Country: Mongolia
Jurisdiction: National/Federal
Law Name: Protection of Personal Information

Overview

Type:
Data Protection Law

Description:

Updated 8/8/22

The purpose of this Law is to regulate the Collection, Processing, Use and security of Personal Data. (Article 1)

Scope of Data Covered:

The Law applies to Personal Data.

Exceptions:

The Law does not apply in the following cases:

- to collect, process, use and ensure the security of Personal Data related to a person or family member without violating the person's right to inviolability and freedom;
- to place audio, video and audio-visual recording devices for the purpose of protecting movable and immovable property owned, possessed and used by a person, or protecting the life and health of the person or family member;
- to use a person's Biometric Information for the purpose of protecting and storing movable and immovable property owned, possessed and used by a person;
- disclosure of information to the public.

Relations related to the Collection, Processing, Use and protection of information in the course of executive work must be regulated by the Law on Executive Work.

Relations other than those specified in the Law on Prevention of Crimes and Violations related to the installation of video equipment in order to ensure the safety of public streets, roads, squares, public places and traffic for the purpose of preventing crimes and violations are regulated by this Law.

(Article 3)

Scope of Entities Covered:

The Law regulates the Collection, Processing, Use and security of Personal Data by individuals, legal entities and non-legal entities, as well as public authorities.

This Law also applies the communication related to the Collection, Processing, Use and security of Personal Data with the help of technical tools and software.

(Article 3)

Legal citation:

Protection of Personal Information Law

URL link to text of the Law:

http://parliament.mn/files/147567 (Mongolian)

Effective Date:

May 1, 2022

Compliance Deadline:

Full compliance required as of May 1, 2022.

Key Law Definitions:

Biometric Information: non-overlapping physical data related to the human body, such as fingerprints, iris, face, voice and body movement characteristics that can be identified with the help of equipment, hardware and software.

Correspondence Information: information exchanged using letters, parcels, e-mails, communications and information technology.

Data Collection ("Collection"): the process of obtaining, compiling and registering information.

Data Controller ("Controller"): a person, legal entity or non-legal entity that collects, processes and uses Personal Data in accordance with the Law or with the consent of the Individual.

Data Owner ("Individual"): a person defined by personal information.

Data Processing ("Processing"): the process of classifying, storing, analyzing, modifying, deleting and restoring Personal Data.

Electronic Identifier: the login name of the information system to identify a person in the electronic environment, e-mail, social network, address of wired and wireless technology, other types of devices and information in the information system.

Genetic Information: unique information that reflects the human body, health, and inherited traits determined by biological sampling.

Health Information: information on a person's physical and mental health and access to health care and services.

Personal Information ("Personal Data"): Sensitive Data and the name of a person's parents, first name, date and place of birth, address, location data, civil registration number, education, membership, online Identifier , direct or indirect identification or other identifiable information.

Property Information: information on the property owned, possessed and used by the Individual.

Sensitive Information of a Person ("Sensitive Data"): a person's nationality, ethnicity, religion, beliefs, health, Correspondence, Genetic and Biometric Information, electronic signature, criminal convictions, and information on gender and sexual orientation.

Use of Information ("Use"): the use, transmission and access to information in activities other than the Collection and Processing of information.

(Article 4)

Notice

General Rules:

The Controller must provide the Individual with certain information in order to obtain consent for Processing. (Article 8) Individuals have the right to the information specified in Article 8 of this Law. (Article 16)

Controllers are required to provide the specified information when obtaining permission from the Individual, and to explain to the Individual clearly the purpose and grounds for collecting the Personal Data. (Article 18)

In addition, the Controller must immediately notify the Individual in the following cases:

- where Sensitive Data are used;
- with the consent of the Individual, the Personal Data have been processed on grounds and for purposes other than Processing, and the Personal Data have been transferred to a third party;
- the conditions specified in 8.2 (see Required Content below) of this Law have changed since the Personal Data of the Individual were collected.

