NOMIN & ADVOCATES
LLP

DRAFT LAW ON PERSONAL DATA PROTECTION

April 2021

1. Introduction

The Cabinet submitted the Draft Law on Personal Data Protection[1] ("**Draft Law**") to the Parliament of Mongolia ("**Parliament**") in March 2021. The Draft Law aims to improve the current legal environment on personal data protection and is yet to be read at the Parliament. If adopted, the Draft Law would transform the existing legal framework on privacy and data protection, and establish new mandatory standards to collect, process, store, use and protect personal data.

Currently, the Law of Mongolia on Personal Confidential Information ("**Personal Confidential Information Law**"), adopted in 1995, regulates the protection and disclosure of personal confidential information. However, the Personal Confidential Information Law has been criticized for its general and outdated terms and limited framework to provide protection for personal data. In today's digital world, personal data is the fuel that drives much commercial activity online. However, how this data is collected and used has raised concerns regarding privacy and the security of information[2]. As such, the Draft Law aims to regulate the protection of personal data under Mongolian law, which may have major implications on the business sector.

The Draft Law contains 8 chapters and 29 articles and defines key terms such as personal data, sensitive personal data and biometric data; regulates the collection, processing and use certain types of personal data; and sets forth the obligations and rights of data subjects, data controllers and government bodies. In terms of scope, the Draft Law regulates the protection of personal data concerning natural persons only.

Although the Draft Law is subject to a number of review and revision until its enactment, we summarize below the key points and implications of the current version of the Draft Law.

2. Definition of the Key Terms

The concept of "personal data" has not been strictly defined in the Personal Confidential Information Law and other relevant legislations. On the other hand, the Draft Law provides a detailed definition for personal data and its special categories.

Under Article 4.1.1 of the Draft Law, personal data is defined as to include the following information relating to the data subject:

(a) sensitive personal data;
(b) first and last name;
(c) date and place of birth;
(d) permanent address and location data;
(e) citizen's registration number;
(f) education and membership;
(g) online identifiers; and
(h) any other information that can be used to directly or indirectly identify a natural person.

The Draft Law further defines sensitive personal data as "information specified in Article 4.1 of the Personal Confidential Information Law, or information about the individual's ethnicity, race, religion and

[1] The full text of the Draft Law can be found here.
[2] Data Protection regulations and international date flows: Implications for trade and development 2020.

beliefs; economic, genetic, biometric data; electronic signature; criminal record, and data concerning natural person's sexual orientation and sex life"[3].

The Draft Law further defines specific components of personal data, such as biometric and genetic data, as well as other terms, including data collection, processing and use. We set out below brief summarizations of some key terms included in the Draft Law[4].

(a) "**biometric data**" means personal data that can confirm the unique identification of a natural person, such as fingerprint, iris, facial images, or voice;

(b) "**genetic data**" means personal data that gives unique information about the physiology, health, or inherited genetic characteristics of an individual;

(c) "**data controller**" means a natural or legal person, which shall determine the purpose, scope, management, organisation, protection, and other necessary measures to be carried out with respect to personal data based on the consent of the data subject or in accordance with provisions of the law; and

(d) "**data processing**" means any operation or combination of operations performed on personal data manually or by automated means to organize, store, alter, erase, analyze, or restore such data.

The above definitions appear to be similar to those of the General Data Protection Regulation[5], with the addition of specific local terms and some revisions. Specific categories of personal data defined above have different conditions for lawful processing with respect to the collection, processing and use of the data.

The Draft Law, in its current form, appears to keep the existing concept of "personal confidential information". This may raise concerns as to the consistency in respect of protection standards of personal data and personal confidential information.

3. Lawfulness of Collecting, Processing and Using Personal Data

3.1. Collection, Processing and Use of Personal Data by Private Entities

Pursuant to the Draft Law, personal data should be collected, processed and used on the basis of the consent of the data subject or other legitimate basis. Article 6.3 of the Draft Law sets forth that the consent from the data subject must be obtained in writing. This requirement shall be satisfied if the consent is obtained in (i) a paper form; or (ii) an electronic form.

Article 6.2 of the Draft Law further sets out the following conditions that must be presented to the data subject in order to obtain his/her consent:

(a) purpose and objectives of collecting data;

(b) data controller's name and contact information;

[3] Article 4.1.2 of the Draft Law.

[4] Article 4 of the Draft Law.

