

# **DATA PROTECTION LAWS OF THE WORLD**

Mongolia



Downloaded: 7 December 2022

## MONGOLIA



Last modified 23 February 2022

### LAW

On 17 December 2021, the Parliament of Mongolia (the “**Parliament**”) adopted the Law of Mongolia on Personal Data Protection (the “**Data Protection Law**”) which will come into effect and full force from 1 May 2022. The Data Protection Law applies to matters related to personal privacy and relations in connection with the collecting, processing, using, and security of Personal Data (as defined below) of an individual, as well as the collection, processing and use of individual’s Personal Data with the help of technology and software. The Data Protection Law regulates the handling of Personal Data and Sensitive Personal Data by Data Controller (as defined below).

The Data Protection Law defines specific components of Personal Data and persons that are subject to regulations of the Data Protection Law. For instance, “data owner” means any individual (or his/her legal representative) who can be determined by his/her Personal Data defined under the Data Protection Law (“**Data Owner**”) and “data controller” means a natural or legal person, who collects, processes and uses Personal Data based on the permission of Data Owner or in accordance with the law (“**Data Controller**”).

The Data Protection Law mainly divides human data (information) into two categories:

- Personal Data; and
- Sensitive Personal Data.

### DEFINITIONS

#### Definition of personal data

Pursuant to Article 4.1.11 of the Data Protection Law, the following information refers to Personal Data:

- sensitive personal data;
- first and last name;
- date and place of birth;
- permanent address and location data;
- citizen’s registration number;
- properties;
- education and membership;
- online identifiers; and
- any other information that can be used to directly or indirectly identify a natural person.

#### Definition of sensitive personal data

Pursuant to the Data Protection Law, Sensitive Personal Data is subject to personal privacy. Sensitive Personal Data as defined in

Article 4.1.12 of the Data Protection Law means:

- ethnicity and race;
- religion and beliefs;
- health, correspondence, genetic and biometric data;
- personal key of an electronic signature;
- criminal status and record; and
- any data concerning sexual orientation and sexual relationships.

## NATIONAL DATA PROTECTION AUTHORITY

The National Human Rights Commission, the Ministry of Digital Development and Communications, and other relevant state authorities have various degrees of oversight of data protection under Chapter 6 of the Data Protection Law.

The Human Rights Commission is entitled to exercise the following with respect to data protection:

- monitor the implementation of the legislation on protection of Personal Data, organise public awareness and advocacy activities and to submit requirements and recommendations to relevant organisations and provide comment on the relevant regulations;
- receive complaints and information for investigation or initiate an investigation in its sole discretion if it is considered that human rights and freedoms protected under the Data Protection Law have been infringed or potentially infringed in the course of collecting, processing, using and protecting Personal Data and to submit requirements and recommendations to the relevant organisations;
- provide requirement and recommendations to the relevant entities in the context of collecting, processing, using and protecting Sensitive Personal Data;
- receive and review records submitted by Data Controller regarding the violations detected during the collection, processing and use of Personal Data and the measures taken to eliminate its negative consequences, and make recommendations on further issues to be considered; and
- make recommendations for the prevention of violations of human rights and freedoms in the collection, processing and use of information through technology without human intervention.

The Ministry of Digital Development and Communications is entitled to exercise the following with respect to data protection:

- maintain the implementation of legislation on protection of Personal Data, organise public awareness and advocacy activities, provide professional advice and cooperate with the relevant organisations;
- adopt the technological safety requirement and regulations to be followed in the processing of personal sensitive, genetics and biometric data; and
- receive and register information about security breaches and cyber-attacks on information systems intended for data collection, processing and use, and take necessary measures immediately.

In addition, other state authorities are entitled to monitor the collection, processing and use of Personal Data by Data Controllers within the scope of their functions specified under relevant laws.

## REGISTRATION

There is no registration requirement for Data Controllers or data processing activities except that Data Controllers have the obligation to keep records of:

- its activities of collection, processing and use of Personal Data; and
- its response to damages occurred to Personal Data.