(Article 21)

Language Requirement:

Not specified

Required Content:

To obtain the Individual's consent, he Controller must provide the Individual with the following information:

- the grounds and purpose of Collection, Processing and Use must be clear and unambiguous;
- the name of the Controller and contact information;
- a list of Personal Data to be processed and used;
- the duration for Processing and Use;
- whether Personal Data will be disclosed to the public;
- whether Personal Data will be transferred to others and, if so, the recipient, the type and content of the data to be transmitted; and
- conditions for revocation of the consent.

(Article 8)

In addition, Controllers are required to explain to the Individual:

- the right to refuse to give consent to collect Personal Data;
- the right to file a complaint related to the Collection, Processing and Use of Personal Data;
- the consequences that may arise if the Individual does not give permission to collect information;
- the consequences with regard to decisions made as a result of automated decision making;

Controllers are responsible for providing to the Individual, upon request, information on Processing and Use activities.

(Article 18)

Timing:

Not specified

Delivery Method:

Not specified

Additional Information:
None

Consent

General Rules:

Personal Data may be processed with the Individual's written consent. (Articles 7-8)

The Controller must obtain permission from the Individual, except in cases provided by law. The Controller must provide the Individual with certain information in order to obtain permission. (See Notice section) (Article 8)

An Individual's non-response in providing consent to collect Personal Data, and the expiration of the time limit or the usual reasonable time for such response, must not be a ground for considering the permission to collect Personal Data. (Article 8)

The Individual may revoke consent at any time and the Processing of the data made before the receipt of the request for revocation must remain lawful if it does not violate this Law. (Article 8) Withdrawal of consent must be in an easy and understandable manner without causing any inconvenience to the Individual. (Article 18)

The Controller must prove that he/she has obtained the consent of the Individual when collecting Personal Data. (Article 8)

If the Controller processes or uses the Personal Data for purposes other than the purpose for which they were originally obtained, the Controller must obtain consent from the Individual again. (Article 8)

Consent Obligations For Specific Uses of Non-Sensitive Data:

To Provide Product or Service or Manage Relationship:

Internal Use

Consent or another legal basis such as contractual necessity is required to use Personal Data in order to provide a product or service. (Article 7)

Affiliate Sharing / Third Party Sharing

A separate consent is required to share Personal Data with affiliates and third parties unless the Individual has consented to the Processing by the Controller and the Individual was informed of the transfers and the recipients in the notice that was provided at the time consent was requested for the Processing. (Article 8)

To Use for Marketing Purposes:

Internal Use

Consent or another legal basis is required to use Personal Data for marketing purposes. (Article 7)

Affiliate Sharing / Third Party Sharing

A separate consent is required to share Personal Data with affiliates and third parties for marketing purposes unless the Individual has consented to the Processing by the Controller and the Individual was informed of the transfers and the recipients in the notice that was provided at the time consent was requested for the Processing. (Article 8)

To Share with Government Authorities/Regulators:

Consent or another legal basis is required to share with government authorities. (Article 7)

To Share with Service Providers:

Controllers may transfer the obligation to collect and process Personal Data to a Processor on a contractual basis. (Article 19). See section on Disclosures to Third Party Service Providers.

Consent Obligations for Collection, Use and Disclosure of Sensitive Data:

Sensitive Data about Health, Correspondence, Genetic and Biometric Information, electronic signature, and information on gender and sexual orientation is considered to be confidential information.

The Law prohibits the Collection, Processing or Use of Sensitive Data except where an Individual has provided written consent or another legal basis specified under the Law applies. See exceptions below and Collection and Use/Legal Basis section.

(Article 9)

Language:

Not specified

Consent Format:

Consent must be in writing (paper or electronic form). Consent in electronic form must be issued by identifying and certifying it electronically by means specified in the law or accepted by the Individual. (Article 8)

Exceptions:

Personal Data

Consent is not required to process non-sensitive Personal Data in the following cases:

- on the grounds specified in the Law;
- in cases provided by law, in the course of labor relations, the Controller exercise his/her rights and fulfill his/her duties;
- enter into an agreement and ensure the implementation of the concluded agreement;
- where the Personal Data are publicly available (in accordance with the law); or
- where the Personal Data are used to create historical, scientific, artistic, and literary works, prepare (anonymized) open data and statistical information.

