

# 蒙古国推行《个人数据保护法》 自2022年5月1日起生效

## 联系我们：

**Michael Ahern**  
合伙人  
税务和法律服务  
michael.ahern@pwc.com

**Tsendmaa Choijamts**  
总监  
税务和法律服务  
tsendmaa.choijamts@pwc.com

**Munkhjargal Ragchaakhuu**  
法务经理  
税务和法律服务  
munkhjargal.ragchaakhuu@pwc.com

**Amarjargal Batchuluun**  
高级顾问  
税务和法律服务  
amarjargal.batchuluun@pwc.com

## PwC Legal LLP

Central Tower, 6<sup>th</sup> floor  
Suite 603, Ulaanbaatar  
14200, Mongolia  
Tel: + 976 70009089  
Fax: +976 11 322068  
[www.pwc.com/mn](http://www.pwc.com/mn)

2021年12月17日，蒙古国议会通过了《个人数据保护法》（“PDPL”），自2022年5月1日起生效。与之前的法案《个人保密法》（1995年）相比，《个人数据保护法》一旦生效，将在蒙古国围绕个人数据设立更广泛和更严格的监管制度。

《个人数据保护法》旨在与《网络安全法》（2021年）、《公共信息透明度法》（2021年）和《电子签名法》（2021年）（均从2022年5月1日起生效）共同规范、并在蒙古国架构管理网络安全和数据隐私保护的框架。我们将重点介绍《个人数据保护法》的关键方面及其对企业的影响。



## 应用

《个人数据保护法》适用于所有在蒙古国无合法身份的个人、法人实体和组织（代表机构和常设机构）收集、处理、使用和保护个人数据。



## 个人数据的范围及定义

### 1. 什么是个人数据？

- 任何可用于直接或间接识别自然人身份的信息，包括但不限于：
  - 敏感的个人数据；
  - 姓名
  - 出生年月及出生地；
  - 居住地址及位置数据；
  - 公民的识别号；
  - 资产和财产；
  - 教育状况；
  - 会员资格和；
  - 网络识别码



### 2. 什么是敏感数据？



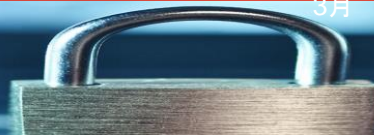
- 个人的种族、肤色、宗教、信仰、健康状况、通信/通讯、遗传和生物特征数据、数字签名私钥、犯罪记录，以及关于自然人的性取向和身份以及性生活的数据。

### 3. 谁是数据主体？

- 由上述信息确定的自然人。

### 4. 谁是数据控制员？

- 依照《个人数据保护法》规定或经数据主体同意收集、处理、使用数据的无合法身份的自然人、法人或组织。

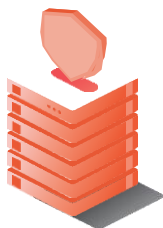


## 推行了新的术语及定义（延续）



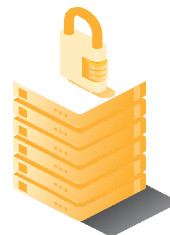
### 数据应用

使用、传输和访问数据



### 数据收集

获取（实现）、收集和注册数据



### 数据处理

对此类活动进行分类、存储、分析、修改、处理、恢复和结合



## 关键要求

### 1. 收集、处理和使用个人数据的法律依据

《个人隐私法》（1995年）长期以来对于是否处理个人数据一直模棱两可（除非“法律规定”允许）以及没有明确规定“同意”要求。《个人数据保护法》规定，无合法身份的法人实体和组织可以在以下情况下收集、处理和使用个人数据：

- 数据主体已同意；
- 按照法律规定行事；
- 在雇佣关系期间必要时；
- 因订立和履行合同需要时；
- 数据已根据法规公开时；和
- 当个人数据已匿名，可用于拟备历史、科学、艺术和文学作品或公开数据和统计资料时。

### 2. 通知和同意的相关规定

当收集、处理和使用个人数据时，需获取数据主体的书面或电子同意书。为获取相关同意书，须通知数据主体并就以下条件达成一致：

- 明确的目的与目标；
- 数据控制员的姓名和联系信息；
- 待处理、收集和使用的数据清单；
- 处理和使用数据所要耗费的时间；
- 数据披露、转移以及撤回的条件。



### 3. 将个人数据转移至蒙古国境外

除非有法规或蒙古国签署的国际条约另有规定，否则禁止未经数据主体同意将个人数据转移至蒙古国境外。由于法律并未对该协议规定提供豁免，因此集团内部转移（将个人数据从一个集团公司转移至海外另一家公司）将构成个人数据转移。

