakhstan Bar Association" and the Oil and Gas Lawyers Association.
- She is an active member of the following working groups::
  - Working group on digitalization of the Council of Foreign Investors under the President of the RK;
  - Working Group of the American Chamber of Commerce (AChC) in Kazakhstan on Foreign Investment, Technology and Innovation;
  - Working Group of the EUROBAK Committee on digitalization;
- Nargiz gave a speech on the following topics:
  - EUROBAK platform (June 2, 2021): Planned changes and additions to the legislation on the protection of personal data;
  - AChC platform (September 28, 2021): Cloud services in the context of the legislation of the RK;
  - AChC platform (December 21, 2021): Digitization of the public sector: GovTech; EUROBAK platform (December 21, 2021):
  - Electronic document management: legal regulation and practice.

Our team (2/2)

Marjona Khafizova

Legal Consultant, Tax and Law

Tel.: + +998 78 140 6482
E-mail: Marjona.Khafizova@uz.ey.com

- Marjona is an EY Legal Consultant in Uzbekistan
- Marjona holds an honors degree from Westminster International University in Tashkent with a degree in commercial law.
- Marjona works in EY Tashkent office since August 2019.
- Marjona has experience in providing legal advisory services in various areas of Uzbekistan legislation, including corporate, labor, currency, and pharmaceutical legislation.
- Marjona participated in projects related to the latest changes in the field of personal data in Uzbekistan.
- Marjona participates in legal consulting projects for both domestic and international companies in various areas of legislation, including corporate, labor, antimonopoly, currency, economic legislation, etc.
- Marjona is involved in the analysis and study of changes in the legislation of Uzbekistan, as well as application in practice for Uzbek and foreign enterprises.

Adilet Sagiyev

Senior Legal Consultant, Tax and Law

Tel.: +7 727 2585960
E-mail: Adilet.Sagiyev@kz.ey.com

- Adilet is Senior Legal Consultant for EY's Tax and Legal practice in Kazakhstan.
- He is an active member of the following working groups :
  - Working group on digitalization of the Council of Foreign Investors under the President of the RK;
  - Working Group of the American Chamber of Commerce (AChC) in Kazakhstan on Foreign Investment, Technology and Innovation;
  - Working Group of the EUROBAK Committee on digitalization;
  - Adilet has experience in projects in the field of personal data, regulation of cloud technologies. In particular, such projects included an analysis of the legislation of the RK regarding the current restrictions on the development of cloud services.
- Adilet also has experience in supporting the activities of the Russian e-commerce platform on the territory of the RK, including issues of personal data, processing of payment cards in terms of the legislation of the RK.

Table of contents

Used abbreviations

SB	State bodies
RUz	The Republic of Uzbekistan
Law «On Cybersecurity»	Law of the Republic of Uzbekistan «On cybersecurity» № ZRU-764 dated 15.04.2022
SSO	State Security Office
CC RUz	Criminal code of the Republic of Uzbekistan (Approved by the Law of the Republic of Uzbekistan № 2012-II dated 22.09.1994)
RLA	Regulatory legal act
IS	Information systems
IT	Information technologies
ICT	Information and Communication technologies
CII	Critical Information infrastructure
OCII	Object of Critical Information Infrastructure
SCII	Subject of Critical Information Infrastructure

Law «On Cybersecurity»: goals and principles

Data / status:	February 25, 2022 – adopted by the Legislative Chamber March 17, 2022 – approved by the Senate April 15, 2022 – signed by the President July 17, 2022 – shall come into effect
Objective of the Law:	regulation of the field of cybersecurity
Cybersecurity:	the state of protection of the interests of the individual, society and the state from external and internal threats in cyberspace
Main principles of the cybersecurity	• legitimacy • the priority of protecting the interests of the individual, society and the state in cybersecurity • unified approach to cybersecurity regulation • **priority for the participation of domestic manufacturers in the cybersecurity system creation** • openness of the RUz to international cooperation in ensuring cybersecurity