(Articles 6-7)

Sensitive Personal Data

Consent is not required to process Sensitive Data in the following cases:

- in order to protect the health of the person and others and to provide health services, a health worker must exercise his/her rights and responsibilities specified in the law;
- to provide explanations, declarations and evidence in accordance with the law on claims of citizens and legal entities;
- on the grounds specified in the Law;
- in cases provided by law, in the course of labor relations, the Controller may exercise its rights and fulfill its duties;
- enter into an agreement and ensure the implementation of the concluded agreement;
- where the Personal Data are publicly available (in accordance with the law); or
- where the Personal Data are used to create historical, scientific, artistic, and literary works, prepare (anonymized) open data and statistical information.

(Articles 9, 6-7)

Additional Information:

Consent must be obtained from the legal representative of a citizen to collect information specified in Articles 16, 17, 18 and 19 of the Civil Code. (Article 8)

The consent of the Individual must not be required for the purpose of Collection for the purpose of identifying the interrelated persons specified in Article 4.1.6 of the Competition Law of the participants in the procurement of goods, works and services with state and local funds. (Article 8)

Collection and Use

General Rules:

A legal basis is required to collect, process, and use Personal Data. (See legal bases subsection below.) (Article 7)

The following principles must be followed for the Collection, Processing and Use of Personal Data:

- not to violate human rights and freedoms;
- respect of human rights and legitimate interests;
- nondiscrimination;
- collect, process and use Personal Data pursuant to consent or another legal basis specified under the Law;
- ensure information security;
- not to compromise the accuracy and integrity of the information.

(Article 5)

Controllers are responsible for verifying the Personal Data with the original of the information holder's ID card or equivalent document, or with the Personal Data sent electronically or in the database. (Article 18)

The Collection, Processing, and Use of Personal Data for purposes other than those specified in the Law and for the purpose of obtaining the Individual's consent is prohibited. (Article 29)

Deceased Individuals

Unless otherwise provided by law, if the Individual has died or is considered dead, the relevant Personal Data must be collected, processed and used with the written consent of the testator, his/her family member or legal representative.

Unless otherwise provided by law, consent to collect, process and use Sensitive Data will not be required 70 years after the death of the Individual.

(Article 13)

Legal Basis for Collection and Use:

Consent

Personal Data and Sensitive Day may be processed with the written consent of the Individual. (Articles 7, 9)

Necessary to Complete the Contract

Personal Data and Sensitive Personal Data may be processed in order to enter into an agreement and ensure the implementation of the concluded agreement. (Articles 7, 9)

Necessary to Comply with a Legal Requirement

Personal Data and Sensitive Personal Data may be processed on the grounds specified in the law. (Articles 7, 9)

Balance of Interest (e.g., Legitimate Interests of the Controller)

Not specified

Vital Interest

Not specified

Where Permissible by Law

Personal Data and Sensitive Personal Data may be processed on the grounds specified in the Law. (Articles 7, 9)

Other

- Personal Data may be collected and processed in cases provided by law, in the course of labor relations, for the Controller to exercise his/her rights and fulfill his/her duties;
- Legal entities, individuals, and non-legal entities may collect and process Personal Data that are disclosed to the public in accordance with the law;
- Legal entities, individuals, and non-legal entities may collect and process anonymized Personal Data to create historical, scientific, artistic and literary works and prepare anonymized statistical information.

(Article 7)

- Sensitive Personal Data may be collected and processed in the following cases:
    - in order to protect the health of the person and others and to provide health services, a health worker must exercise his/her rights and responsibilities specified in the law;
    - to provide explanations, declarations and evidence in accordance with the law on claims of citizens and legal entities;
    - in cases provided by law, in the course of labor relations, the Controller may exercise its rights and fulfill its duties;
    - where the Personal Data are publicly available (in accordance with the law); or
    - where the Personal Data are used to create historical, scientific, artistic, and literary works, prepare (anonymized) open data and statistical information.

(Articles 9, 6-7)

Purposes of Use:

Biometric and Genetic Information

With the consent of the employee, the employer may use his/her Biometric Information other than non-identifiable Personal Data (fingerprints) in order to facilitate the process of identifying and verifying the employee in accordance with the internal labor regulations established in accordance with the Labor Law. Employers are prohibited from modifying or transferring such Personal Data to other persons.