### 4. 数据处理员的使用

根据《个人数据保护法》，数据控制员可以根据合同将收集和处理数据的义务转移给数据处理员。

### 5. 数据安全评估

《个人数据保护法》要求数据控制员和数据处理员进行评估以确保数据安全。在以下通过电子处理技术收集、处理和使用数据的情况下，尤其需要进行数据安全评估：

- 在侵犯数据主体的权利、自由和合法利益的决策过程中；和
- 定期处理敏感数据。

### 6. 销毁个人数据的相关规定

如果数据主体提出相关要求（在非法处理的情况下）、根据相关当局命令并按照同意书或相关协议的约定，数据控制员将需要销毁个人数据。如果收集数据的初始目标已达到，数据控制员也必须销毁个人数据。



### 数据主体的权利

转移其个人数据的权利

访问其个人数据的权利

相关数据是否被收集、处理或使用的知情权

要求依法处置其数据的权利

异议权

被遗忘权

了解接收其个人数据的第三方的权利

要求终止数据收集、处理和使用过程的权利

在自愿的基础上给予或拒绝给予数据控制员同意书的权利

更正其个人数据的权利

以纸质或电子形式从数据控制员处获取与其相关的数据副本的权利

对因处理数据等而做出的决定提出投诉或评论的权利。



### 数据控制员的义务

数据控制员在个人数据保护方面的主要义务包括：

批准和执行数据收集、处理和使用的**内部政策**

在识别及确认数据主体后，获取收集数据的**同意书**

向数据主体明确说明目的和理由，**拒绝同意收集数据的权利**

保存数据收集、处理和使用的记录

接收、解决和回应数据主体的投诉

依法进行评估工作

应数据主体的要求**更正、更改、处置数据**并就此通知数据主体

应数据主体的要求以电子形式免费提供数据副本

在不影响他人权利和合法权益的情况下，应数据主体的要求终止对数据的处理和使用

依法对数据主体、主管部门和第三方负责

依法采取措施，保障信息安全





## 通知和提交报告的相关规定

### 向国家人权委员会提交报告的义务 (“NHRC”)

- 数据控制员必须记录为消除数据泄露及其负面后果而采取的行动。应于每年 1 月将该记录提交予 NHRC。
- 应向国家人权委员会提交评估报告，并根据国家人权委员会的建议，采用电子处理技术收集、处理和使用数据。



## 处罚

继《个人数据保护法》通过后，议会又对《侵权法》（2017 年）和《刑法》（2015 年）进行了修订。《侵权法》对各种违反《个人数据保护法》的行为规定了制裁措施，包括但不限于非法收集、处理、传输或披露敏感数据。对法人实体的罚款通常最高可达 20,000,000 蒙古图格里克。

数据主体可以就潜在的侵犯人权行为向 NHRC 提出投诉。如果数据主体对 NHRC 的决定不满意，他们即可以向蒙古国法院提出上诉。


此外，数据主体有权要求赔偿因数据控制员的非法行为而造成的损失。



## 将采取的进一步行动

### 建议组织采取以下措施，以确保遵守《个人数据保护法》：

- 根据由数字发展和通信部批准的评估规定，在组织内进行数据安全影响评估；
- 进行差距分析，以确保符合《个人数据保护法》；
- 制定或修订涵盖以下事项的内部政策和/指南：
  - 个人数据的收集、处理和使用；
  - 数据安全；
  - 数据的使用和处置；和
  - 数据的匿名化。
- 批准同意书、隐私声明或数据收集条款和其他必要的表格；
- 与客户、供应商和其他相关第三方签订/修订数据处理协议；
- 为数据事故创建登记表格，并维护数据泄露事故的记录；
- 批准在发生数据事故时应采取的行动计划/措施，并通知数据主体和相应的国家当局；
- 考虑使用音频、视频和视听记录设备的禁区和附加要求；
- 通知隐私声明，并征求数据主体的同意；和
- 由数据控制员收集的生物特征数据（指纹）必须在2022年5月1日前销毁。

 如果您需要更深入地讨论上述关键要求、违规风险以及您对《个人数据保护法》可能有的任何其他问题，请随时与我们联系。

有关《个人数据保护法》的详情，请浏览 <https://legalinfo.mn/mn/detail?lawId=16390288615991>

[pwc.com/mn](https://pwc.com/mn)

This Alert is produced by PwC Legal LLP. The material contained in this alert is provided for general information purposes only and does not contain a comprehensive analysis of each item described. Before taking (or not taking) any action, readers should seek professional advice specific to their situation. No liability is accepted for acts or omissions taken in reliance upon the contents of this alert.

