# Mongolia introduces Personal Data Protection Law effective from 1 May 2022

**Contact us:**

**Michael Ahern**
Partner
Tax and Legal Services
michael.ahern@pwc.com

**Tsendmaa Choijamts**
Director
Tax and Legal Services
tsendmaa.choijamts@pwc.com

**Munkhjargal Ragchaakhuu**
Legal Manager
Tax and Legal Services
munkhjargal.ragchaakhuu@pwc.com

**Amarjargal Batchuluun**
Senior consultant
Tax and Legal Services
amarjargal.batchuluun@pwc.com

**PwC Legal LLP**

Central Tower, 6th floor
Suite 603, Ulaanbaatar
14200, Mongolia
Tel : + 976 70009089
Fax : +976 11 322068
www.pwc.com/mn

On 17 December 2021, the Parliament of Mongolia passed *the Law on Personal Data Protection* (the "PDPL") effective from 1 May 2022. The PDPL, once effective, will establish broader and more stringent regulatory regimes surrounding personal data in Mongolia, compared to its preceding law the *Law on Personal Secrecy (1995)*.

The PDPL is intended to regulate together with *the Cybersecurity law (2021)*, *Public Information Transparency Law (2021)*, and *Electronic Signature Law (2021)* (each effective from 1 May 2022) and create a comprehensive framework governing cybersecurity and data privacy protection in Mongolia. We highlight the key aspects of the PDPL and its impact on businesses.

## Application

The PDPL applies to all individuals, legal entities and organizations without legal status (representative offices and permanent establishments) collecting, processing, using and protecting personal data in Mongolia.

## Scope of personal information and definitions

### 1. What is personal data ?

- ❑ any information that can be used to directly or indirectly identify a natural person including but not limited to:
  - sensitive personal data;
  - first and last name;
  - date and place of birth;
  - residential address and location data;
  - citizen's registration number;
  - assets and properties;
  - education;
  - membership; and
  - online identifiers.

### 2. What is sensitive data ?

- ❑ information about the individual's ethnicity, race, religion, beliefs, health, communications / correspondence, genetic and biometric data, digital signature private key, criminal record, and data concerning natural person's sexual orientation and identity as well as sex life.

### 3. Who is data subject ?

- ❑ A natural person identified by the above-mentioned information.

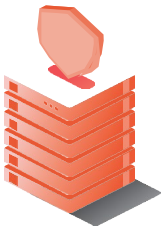
### 4. Who is data controller ?

- ❑ a natural person, legal entity or organizations without legal status that collects, processes and uses data in accordance with the PDPL or with the consent of the data subject.

## Introduced new terms and definitions (cont'd)

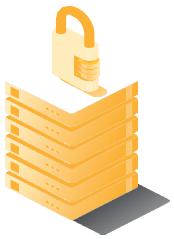
**Data use**

Using, transferring and accessing data



**Data collecting**

Obtaining (procuring), gathering and registering data



**Data processing**

Classifying, storing, analyzing, modifying, disposing, restoring and combination of those activities

## Key requirements

**1. Legal basis for collecting, processing and using personal data**

The Law on Personal Secrecy (1995) has long been ambiguous as to whether processing personal information unless 'legally required' is permissible and has not clearly provided for a 'consent' requirement. The PDPL provides that legal entities and organizations without legal status may collect, process and use personal data in the following cases:

- the data subject has consented;
- it is legally required to do so;
- where necessary during employment relations;
- where necessary for entry into and performance under a contract;
- where the data is already publicly available under a law; and
- where the personal data has become anonymous to be used in preparing historical, scientific, artistic and literary works or open data and statistics.

**2. Requirement for notification and consent**

A written or electronic consent of the data subject is required when collecting, processing and using personal data. In order to obtain a consent the following conditions must be notified to and agreed with the data subject:

- explicit purpose and objectives;
- data controller's name and contact information;
- list of data to be processed, collected and used;
- duration of the data processing and using;
- disclosure, transfer and revocation conditions.


**3. Transfer of personal data outside of Mongolia**

Transferring personal data outside of Mongolia without a consent of the data subject is prohibited unless otherwise provided in the law or an international treaty to which Mongolia is a signatory. Since the law does not provide exemption to this rule of consent, an intra group transfer (transferring personal data from one group company to another in overseas) would constitute transfer of personal data.