The information officer must ensure the safety of the Collection and Use of Biometric and Genetic information Collection.

(Article 10)

History, Research, Art and Literature / Statistical Data

Where anonymized Personal Data are used for the purpose of creating historical, scientific, artistic and literary works and preparing statistical information, such use does not require the written consent of the Individual. However, where such data are not anonymized, the written consent of the Individual is required unless otherwise provided by law.

Regardless of the purpose of Collection, Personal Data may be processed and used for the purpose of creating historical, scientific, artistic and literary works and preparing statistical information.

The rights and legitimate interests of the Individual and others may not be violated when compiling historical, scientific, artistic and literary works and preparing statistical information.

Provisions pertaining to the right to give or revoke consent, receive information/notice, or obtain access (Articles 16.1.1, 16.1.2 and 16.1.3) do not apply when Processing and Using information for the purposes of creating historical, scientific, artistic and literary works and preparing statistical information.

Security measures must be taken in accordance with this Law when Processing and Using information for the purpose of creating historical, scientific, artistic and literary works and preparing statistical information.

(Article 11)

Collection, Processing and Use of Personal Data for Journalistic Purposes

Personal Data may be collected, processed and used for journalistic purposes with the consent of the Individual or in order to protect the public interest.

It is prohibited to collect, process and use information on Health, Correspondence, Genetics, Biometrics, sexual orientation and sexual intercourse for journalistic purposes without the consent of the Individual.

The rights and legitimate interests of the Individual and others may not be violated when collecting, processing and using information for journalistic purposes.

(Article 12)

Automated Individual Decision Making

Personal Data may be collected, processed and used using electronic Processing technology without the participation of the Controller, and an assessment must be made in the following cases:

- to make decisions that may affect the rights, freedoms and legitimate interests of the Individual to be processed in electronic form without human intervention;
- regularly process Sensitive Data.

The assessment must be submitted to the National Human Rights Commission and data must be collected, processed and used using electronic Processing technology based on recommendations.

The methodology and procedure for conducting the assessment must be approved by the state administrative body in charge of communications based on the proposal of the National Human Rights Commission.

(Article 23)

Violations of the rights and freedoms of the Individual as a result of automated Processing is prohibited. (Article 29)

Video Surveillance

Audio, video and audio-video recording systems consist of fixed and mobile video recording equipment, data transmission network and storage devices that can collect, store and use audio, video and audio-visual information with the help of technology. Audio, video and audio-visual recording equipment must consist of stationary and mobile video recording equipment capable of collecting, transmitting and storing audio, video and audio-visual information with the help of technology.

Unless otherwise provided by law, a video recording device may be installed for the following purposes:

- to protect the safety of residents at the entrances and exits of public housing and common areas, and to ensure the integrity of common property;
- to protect human and information security in the workplace and ensure the integrity of the organization's property;
- to collect, process, use and analyze traffic information.

Unless otherwise provided by law, the following activities are prohibited when installing or using video recording equipment:

- to place video equipment in a location that clearly violates the right to liberty and security of person, such as bathrooms, dressing rooms, special purpose service rooms of public service centers, karaoke, hotel rooms, and inpatient rooms for providing health care and services;
- to install video recording equipment covering the entrances and exits of households and households residing in public apartments;
- distribute video footage of public housing through visual media;
- to show and copy the video if the video contains information of other than the Individual's information.

The Law prohibits placing audio and video recording devices in the places specified in Articles 27.3.1 (public housing and common areas), 27.4.1 (a location that clearly violates the right to liberty and security of person, such as toilets, dressing rooms, etc.) and 27.4.2 (entrances/exists of households in public apartments) of this Law.

Warnings on audio, video and audio-visual recording devices must be posted so that citizens can see them without any obstacles.

The state administrative body in charge of communications must determine the information to be reflected in the requirements and warnings for the audio, video and audio-visual recording system based on the proposal of the National Human Rights Commission.

The National Human Rights Commission may conduct inspections in cooperation with law enforcement agencies in order to monitor the activities specified in Articles 27.3 and 27.4 of this Law and the lawful use of audio, video and audio-visual recording systems used under other laws.