© 2022 PricewaterhouseCoopers Legal LLP. PricewaterhouseCoopers Tax TMZ LLC

All rights reserved. In this document, “PwC” refers to PricewaterhouseCoopers Legal LLP, which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.





## 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, 6<sup>th</sup> floor  
Suite 603, Ulaanbaatar  
14200, Mongolia  
Tel : + 976 70009089  
Fax : +976 11 322068  
[www.pwc.com/mn](http://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.

This Alert is produced by PwC Legal LLP. The material contained in this alert is provided for general information purposes only and does not contain a comprehensive analysis of each item described. Before taking (or not taking) any action, readers should seek professional advice specific to their situation. No liability is accepted for acts or omissions taken in reliance upon the contents of this alert.

© 2022 PricewaterhouseCoopers Legal LLP. PricewaterhouseCoopers Tax TMZ LLC  
All rights reserved. In this document, “PwC” refers to PricewaterhouseCoopers Legal LLP, which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.

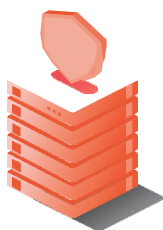


## Introduced new terms and definitions (cont'd)



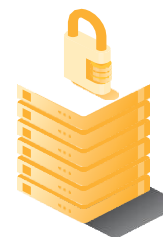
### Data use

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.

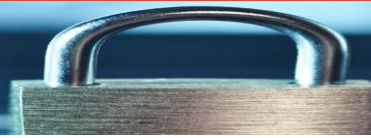
### 5. Data security assessment

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:

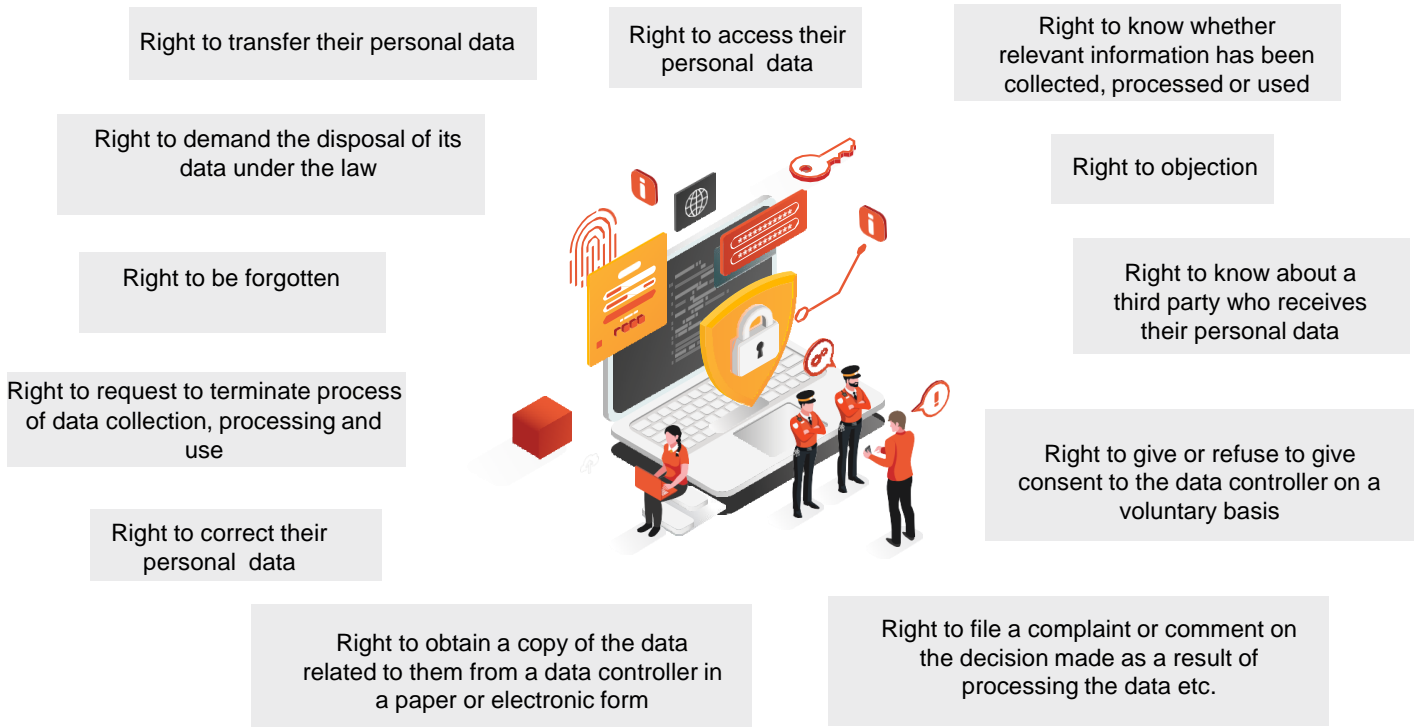
- in decision making process that affect the rights, freedoms and legitimate interests of the data subject; and
- regular processing of sensitive data.

