ALEGAL ALERT: LAW ON CYBER SECURITY

GRATA International Mongolia

LAW ON CYBER SECURITY

On June 30, 2021, the Government of Mongolia submitted a draft Law on Cyber security and supplementary draft laws to the State Great Khural(or the Parliament). On December 17, 2021 at the plenary session, the State Great Khural approved the draft Law on Cyber security. The law has adopted the first time in Mongolia and has been discussed and developed 7 times over the past decade.

Within framework of the Fourth Industrial Revolution, our country has established a legal system for ensuring national cybersecurity, a vital law that creates legal conditions for the development and security of the country, as well as information security, which is an integral part of national security[1].

In case of violation of the Law on Cyber security and investigating the violation, the terminology, element of crime and the concept of Chapter 26 of the Criminal Code of Mongolia have been amended in accordance with the Law on Cyber Security and the UN Budapest Convention. In addition, Law on Infringement, the Law on Communications, the Law on Infringement procedure and the Law on Criminal Procedure have been amended in connection with the adoption of the Law on Cyber security[2].

An overview of highlighted new regulations of the Law on Cyber security is outlined in this legal alert.

Purpose of the Law

The purpose of the Law on Cyber security is to establish a system, principles and legal basis for cybersecurity operations, and to manage the relations ensuring the integrity, confidentiality and accessibility of information in cyberspace and cyber environment.

Scope of the Law

Coordinates, organizes and monitors the relations between the state, individuals and legal entities related to cyber security.

Unless otherwise provided by law, this law shall apply to foreign citizens, stateless persons, and legal entities of foreign country and with foreign investment which operates through Mongolia's information system and information network.

Definitions

"Cyber security"- means the integrity and confidentiality of information in a cyber environment;

"Cyber space"- means tangible and intangible field consisting of the Internet and other information and communication networks and the interconnected set of information infrastructure to ensure their operation;

"Cyber environment"- means an information system and information network environment that allows to access, login, collect, process, store and use of information;

"Cyber- attack"- means an action aimed at undermining the cyber security of an information system or information network;

"Cyber security breach"- means an act or omission that threatens the integrity, confidentiality or accessibility of information;

"Center for Combatting Cyber-attacks and violations"- means an entity with the main function to coordinate the activities of preventing, detecting, suppressing, responding to and restoring information systems and providing professional management;

[1] http://parliament.mn/n/mo3on

“Cyber security risk assessment”- means specialized activities to determine the probability of a cyber security breach, threat, vulnerability its consequences, risk reduction and prevention measures for electronic information, information systems and information networks;

“*Organization with critical information infrastructure*”- means an organization with an information system and information network that could cause a damage to Mongolia's national security, society and economy due to the loss of cyber security;

"National cyber-attack"- an attack on the information systems and information networks of an organization with critical information infrastructure that can disrupt the normal functioning of the organization and harm the national Security, society and economy of Mongolia;

"Integrated state information network" - a set of state Internet, official and special use networks with integrated infrastructure aimed at exchanging information between government organizations and ensuring cyber security;

Areas of cyber security:

- cyber security policy, management and organization;
- technical and technological measures to ensure cyber security;
- prevention and education of cyber-attacks and violations;
- detection, suppression, retaliation and recovery of cyber-attacks and violations.

Cyber security risk assessment

- Cyber security risk assessment will be conducted by a legal entity which registered with the state central administrative body in charge of digital development and telecommunications. The legal entity shall have a full-time employee with a valid certificate issued by an international professional association, standardization organization or equivalent or similar organization.
- Procedures and methodologies for cyber security risk assessment shall be approved by the state central administrative body in charge of digital development and telecommunications in cooperation with intelligence agencies.

Information security audit

An information security auditing shall be performed by a legal entity registered with the state central administrative body in charge of digital development and telecommunication. The legal entity to conduct an information security auditing shall have:

- a full-time staff member with a valid certificate of information security auditing which issued by an international professional association, standardization organization or equivalent or similar organization;
- the employee does not work under a parallel contract with other legal entities authorized to conduct similar audits;
- other requirements under the law.