[5] Regulation 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 (Data Protection Directive).

(c) list of data to be processed;
(d) how long the data will be processed and stored;
(e) whether the data will be disclosed;
(f) whether the data will be transferred to a third party; and
(a) conditions for revoking the consent.

Communication and Information Technology Authority of Mongolia shall approve the model consent form template for the collection of personal data[6].

The consent regarding the collection, processing and use of sensitive personal data must be obtained by paper or electronic signature.[7] The Draft Law specifically requires the consent form for sensitive personal data be obtained by "**electronic signature**", but it is unclear whether the "**electronic consent**" to be obtained for non-sensitive personal data must also be evidenced by electronic signature.

In relation to this requirement, an Amendment to the Law of Mongolia on Electronic Signature has also been simultaneously proposed with the Draft Law. According to this amendment, every citizen above the age of 16 shall be provided with an electronic signature to ensure the implementation of the Draft Law.

The regulation on the processing of sensitive personal data shall be further approved by the Government of Mongolia based on the proposal of the National Human Rights Commission of Mongolia[8].

The Draft Law also imposes further restrictions with respect to the collection and use of biometric data. Currently, the service providers can and do collect fingerprints, i.e., biometric data, for the purpose of awarding discount cards and identifying its customers. Pursuant to the Draft Law, only the state authorities; and employers (to a certain extent) can collect, process, and use biometric data based on the data subject's consent[9]. In other words, if the Draft Law is approved, private entities can no longer collect, process or use biometric data of individuals, even with their consent.

3.2. Collection, Processing and Use of Personal Data by State Authorities

Pursuant to Article 7.1 of the Draft Law, the state authorities can collect and process personal data if the collection and processing of such data is permitted by law, necessary for the performance of its obligations under the international treaties or agreements entered with individuals, to implement its legal functions, and if the data subject consented to the collection and processing of his/her personal data.

On the other hand, the use of personal data by the state authorities is allowed on the following grounds:

(a) the data subject consented to its use;
(b) the use of personal data is permitted by law;
(c) the personal data is used for the purpose of protecting national security and public policy;

[6] Article 24.1.3 of the Draft Law.
[7] Article 9.1 of the Draft Law.
[8] Article 9.3 of the Draft Law.
[9] Article 10.1-10.2 of the Draft Law.

(d) the use of personal data is necessary in order to protect vital interests of the data subject or of another natural person; and
(e) the personal data is used for the purpose of preparing non-identifiable statistical surveys.

In addition, the Draft Law provides that the state authorities can disclose the collected personal data as publicly available information after making it non-identifiable. The disclosure of such data shall be carried out in accordance with Article 11 of the Law of Mongolia on Public Information ("**Public Information Law**"), which has also been proposed to the Parliament. According to the Public Information Law, the disclosed data can be accessed and used, with or without fee, for the purpose of supporting the business sector, economic growth, academic studies, and surveys[10].

4. Data Controller and Data Processor

As defined in the Draft Law, data controllers determine the purpose and means to collect, process and use personal data, as well as the scope of the personal data to be processed. In short, the person/organisation deciding "why" and "how" the personal data is being collected, processed and used is the data controller. On the other hand, data processors only collect and process personal data on behalf of the controller based on a contract.

As data controllers and data processors have different status under the Draft Law, obligations and responsibilities of each one are also provided differently. In particular, data controllers have more direct obligations to the data subject, whereas the data processors shall operate under the instructions of the data controller. Among others, the data controllers shall have the following obligations[11]:

(a) to approve and follow an internal regulation on data collection, processing and use;
(b) to inform the data subjects about data processing;
(c) to notify the data subjects of the rectification or erasure of the data;
(d) upon request, to provide an electronic copy of the collected data to the data subject for free; and
(e) to respond to complaints lodged by data subjects within 3 days.

The data processor, on the other hand, shall collect, process or use personal data under the supervision of the data controller. Unless otherwise agreed in the contract entered between the data processor and controller, the data processor shall not assign its obligations to a third party. In addition, the data processor shall also return all collected and processed data to the data controller upon termination/expiry of the agreement without retaining any copies.

5. Data Breach and Remedial Actions

Another area in which the Draft Law aims to improve upon is the security and protection of personal data. Currently, there are no specific requirements regarding data breaches and what measures should

[10] Article 11 of the Public Information Law.
[11] Article 17 of the Draft Law.

be taken if such breach occurs. Chapter 5 of the Draft Law focuses on legal requirements with respect to this matter.