Powers of the State bodies in the sphere of cybersecurity (1/2)

Governance bodies	Powers
President of the RUz	• Defines a unified state policy in the field of cybersecurity
SSO	• Development of RLA and state programs • Conducting operational-search activities, pre-investigation checks and investigative actions on cybersecurity incidents • Detection and prevention of cybersecurity incidents and taking appropriate measures on them, including organizational and technical measures to eliminate their consequences • Organization of work on certification of hardware and software in IS and resources in accordance with the requirements of cybersecurity • Formation of a unified register of OCII, as well as its organization and maintenance • Making a decision on the inclusion of objects in the unified register of OCII based on information provided by cybersecurity subjects • Determination of the procedure for attestation of informatization objects and OCII in accordance with the requirements of cybersecurity • Licensing of activities for the development, production and sale of cryptographic information protection tools

Powers of the State bodies in the sphere of cybersecurity(2/2)

(Continuation)

Governance bodies	Powers
SSO *(continuation)*	• Regulation of the activities of cybersecurity units, services and groups of independent experts, interaction with law enforcement agencies in the field of countering cyberthreats • Creation of a classifier according to the level of cybersecurity provision in IS and resources • Determination of mechanisms for conducting an expertise for compliance with cybersecurity requirements • Determination of assessment methods and assessment of the implementation of cybersecurity of cybersecurity objects and OCII • Definition of categorization criteria and categorization of OCII

Rights of the SSO

The State Security Office, in exercising the powers listed above, has the right, among other things:

- **to use technical installations and services free of charge to take** immediate measures to eliminate cyber attacks
- to visit state bodies and other organizations, get acquainted with the necessary documents and materials, as well as request and receive information and other necessary documents and materials from state bodies and other organizations, citizens, identify them and use them in investigative actions on cybersecurity incidents
- **to have an unimpeded access and connection in the prescribed manner to the IS and resources of state bodies and organizations,** OCII, as well as the study of data regarding the implementation and operation of cybersecurity tools for information systems and resources of these objects
- to enter freely, if necessary with damage to locking devices and other items, into residential premises and other objects of individuals and legal entities, inspect them when pursuing persons suspected of committing crimes in the field of IT, or if there are sufficient grounds to believe that there is being committed or committed such a crime, or there is a person hiding from law enforcement agencies, or if the delay may endanger the life and health of citizens, with subsequent notification of the prosecutor within 24 hours, as well as with compensation for the harm caused in accordance with the law

Right and obligations of the subjects of cybersecurity (article 16)

Subjects have the following rights:

1. to receive information from the SSO about cyber threats, software vulnerabilities, equipment and technologies in order to ensure their cybersecurity
2. to receive information and advice from the SSO on the means and methods of protection against cyber attacks, as well as methods for their detection and prevention
3. to develop and implement measures to ensure cybersecurity

Subjects are obliged, inter alia:

1. to prevent illegal distribution, theft, loss, violation of integrity, blocking and falsification of data, as well as other types of unauthorized access, take timely appropriate measures
2. to notify the SSO of cybersecurity incidents and cybercrime that have occurred, take measures to prevent the loss of relevant digital traces, and ensure the permanent storage of information necessary for analyzing cybersecurity incidents and investigating cybercrime
3. to exchange data with the SSO
4. to maintain cybersecurity incident response mechanisms and cyber security teams
5. **to ensure the storage of IS and resources in accordance with the internal policy of IS by creating a backup copy of data for a period of less than the last 3 months**
6. to grant the SSO the right to access monitoring systems and (or) cybersecurity facilities

Mechanisms ensuring cybersecurity (1/2)