In accordance with the procedures set forth in the Law, the Controller may review, access, display, listen to and copy the stored information in the audio, video and audio-visual recording system.

The audio, video and audio-visual recording system must create technical and operational conditions to prevent access to information by unauthorized persons.

In case of obtaining audio, video, audio-visual recordings as evidence of a crime or violation, the grounds and procedures specified in the relevant law must be followed.

(Article 27)

Additional Information:
None

Disclosures to Third Party Service Providers

General Rules:

The Controller may transfer the obligation to collect and process Personal Data to a Processor on a contractual basis. Such contract specified must specify the purpose of Collection and Processing, the term of the contract, the classification of information and the conditions for protecting the rights of the Individual. (Article 19)

A Processor who has taken over the responsibility of Collection and Processing of Personal Data must have the following responsibilities:

- to collect and process Personal Data under the supervision of the Controller within the permission given by the Individual;
- to correct, change or delete the Personal Data of the Individual in accordance with the duties, directions and instructions given by the Controller;
- to provide information to the Controller related to Collection and Processing;
- if the purpose of Collection and Processing has been achieved, return the information and results of Processing to the Controller within the period specified in the contract without leaving a copy, and destroy the information obtained for Processing without re-use;
- to store Personal Data obtained in the course of Collection and Processing;
- to take security measures in accordance with Article 20 of the Law;
- to perform the duties and instructions given by the Controller.

Subcontracting

Unless otherwise provided in the contract, the Processor is prohibited from transferring its obligations to another entity and the contract must clearly state the responsibilities of the Processor in case of transfer. (Article 19)

Additional Information:

Violation of the duties, directions and instructions given to the Processor by the Controller must not serve as a ground to release the Controller from the obligations and responsibilities to the Individual.

If the Controller has not transferred the obligation to collect and process information to the Processor on a contractual basis, it must perform the duties specified in Articles 18 and 19 (i.e., responsibilities of the Controller and Processor) of this Law.

(Article 19)

Disclosures to Third Parties

General Rules:

A separate consent is required to transfer Personal Data to third parties unless the consent obtained by the Controller at the time of Collection is based on a notice that sets forth the purposes of the Processing and specifically includes the envisioned transfers and recipients identified in the notice. See Consent section for information regarding the rules applicable to the provision of consent. (Article 8)

Individuals have the right to know about a third party who has transferred or is about to transfer Personal Data related to the Individual to another third party. (Article 16)

DPA Authorization:

Not specified

Special Rule for Joint Controllers:

Not specified

Additional Information:
None

Access and Correction Obligation

General Rules:

Individuals have access, correction, erasure, objection, cancellation, and data portability rights. In addition, Individuals have the right to file a complaint or request explanation on the decision made as a result of Processing. (Article 16)

Access Rules:

Individuals have the right know whether relevant Personal Data have been collected, processed or used. Individuals also have the right to obtain a copy of the relevant data from the Controller, in paper or electronic form. (Article 16)

Controllers must provide a copy of the Personal Data in electronic form, free of charge, at the request of the Individual. (Article 18)

Contact For Access Requests:

Not specified

Timeframe For Responding To Access Requests:

Not specified

Access Exceptions:

Not specified

Correction Rules:

Individuals have the right to notify the Controller about the correction of erroneous information, make changes and provide additional information. (Article 16)

Individuals must ensure the accuracy of information related to him/her. Individuals must notify the Controller about the correction of erroneous information, to make changes and provide additional information. (Article 17)

Controllers must correct, change, delete the Personal Data at the request of the Individual and notify the Individual. (Article 18)

Timeframe for Responding to Correction Requests:

Not specified

Correction Exceptions:

Not specified

Language Requirement:

Not specified

Additional Information:

Right to Erasure ("Right to be Forgotten")

Individuals have the right to request the destruction of his/her Personal Data in accordance with the Law. Individuals also have the right to demand that Personal Data be destroyed if the data are prohibited from being collected in accordance with the legislation. (Article 16)

Controllers must delete the Personal Data at the request of the Individual and notify the Individual. (Article 18)

Right to Object

Individuals have the right to voluntarily refuse to give consent to collect Personal Data. (Article 16)