Data Controllers are required to submit records of their response to damages occurred to Personal Data to the National Human Rights Commission annually or at any time as requested by the National Human Rights Commission.

## DATA PROTECTION OFFICERS

Organisations are not required to appoint a data protection officer. However, the Data Protection Law provides that Data Controller and any person who processes the data must adopt internal rules and regulations on:

- maintaining an information security; and
- measures to be taken in case of data loss and a plan to deliver information to the Data Owner and the relevant state authority.

In this regard, organisations, as a Data Controller and processor, may appoint a data protection officer of their own volition.

## COLLECTION & PROCESSING

In accordance with Chapter 2 of the Data Protection Law, state authorities, individuals, legal entities and other natural persons may collect, process and use (i) Personal Data and (ii) Sensitive Personal Data on the grounds provided by law and with the permission of the Data Owner.

The Data Protection Law mainly divides the collection and processing of Personal and Sensitive Personal Data as follows:

- collection and processing of Personal Data;
- collection and processing of Sensitive Personal Data;
- collection and processing of Genetics and Biometric data (types of Sensitive Personal Data); and
- collection and processing of Personal Data after death of the Data Owner.

State authorities can collect and process Personal Data if:

- permitted to by the Data Owner or permitted by law;
- execution and enforcement of contractual obligations;
- exercising the rights and obligations by the data controller during the employment relations;
- enforcement of obligations under the international treaties to which Mongolia is a party to; or
- enforcement actions by authorities as provided under applicable laws without interfering with the legitimate interests and rights of the Data Owner.

Legal entity and any persons other than the state authority can collect and process Personal Data if:

- permitted by the Data Owner or permitted by law;
- execution and enforcement of contractual obligations;
- exercising the rights and obligations by the data controller during the employment relations;
- Personal Data that became legally available to the public; or
- for making historical, scientific, artistic and literary works by maintaining the anonymity of the Data Owner.

Unless otherwise provided under relevant laws, Data Controller must obtain digital/electronic or written permission from Data Owner upon presenting the following terms and conditions to the Data Owner:

- definitive purpose of collecting, processing and using the Personal Data;
- name and contact information of the Data Controller;
- list of Personal Data to be collected, processed, and used;
- period of processing and using Personal Data;
- whether to make the Personal Data publicly available;
- whether to transfer Personal Data to other persons together with the name of recipient and list of Personal Data to be transferred; and
- form of cancelling the permission.

The collection, processing and use of Sensitive Personal Data is prohibited except as follows:

- state authorities and other persons as permitted by Data Owner;
- health worker to exercise their rights and responsibilities under applicable laws in order to protect the health of an individual; or

- in the process of providing explanations, declarations and evidence in accordance with the law on claims of citizens or legal entities.

Genetic and Biometric data can only be collected and used by the following state authorities in accordance with applicable laws:

- non-overlapping data of the human body (fingerprints) by the state registration authority for the purpose civil registration and overseeing the voter registration;
- biometric data by the border protection authority for the purpose of identifying and verifying a foreign citizen crossing the state border;
- genetic and biometric information by the competent authorities specified in the law for the purpose of combating, preventing and investigating crimes and violations;
- genetic and biometric data by court forensic organisation for forensic examination of criminal, civil, administrative and other cases and dispute proceedings;
- Biometric information of the Parliament member for the purposes of attendance and voting; and
- an employer may, with the employee's permission, use biometric data other than non-identifiable human data (fingerprints) to facilitate the identification and verification of employees in accordance with the internal employment regulations established in accordance with the Labour Law.

Also, Personal Data and Sensitive Personal Data may be collected, processed and used for (i) journalistic purposes or (ii) for the purpose of creating historical, scientific, artistic and literary works and preparing statistical information based on the permission from Data Owner.