### 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.

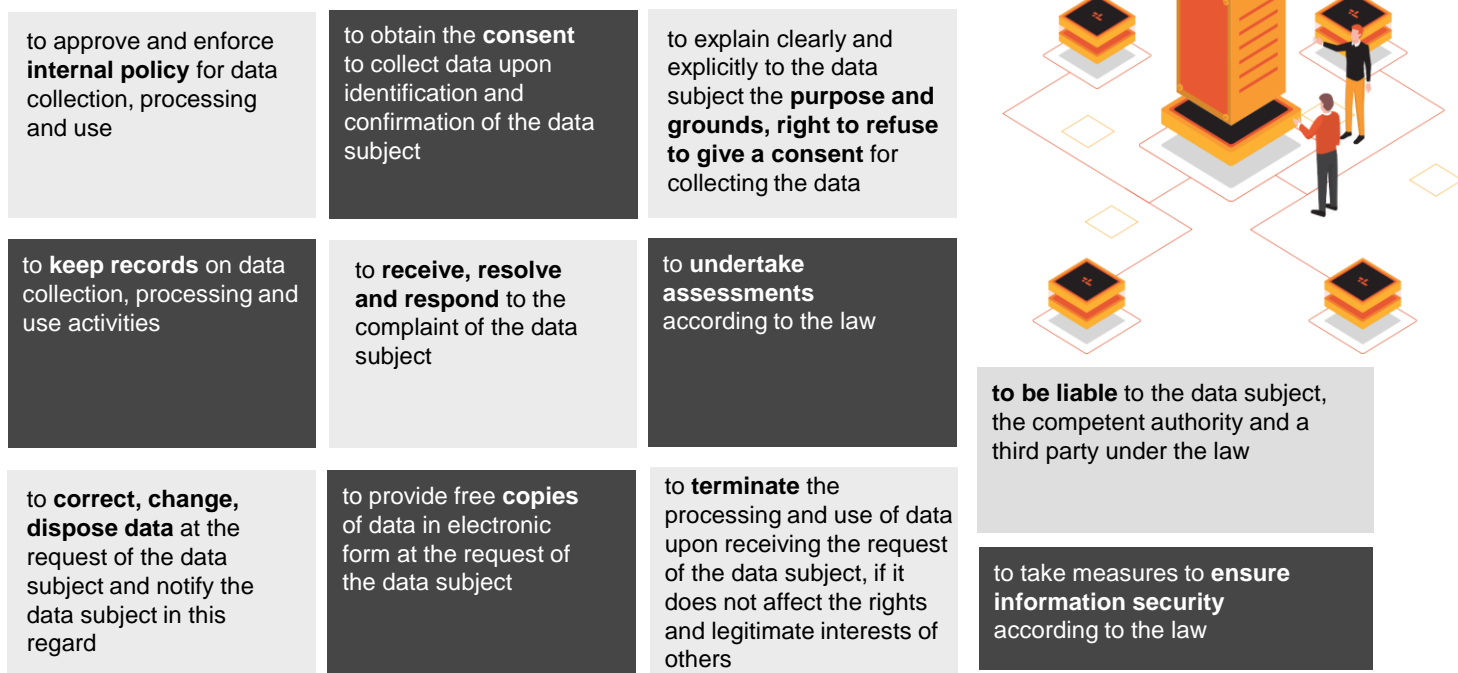


## Data subject's rights



## Data controller's obligations

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





## 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](https://pwc.com/mn)

This Alert is produced by PwC Legal LLP. The material contained in this alert is provided for general information purposes only and does not contain a comprehensive analysis of each item described. Before taking (or not taking) any action, readers should seek professional advice specific to their situation. No liability is accepted for acts or omissions taken in reliance upon the contents of this alert.

© 2022 PricewaterhouseCoopers Legal LLP. PricewaterhouseCoopers Tax TMZ LLC

All rights reserved. In this document, “PwC” refers to PricewaterhouseCoopers Legal LLP, which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.