Controllers must terminate the Processing and Use of Personal Data after receiving an Individual's request, provided that it does not affect the rights and legitimate interests of others. (Article 18)

Right to Cancellation

Individuals have the right to request cancellation in the course of Collection, Processing and Use. Individuals must notify the Controller in writing in making such request. (Article 16)

Right to Data Portability

Individuals have the right to provide a copy of the Personal Data held by the Controller to another person. (Article 16)

Individuals have the responsibility to not violate the rights and freedoms of others and not to infringe on legitimate interests while exercising their data portability rights. (Article 17)

Security

General Rules:

The Controller and Processor must take the following organizational and technical measures to ensure information security:

- approve and follow internal procedures to ensure information security in accordance with the Law's requirements;
- measures to be taken in case of Personal Data loss and the plan to deliver information to the Individual and relevant government organizations must be approved in accordance with the Law;
- take all measures to ensure the integrity, confidentiality and accessibility of the information system used for Collection, Processing and Use;
- approve and follow certain procedures and instructions on restricting the use of Personal Data, deleting Personal Data and making it impossible to identify the individual;
- evaluate to ensure the security of data Processing activities.

The state administrative body in charge of communications must determine the requirements for information security, instructions for assessment and requirements for storage technology when Collecting, Processing and Using information

(Article 20)

Compliance with the information security requirements established by the government for Processing Sensitive Personal Data, Genetic and Biometric Information will not serve as a ground for exemption from liability for information loss. (Article 10)

Risk Assessment:

The Controller and Processor must take certain organizational and technical measures to ensure information security, which include conducting an assessment in order to ensure the security of data Processing activities. (Article 20)

Information Security Program:

See General Rules

Physical Security:

See General Rules

Electronic Security:

See General Rules

Encryption:

See General Rules

Disposal:

See General Rules

Service Provider Supervision:

The Controller may transfer the obligation to collect and process Personal Data to a Processor on a contractual basis. Such contract specified must specify the purpose of Collection and Processing, the term of the contract, the classification of information and the conditions for protecting the rights of the Individual. (Article 19) (See section on Disclosures to Third Party Service Providers)

Employee TrainingAwareness:

Not specified

Security OfficerManager:

Not specified

Other:
None

Exceptions:
None

Additional Information:
None

Security Breach

General Rules:

The Processor must notify the Controller as soon as it becomes aware of the violations revealed during data Collection and Processing. If the violation harms the rights and legitimate interests of the Individual, the Controller must immediately notify the Individual.

The Controller must keep a record of the response taken to eliminate the violation and its negative consequences. This record must be submitted to the National Human Rights Commission annually and upon its request.

(Article 22)

Types of Records Covered:

Paper or electronic records that contain Personal Data.

Covered Information:

All Personal Data

Notice Trigger:

Notice to Individuals must be provided if the violation harms their rights and legitimate interests. (Article 22)

Notice to Individuals:

Content

Notice must contain the following information:

- the affected Individual and the record of the information;
- name and contact information of the Controller;
- the violation and its possible negative consequences;
- the response taken to eliminate the violation and its potential negative consequences.

(Article 22)

Timing

Not specified

Notice to Government:

The Controller must keep a record of the response taken to eliminate the violation and its negative consequences. This record must be submitted to the National Human Rights Commission annually and upon its request. (Article 22)

Note. While the Law does not expressly provide that notifications regarding data breaches must be provided to the government, Article 25 authorizes the state central administrative body in charge of e-development and communications to receive and register the notification submitted by the Personal Data Officer on the loss of security of the information system for the purpose of Collecting, Processing and Using Personal Data and being affected by the cyber attack, and to take necessary measures immediately. (Article 25)

Notice Content

Not specified.

Timing

Annual reports required.

Delay for Law Enforcement Investigations

No requirements specified

Notice to Credit Reporting Agencies:

Not specified

Notice by Service Provider:

The Processor must notify the Controller as soon as he/she becomes aware of the violations revealed during data Collection and Processing. (Article 22)

Substitute Notice:

Not specified

Exceptions:

Not specified

Enforcement Authority:

National Human Rights Commission

Language Requirement:

Not specified

Additional Information:

The Individual must have the right to file a complaint to the relevant authority in accordance with the law if he/she considers that the violation harms his/her rights and legitimate interests. (Article 22)

Cross Border Limitations

General Rules:

The Law prohibits cross-border transfers, except as provided by law, international treaties to which Mongolia is a party, or with the consent of the Individual. (Article 14)

DPA Authorization:

Not specified

Additional Information:
None

Database Registration

General Rules:

No requirements specified; however, see record-keeping requirements below.