CYBER SECURITY SYSTEM

Government	• The Government shall approve the national cyber security strategy; • Incorporate cyber security in development policy and planning documents and organize the implementation of legislation; • Shall approve the list of organizations with critical information infrastructure;
Cyber security council	• ***The Council is headed by the Prime Minister and chaired by a member of the Government in charge of digital development and telecommunications the Head of the General Intelligence Agency of Mongolia. The council has a Secretariat.*** • The Council shall monitor the implementation of Law on Cyber security; • Shall provide integrated management and organization of national cyber security activities and coordinate the activities of relevant organizations;
State central administrative body in charge of digital development and telecommunication	• Implement legislation and decisions of the competent authorities to ensure cyber security; • Develop a development policy on cyber security and organize its implementation; • Develop common procedures for cyber security in cooperation with intelligence agencies and cyber security organzations of the armed forces;
Intelligence agency	• Intelligence agency shall organize integrated state information network and ensure its cyber security; • Monitor the cyber security activities of state-owned legal entities connected to the state information network and have critical information infrastructure, and organize training for relevant persons; • Develop a national cyber-attack protection plan and monitor its implementation;
Armed Forces	• Organize the implementation of cyber security legislation in the defense sector; • Ensure cyber security of defence operations in peacetime, security of information networks of the armed forces, and if necessary, support the activities of ensuring the security of the country's cyber space;
Police	• Receive information on crimes related to cyber attacks and violations, obtain information from relevant government agencies, officials, individuals and legal entities to carry out activities specified in the law and perform related functions; • Deliver recommendations requirements and warnings to individuals and legal entities on issues of cyber security;
State-owned enterprise	• Approve internal procedures for cyber security activities; • Comply with the recommendations and requirements given by the competent authority on ensuring cyber security; • Immediately inform cyber attacks and violations to the Center for combatting cyber attacks and violations ;
Legal entity	• Approve internal procedures for cyber security activities; • Immediately inform and receive assistance on cyber-attacks and violations from the Center for combatting cyber attacks and violations;
Citizen	• Responsible for the cyber security of her/his own or person under his/her care; • Follow the recommendations issued by the relevant organization and comply with the requirements;

National center shall work within the structure of the Intelligence Agency.

- National center shall coordinate and harmonize the activities of cyber-attack and violations control centers nationwide and provide professional assistance;
- Exchange information and cooperate with similar international and foreign organizations within the scope of its responsibilities on behalf of Mongolia;
- Receive and transfer information on cyber attacks and violations to the relevant authorities;
- Provide recommendations and requirements on cyber attacks and violations to organizations with critical information infrastructure, other relevant organizations and officials;
- Classification of information on cyber-attack and violations registered nationwide;

Community center shall operate under the state central administrative body in charge of digital development and telecommunication.

- Community center shall detect, suppress and respond to cyber-attacks and violations of information systems and information networks of the citizens and legal entities, and to support the rehabilitation of information systems affected by cyber-attack and violation;
- Conduct research and analysis on cyber-attacks and violations, and disseminate recommendations and information to the public;
- Collaborate with other Centers;
- Provide recommendations and requirements to citizens and legal entities on cyber-attack and violation;

Armed force center shall operate within the structure of the cyber security organization of the Armed Forces.

- Prevent, detect, suppress and respond to cyber-attack and violation of defense information systems, and rehabilitate information systems affected by cyber attack and violation;
- Support protection against external cyber-attack and aggression;
- Exchange and cooperate with foreign and domestic organizations with similar functions;
- Review and validate hardware and software for cyber security in the defense sector.

Liability for the violation of the Law

- In case of infringement of this law, a legal entity shall be imposed a fine in amount of MNT300,000(app 100USD) to MNT10,000,000 (app 3317USD) in accordance with the Article 14.13 of the Law on Infringement;
- While, pursuant to the Article 26 of the Criminal code, depending on the nature/elements of the crime, a fine of MNT 2,700,000(app 895USD) up to MNT40,000,000(app 13,270USD) or restriction of the travel right for a period of 6 months up to 2 years or imprisonment for a term of 6 months up to 12 years shall be imposed.
- If an action of an state Official which violated this law are not considered as a crime, he / she shall be subject to liability specified under the Law on Civil Service or the Labour Law.

Source:

https://legalinfo.mn/mn/detail?lawId=16390365491061 – “Law on Cyber security”

https://legalinfo.mn/mn/detail/12695 - “Law on Infringement” /2017/

https://legalinfo.mn/mn/detail/11634 - “Criminal Code” /2015/

http://parliament.mn/n/mo3on - “Infographic: Introduction to the Law on Cyber security”

For more information or any queries, please feel free to contact Bolormaa.V, Partner by bvolodya@gratanet.com or +976 70155031.