Pursuant to Article 19.1.3 of the Draft Law, data controllers and processors must take all measures to ensure that the system handling personal data is secure. Both the data controller and processor must approve and implement internal data security regulation.

In addition to the internal data security regulation, data controllers and processers must approve a security plan to be implemented in the event of a data breach; and a regulation/instruction to limit the use of personal data, erasure of data and pseudonymization[12].

In the case of security breach, the data processor shall immediately notify the data controller. If such breach could cause harm to the data subject's rights and legal interests, the data controller shall immediately send a notice to the data subject. The notice to the data subject shall include the following:

(a) register of the data subject;
(b) data controller's name and contact information;
(c) negative impacts that could occur due to the data breach; and
(d) measures being taken or have been taken to mitigate the negative impact of the data breach[13].

The Draft Law further provides that the data subjects may file complaints to the Communications Regulatory Commission ("**CRC**") or other relevant authorities if the breach infringed their rights and interests.

In addition, the data controller must keep a record of data breaches and remedial actions taken to mitigate the negative impact of such breach. This record shall be submitted to the CRC annually or immediately, if requested.

Further, all data controllers and processors shall conduct risk assessment to ensure the safety of the data processing system. In addition to this assessment, if the data processing is being conducted fully automatically and (i) such automatic processing could harm the rights and legal interests of the data subject; or (ii) sensitive personal data is regularly processed, the data controller shall conduct specific risk assessment on the automated technology[14]. The risk assessment report shall be submitted to the CRC and only upon CRC's approval, the automated technology can be used to collect, process and use data.

Lastly, specific regulations are to be approved by the authorities with respect to the security and protection of personal data. Namely, the Communication and Information Technology Authority shall approve the regulation on security requirements for the collection, processing and use of personal data; risk assessment; and the regulation regarding storage of biometric data. Based on the proposal of the National Human Rights Commission, Communication and Information Technology Authority and CRC

[12] Article 21.6 of the Draft Law.
[13] Article 21.5 of the Draft Law.
[14] Article 22.1 of the Draft Law.

shall jointly approve the regulation on the risk assessment to be conducted on the automated technology.

6. Concluding Comments

Although the use of personal data has been integral part of our lives in the last two decades, there has not been major developments in the legislation to ensure its protection. As such, we view that the introduction of the Draft Law is a much-needed reform regarding privacy and data protection as it provides detailed regulations regarding the collection, processing and use of personal data.

The Draft Law introduces a comprehensive definition of personal data to be protected under law and employs a consent-based approach, with specific requirements applying to different categories of personal data, the form and substance of the consent, but it also sets out other legal grounds to collect, process and use personal data without the consent of the data subject. If the Draft Law is passed by the Parliament in its current form, the data controllers and processors will have to comply with strict regulatory requirements with respect to the use of personal data in its operations. Further, the collection and use of biometric data by private entities will be prohibited altogether.

As for sanctions, in order for effective enforcement of the Draft Law, amendments to the Criminal Code of Mongolia (“**Criminal Code**”) and the Law of Mongolia on Offence (“**Offence Law**”) have been proposed concurrently with the Draft Law, providing specific criminal and administrative sanctions for the breach of data protection.

As the rules surrounding data protection affect individuals and businesses alike, it is important to find a balanced approach. On this basis, we view that while the main objective of the Draft Law to protect the right to privacy is certainly commendable, certain strict requirements could be burdensome to implement for small and medium businesses. Further, as the extraterritorial application and enforcement of the requirements of the Draft Law is vague, the Draft Law may disproportionately affect domestic business entities.

***

If you would like further information on this publication, please contact:

Nominchimeg Odsuren
Managing Partner
nominchimeg@nominadvocates.com

+976 7505 3003

Tushigjargal Bold
Associate

tushigjargal@nominadvocates.com

+976 7505 3001

This publication should not be considered as legal advice or as a substitute for legal counsel. It is provided by Nomin & Advocates LLP as a general informational service. Prior results do not guarantee a similar outcome.

Nomin & Advocates LLP
Suite 701, Level 7, New Horizons Office,
Olympic street, 1st khoroo,
Sukhbaatar district, Ulaanbaatar, Mongolia
(+976) 7505 3000
www.nominadvocates.com

* * *