Database Registration Requirements:
None

Level of Reporting Required:

Controllers are required to keep records on Collection, Processing and Use, and to store information obtained in the course of data Collection, Processing and Use. (Article 18)

Cross Border Transfers:
None

Whistleblowing Programs:
None

Language Requirement:
None

Additional Information:
None

Data Privacy Officer

General Requirements:

The Law sets forth responsibilities for a Personal Data Officer. (Article 18) See section below on duties and responsibilities.

While the Law does not expressly provide that notifications regarding data breaches must be provided to the government, Article 25 authorizes the state central administrative body in charge of e-development and communications to receive and register the notification submitted by the Personal Data Officer on the loss of security of the information system for the purpose of Collecting, Processing and Using Personal Data and being affected by the cyber attack, and to take necessary measures immediately. (Article 25)

QualificationsLocation:

Not specified

Duties Responsibilities:

The Information Officer has the following responsibilities:

- approve and enforce procedures for the Collection, Processing, and Use of Personal Data in accordance with the Law;
- obtain permission to collect Personal Data about the Individual in accordance with the Law or on the basis of identifying and certifying the Individual with his/her ID card or similar document;
- provide the required information when requesting consent from the Individual, explain clearly the purposes and legal bases for the Collection;
- explain to the Individual about their objection right and the right to file a complaint related to the Collection, Processing, and Use of Personal Data;
- explain the consequences that may arise if the Individual does not consent to the Collection;
- make a decision as a result of automated Processing and explain to the Individual the consequences of such Processing;
- verify the Personal Data with the original of the Individual's ID card or equivalent document or with the data sent electronically or in the database;
- provide information on Processing and Use activities in response to a request from the Individual;
- correct, change, or delete data at the request of the Individual and notify the Individual accordingly;
- terminate the Processing and Use after receiving a request from the Individual, provided it does not affect the rights and legitimate interests of others;
- provide a copy of the information in electronic form free of charge upon request of the Individual;

- keep records on data Collection, Processing and Use activities;
- store the information obtained in the course of data Collection, Processing, and Use;
- receive, resolve, and respond to complaints from Individuals; and
- be liable to the Individual for the Collection, Processing, and Use of Personal Data, to the competent authority and third parties in cases provided by law.

(Article 18)

Additional Information:
None

Audits

Internal Audits:

The Controller and Processor must follow organizational and technical measures to ensure information security, which include conducting an assessment in order to ensure the security of data Processing activities. (Article 20)

DPA Audits:

Not specified

Additional Information:
None

Internal Policy

General Rules:

The Controller and Processor must follow organizational and technical measures to ensure information security, which include approving internal regulations to ensure information security and follow those regulations in its activities. (Article 20)

Language Requirement:
None

Additional Information:
None

Data Retention Destruction

General Rules:

The Controller must destroy the Personal Data Collected, Processed and Used in the following circumstances:

- at the request of the Individual, if the data have not been Collected, Processed or Used in accordance with the grounds and procedures specified in the Law;
- by the law, international treaties of Mongolia and a court decision that has entered into force, where the Controller has been required to destroy the information;
- information other than collected in accordance with the law have achieved the purpose for which they were originally collected, or specified in the contract;
- otherwise as specified in the Law.

Unless otherwise provided by law, it is prohibited to destroy information on grounds other than those specified above.

(Article 15)

Additional Information:
None

Data Quality

General Rules:

The principles that must be followed for the Collection, Processing and Use of Personal Data include not compromising the accuracy and integrity of the information. (Article 5)

Additional Information:
None

Whistleblowing

General Rules:

No requirements specified; however, the general rules for Processing Personal Data would apply.

Additional Information:
None

Works Council/Labor Unions Obligations

General Rules:

There is no requirement under the Law to consult with Works Councils on data privacy matters.