**4. Use of data processors**

Under the PDPL, a data controller is allowed to transfer the obligation to collect and process data to the data processor on a contractual basis.

**5. Data security assessment**

The PDPL requires data controllers and data processors to undertake assessments to ensure data security. Data security assessment is especially required in the following circumstances where the data is collected, processed and used through electronic processing technology:

- in decision making process that affect the rights, freedoms and legitimate interests of the data subject; and
- regular processing of sensitive data.

**6. Requirement to destroy personal data**

Data controllers will need to destroy personal data if requested by the data subject (in case of illegal processing), ordered to do so by relevant authority and as agreed under the consent form or relevant agreement. Data controllers must also destroy personal data if the initial goal of collecting the data has completed.

## Data subject's rights

Right to transfer their personal data

Right to access their personal data

Right to know whether relevant information has been collected, processed or used

Right to demand the disposal of its data under the law

Right to objection

Right to be forgotten

Right to know about a third party who receives their personal data

Right to request to terminate process of data collection, processing and use

Right to give or refuse to give consent to the data controller on a voluntary basis

Right to correct their personal data

Right to obtain a copy of the data related to them from a data controller in a paper or electronic form

Right to file a complaint or comment on the decision made as a result of processing the data etc.

## Data controller's obligations

Key obligations of a data controller in terms of personal data protection include:

to approve and enforce **internal policy** for data collection, processing and use

to obtain the **consent** to collect data upon identification and confirmation of the data subject

to explain clearly and explicitly to the data subject the **purpose and grounds, right to refuse to give a consent** for collecting the data

to **keep records** on data collection, processing and use activities

to **receive, resolve and respond** to the complaint of the data subject

to **undertake assessments** according to the law

**to be liable** to the data subject, the competent authority and a third party under the law

to **correct, change, dispose data** at the request of the data subject and notify the data subject in this regard

to provide free **copies** of data in electronic form at the request of the data subject

to **terminate** the processing and use of data upon receiving the request of the data subject, if it does not affect the rights and legitimate interests of others

to take measures to **ensure information security** according to the law

## Notification and reporting requirements

**Reporting obligations to National Human Rights Commission ("NHRC")**

- Data controllers must maintain a record of actions taken to eliminate a data breach and its negative consequences. This record shall be submitted to the NHRC in January of each year.
- An assessment report shall be submitted to the NHRC and data shall be collected, processed and used using electronic processing technology based on recommendations given by the NHRC.

## Penalties

Following the adoption of the PDPL, the Infringement Law (2017) and Criminal Code (2015) have been amended. The Infringement Law provides sanctions for various violations of the PDPL including but not limited to Illegal collection, processing, transfer or disclosure of sensitive data. Penalty is generally a fine of up to MNT 20,000,000 for legal entities.

A data subject may file complaints to the NHRC for potential human right violations. If the data subject is not satisfied with the NHRC's decision, they may appeal to the courts of Mongolia.

In addition, data subjects are entitled to claim to recover damages incurred by unlawful acts of the data controller.

## Further actions to be taken

**Organizations are recommended to take the following measures to ensure compliance with the PDPL:**

- Procure an impact assessment on data security within the organization subject to assessment regulations to be approved by the Ministry of Digital Development and Communications;
- Conduct gap analysis to ensure compliance with the PDPL;
- Develop or revise the internal policy(s) and/guidelines covering the below matters:
  - personal data collection, processing and use;
  - data security;
  - usage and disposal of data; and
  - anonymization of data.
- Approve a form of consent, privacy statement or data collection terms and other necessary forms;
- Enter into/amend a data processing agreement with customers, vendors and other third parties where relevant;
- Create a registration form for data incidents and maintain record of data breach incidents;
- Approve action plan/ measures to follow in case of data incidents and notification to data subject and respective state authorities;
- Consider prohibited locations and additional requirements surrounding use of audio, video, and audio-visual recording devices;
- Notify the privacy statement and collect consent from the data subjects; and
- Biometric data (fingerprints) collected by the data controller must be disposed by 1 May 2022.

For more in-depth discussion about the key requirements described above, non-compliance risks and any other questions you may have about the PDPL, please do not hesitate to contact us.

For details of the Personal Data Protection Law, please visit https://legalinfo.mn/mn/detail?lawId=16390288615991

pwc.com/mn