In addition, the Data Protection Law provides that unless otherwise provided by law, (i) if Data Owner has died or is considered dead, the relevant data shall be collected, processed and used with the written permission of the successor, his/her family member or legal representative and (ii) permission to collect, process or use Sensitive Personal Data is not required 70 years after the death of the Data Owner.

## TRANSFER

Under the Data Protection Law, transfer of Personal Data to is prohibited unless otherwise approved under the relevant laws or permitted by the Data Owner.

## SECURITY

Data Controller must take the following measures for the purpose of maintaining data security:

- adopt internal data security rules and regulations;
- approve a plan in accordance with the law to take measures and deliver notice to the state authority and Data Owner in the event of data loss;
- take all measures to ensure the integrity, confidentiality and accessibility of information technology system used for data collection, processing and use;
- adopt and follow procedures and instructions on restricting the use of data, deleting the data and making it impossible to identify the Data Owner; and
- in the event of making decisions that affect the rights, freedom and legitimate interests of the Data Owner or regularly processing Sensitive Personal Data, Data Controller must evaluate the situation in order to ensure the security of data processing activities. Guidelines and procedures for the evaluation will be adopted by the Ministry of Digital Development and Communications as recommended by the National Human Rights Commission.

The Ministry of Digital Development and Communications will determine the minimum requirements for data security, instructions for assessment and technology of storage during the data collection, processing and use.

## BREACH NOTIFICATION

The Data Protection Law states that data collector must promptly notify the Data Controller of any breaches occurred during the data collection and processing. If such breach has potential to cause damages to the rights and legitimate interest of Data Owner,

the Data Controller must immediately provide notice to the Data Owner including the following:

- the Data Owner who will be affected by the breach;
- name and contact information of the Data Controller;
- possible negative consequences from the breach; and
- measures taken to eliminate potential negative consequences from the breach.

## ENFORCEMENT

The Ministry of Digital Development and Communications and the National Human Rights Commission are responsible for the enforcement of the Data Protection Law and will investigate an act or practice if such act or practice may be (i) a violation of the privacy of an individual and (ii) a complaint about the act or practice have been submitted. Pursuant to the Data Protection Law, Data Owner can submit a claim to the administrative courts or the competent authority as provided under the relevant laws with respect to its complaint on the data collection, processing and use by the state authority. Complaints on data collection, processing and use by the other data controllers can be submitted to the other authorised entity or the Human Rights Commission.

Any breach or violations of the Data Protection Law is subject to sanctions under the Violations Law or the Criminal Code of Mongolia.

## ELECTRONIC MARKETING

There are no specific provisions under the Data Protection Law or other Mongolian laws regulating electronic marketing communications. It is important to point out, however, that, according to the Data Protection Law, all processing of consumer Personal Data (which includes the collection, storage and making available to the public) can only occur upon the appropriate legal basis for such purpose and permission provided by the Data Owner.

## ONLINE PRIVACY

Currently, there are no laws or regulations in Mongolia regulating online privacy, including cookies and location data. Although the Data Protection Law does not address online privacy including cookies and location data, the Ministry of Digital Development and Communications, within the authority entitled to it under the Data Protection Law and other relevant laws, may adopt regulations concerning the storage, use, disclosure and other processing of data collected on the internet.

## KEY CONTACTS

### DB&GTS LLP

[dblaw.mn/](http://dblaw.mn/)



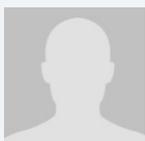
**Battushig Batsuren**

Partner

DB&GTS LLP

T +976 99075047

[b.batsuren@dblaw.mn](mailto:b.batsuren@dblaw.mn)



**Ariunbayar Enkhbat**

Associate

DB&GTS LLP

T +976 88006058

[e.ariunbayar@dblaw.mn](mailto:e.ariunbayar@dblaw.mn)

## DATA PRIVACY TOOL

You may also be interested in our [Data Privacy Scorebox](#) to assess your organization's level of data protection maturity.

## **Disclaimer**

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at [www.dlapiper.com](http://www.dlapiper.com).

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2022 DLA Piper. All rights reserved.