№	Mechanisms ensuring cybersecurity	Description	Status of RLA
1.	Classification of cybersecurity objects (article 17)	Determination of the level of organizational and technical complexity of cybersecurity objects types. The categories of cybersecurity objects to be classified are determined in accordance with the law.	*As of the date of this presentation, the RLA has not been enacted*
2.	Expertise for compliance with cybersecurity requirements (article18)	Expertise can be mandatory or initiated by cybersecurity subjects. Expertise is mandatory for: (i) information resources of SB, (ii) IS of SB, (iii) IS included in the category of OCII. The procedure for the examination is determined by the SSO.	*As of the date of this presentation, the RLA has not been enacted*
3.	Certification of hardware and software used to ensure the cybersecurity of IS and resources (article 19)	Certification is mandatory. The certification procedure is determined by the SSO.	*As of the date of this presentation, the RLA has not been enacted*

Mechanisms ensuring cybersecurity(2/2)

№	Mechanisms ensuring cybersecurity	Description	Status of RLA
4.	Attestation of informatization objects and OCII (article 20)	Attestation of objects of informatization and OCII is a set of organizational and technical measures aimed at determining the compliance of the actual state of security of objects of informatization with the requirements of state standards and RLA in the field of cybersecurity. Categories of objects of informatization and OCII subject to attestation are determined in accordance with the law. The attestation procedure is determined by the SSO.	*As of the date of this presentation, the RLA has not been enacted*
5.	Assessment of the level of cybersecurity assurance (article 21)	Assessment of the level of cybersecurity is a set of organizational and technical measures aimed at determining the state of security of IS and resources, as well as the effectiveness of organizational measures taken. Categories of objects of informatization and OCII subject to assessment are determined in accordance with the law. The assessment procedure is determined by the SSO.	*As of the date of this presentation, the RLA has not been enacted*

OCII

In accordance with the Law "On Cybersecurity", OCII includes informatization systems used in the following areas::

1. in the field of public administration and the provision of public services
2. defense
3. ensuring state security and public order
4. fuel and energy complex (nuclear energy)
5. chemical, petrochemical industries
6. metallurgy
7. water use and water supply
8. agriculture
9. health care
10. housing and communal services
11. banking and financial system
12. transport
13. ICT
14. ecology and environmental protection, mining and processing of minerals of strategic importance
15. industry
16. as well as in other sectors of the economy and the social sphere

Basic provisions regarding OCII

i. **OCII are divided into the following categories:**

- Hight level OCII
- Medium level OCII
- Low level OCII

The criteria for categorizing OCII is determined by the SSO

(As of the date of this presentation, these criteria have not been approved)

ii. **The SSO maintains a unified register of OCII.** As of the date of this presentation, RLA regarding the category of OCII subjects mandatory to entry into the unified register, as well as the procedure for entry, have not been approved.

iii. **The subjects of critical information infrastructure, among other things, are obliged:**

- To provide information about cybersecurity incidents to the attention of the SSO
- To provide the SSO with access rights to monitoring systems or to OCII for the implementation of organizational and technical measures for monitoring the state of ensuring cybersecurity
- To notify the SSO when changing information about an object included in the unified register of OCII
- To ensure the security of OCII in accordance with the requirements of cybersecurity

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, strategy and transactions and consulting services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY works together with companies across the CIS and assists them in realizing their business goals. 5,500 professionals work at 19 CIS offices (in Moscow, St. Petersburg, Novosibirsk, Ekaterinburg, Kazan, Krasnodar, Rostov-on-Don, Togliatti, Vladivostok, Almaty, Nur-Sultan, Atyrau, Bishkek, Baku, Kyiv, Tashkent, Tbilisi, Yerevan, and Minsk).

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

www.ey.com/en_uz

The information contained in this publication is presented in summary form and is therefore intended for general guidance only. Although prepared with utmost care this publication is not intended to be a substitute for detailed research or the exercise of professional judgment. EY is not responsible for any damage caused to any person as a result of an action or refusal to act based on the information contained in this publication. For all specific questions, contact a specialist in the relevant field.
.
www.ey.com/en_uz