Additional Information:
None

National Identification Numbers

General Rules:

No requirements specified

Definition of National ID:
None
Prohibitions:
None
Exceptions:
None
Safeguards:
None
Additional Information:
None

Dispute Resolution

General Rules:

Individuals have the right to file a complaint or request explanation on the decision made as a result of Processing. (Article 16)

Controllers are required to receive and resolve the complaint of the Individual and respond to it. (Article 18)

Complaints related to the Collection, Processing and Use of information by the Controller must be submitted to the competent authority or the National Human Rights Commission for resolution.

If the Individual does not agree with the decision, he/she may appeal to the court.

(Article 28)

Language Requirement:

Not specified

Additional Information:
None

Responsible Regulatory/Enforcement Authority (Authorities)

Name:

National Human Rights Commission ("Commission" or "DPA")

The Commission has the following responsibilities under the Law:

- to monitor the implementation of the legislation on protection of Personal Data, to organize public awareness and advocacy activities, to submit recommendations and requirements to relevant organizations in this regard, and to comment on relevant regulations;
- to monitor the activities of the Controller and submit recommendations and requirements;
- if it is considered that in the course of Collecting, Processing, Using and protecting information, human rights and freedoms protected by this Law have been infringed or potentially infringed, complaints and information must be received and investigated or resolved on its own initiative, and to submit recommendations and requirements to the relevant authorities on this issue;
- to provide legal assistance to relevant organizations in the field of Collection, Processing, Use and protection of Sensitive Data;
- to receive and review the records submitted by the Controller on the violations detected in the Collection, Processing and Use of information and the measures taken to eliminate its negative consequences, and make recommendations on further issues to be considered;
- to make recommendations for the purpose of preventing violations of human rights and freedoms in the process of Collecting, Processing and Using information using electronic Processing technology in accordance with Article 23 of this Law;
- include information on Personal Data protection activities, violations, and implementation of Personal Data rights in the report on human rights and freedoms in Mongolia.

(Article 24)

Information Protection in Cyberspace / Communications Administrative Body

The state administrative body in charge of e-development and communications must exercise the following powers:

- ensure the implementation of the legislation on protection of Personal Data, to advertise to the public, to cooperate with relevant organizations, to provide professional and methodological assistance;
- approve technological safety requirements and procedures to be followed in processing Sensitive Data, Biometric and Genetic information;
- receive and register the notification submitted by the Personal Data Officer on the loss of security of the information system for the purpose of Collecting, Processing and Using information and being affected by the cyber attack, and to take necessary measures immediately.

(Article 25)

Other State Information Protection Authority of the Organization

The state organization must monitor the Collection, Processing and Use of Personal Data by the Controller within the scope of its functions specified in the relevant legislation.

(Article 26)

Contact InformationAddress:

National Human Rights Commission of Mongolia
5th floor, Government Building 11
Independence Square, Chingeltei District, Ulaanbaatar, Mongolia
info@nhrcm.gov.mn
70 000 222
51-262786

URL:

https://en.nhrcm.gov.mn

Penalties

Criminal Sanctions:

A person or legal entity that violates this Law must be subject to liability specified in the Criminal Code or the Law on Violations. (Article 30)

Article 135 the Criminal Code provides that violation of the inviolability of secrecy of private correspondence is punishable by a fine equal to 20 to 50 amounts of minimum salary or by incarceration for a term of 1 to 3 months. Similarly, Article 136 provides that intentional disclosure of a citizen's private secrets protected by law learnt in the course of official or professional activities is punishable by a fine equal to 20 to 50 amounts of minimum salary or by incarceration for a term of 1 to 3 months.

AdministrativeCivil Penalties:

None specified for non-governmental entities.

Private Right of Action:

If the Individual considers that his/her rights and freedoms specified in this Law and international treaties of Mongolia have been violated, he/she must have the right to protect his/her rights and to compensate for illegal damage and non-pecuniary damage. (Article 16)

Additional Information:
None

Level of Enforcement

Overview:

The Law entered into force on May 1, 2022.

Additional Information:
None

References

References:
None

Implementing Regulation(s)

Implementing Regulations:
None