DRAFT LAW ON PERSONAL DATA PROTECTION

CHAPTER 1
GENERAL PROVISIONS

Article 1.- Purpose

This law establishes the principles, rules and mechanisms of processing personal data with responsibility, transparency and adherence to ethical conducts, with the aim of protecting the rights of data subjects and promoting the investment environment, competition, and the development of national and international trade in the context of the digital economy and society.

Article 2.- Scope

This Law is a basic law that applies to the processing of personal data through automated or non-automated means, which form the filing system by:

a- Data controllers and data processors located in the Kingdom of Cambodia, regardless of the purposes.

b- Data controllers and data processors located outside the Kingdom of Cambodia for the purpose of supplying goods or services to data subjects or monitoring activities related to data subjects residing in the Kingdom of Cambodia.

This law does not apply to the processing of personal data by:

a- Public authorities performing functions within their jurisdiction.

b- Natural person acting only for personal or household activities.

Article 3.- Definition

The key terms used in this law are defined in the glossary attached hereto.

CHAPTER 2
COMPETENT INSTITUTION

Article 4.- Ministry of Post and Telecommunications

Ministry of Post and Telecommunications has the authority to manage personal data protection and shall have duties as follows:

a- Regulate, audit and monitor the protection of personal data in accordance with the provisions of this law;

b- Have the power to instruct data controllers and data processors to provide personal data or information necessary to perform its functions and duties;

c- Have right to access all personal data and information necessary to perform its functions and duties;

d- Receive complaints and mediate disputes related to the protection of personal data;

e- Promote and raise awareness of personal data protection;

f- Cooperate and exchange information related to personal data protection with national and international ministries and institutions;

g- Monitor the evolution of works related to the personal data protection;

h- Manage the cross-border transfer of personal data by monitoring and restricting or permitting the cross-border transfer of personal data

i- Perform other duties as assigned by head of the Royal Government.

Article 5.- Personal Data Protection Unit

If necessity, the Minister of post and telecommunications may request a decision from the Royal Government to establish a Personal Data Protection Unit, which is a legal entity under public law.

CHAPTER 3
PROCESSING OF PERSONAL DATA

Article 6.- Principles for Processing Personal Data

All processing of personal data shall be carried out in accordance with the following principles:

a- Personal data shall be processed lawfully, fairly and transparently. (lawfulness, fairness and transparency)
b- Personal data shall be collected only for specific, explicit, and legitimate purposes, and shall not be further processed in a manner that is incompatible with those original purposes, except for processing carried out for archival purposes in the public interest, or for scientific, historical, or statistical research, in accordance with relevant data protection guidelines. (purpose limitation)
c- Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. (data minimization)
d- Personal data that needs to be processed shall be accurate and, where necessary, kept up to date. Personal data that is incorrect shall be erased or rectified without delay through reasonable means in accordance with the purposes for which they are processed. (accuracy)
e- Personal data shall be kept in a form which permits identification of data subjects for the necessary period, except for the processing of personal data for archiving purposes in the public interest or for scientific or historical research purposes or for statistical purposes in accordance with the Data Protection Directive or for the performance of an obligation under applicable law. (storage limitation)
f- Personal data must be processed in a manner that ensures the security of personal data in accordance with technical measures and personal data management measures as stipulated in Article 39 of this Law.

The data controller shall be responsible for, and be able to demonstrate compliance with the principles for processing of personal data as determined in this article.

Article 7.- Legal Basis for Processing Personal Data

The processing of personal data shall be based on one of the following legal basis:

a- Consent of the data subject.
b- The necessity of performing a contract to which the data subject is a party, or at the request of the data subject prior to entering into a contract.
c- The necessity of the data controller to perform legal obligations as required by law.
d- The necessity for the protection of the vital interests of the data subject or another natural person.
e- The necessity for the purposes of the performance of a task carried out in the public interest.
f- The necessity for the purposes of legitimate interests pursued by the data controller or a third party.

Article 8.- Consent of the Data Subject

The processing of personal data based on point (a) of Article 7 of this law requires the notification of the purpose of the processing and shall receive the explicit consent of the data subject for that purpose. The data controller shall be required to demonstrate that the data subject has given consent to the processing of personal data in compliance with the provisions of this law.

The notification to the data subject shall comply with the following conditions:

a- It shall be in an easily understandable form and clear.
b- It shall be provided prior to the processing of personal data.
c- The purpose of processing personal data must be specified and appropriate, and information related to that purpose must be provided.
d- It shall specify the right to withdraw consent and other rights of the data subject as determined under this law.
e- It shall provide information regarding the data controller's personal data protection officer or other representative if any, in case the data subject requests further information or explanation.

In the case of the processing of personal data of a data subject under the age of 16 (sixteen) years, the consent of data subject's parent or guardian is required. In this case, the data controller shall verify and confirm the consent of the parent or guardian through the available technology or the other feasible means.

The data subject shall have the right to withdraw consent to the processing of personal data for any specific purposes at any time by notifying the data controller. The data controller shall make it easy to withdraw consent. Upon receipt of the notification for withdrawal of consent, the data controller shall notify the data subject of the consequences of such withdrawal and shall cease the processing of personal data immediately. The withdrawal of consent shall not apply retroactively to the prior processing of personal data based on the previous consent.

Article 9.- The Necessity for the Performance of a Contract or to Entering into a Contract

The processing of personal data based on point (b) of Article 7 of this law shall be necessary for the performance of a contract to which the data subject is a party or at the request of the data subject prior to entering into a contract. Such necessity shall be applied strictly, taking into account the nature and purpose of the contract and in compliance with the principles of processing of personal data as stipulated under Article 6 of this law.

The processing of personal data based on the performances of a contract shall terminate in accordance with the terms and conditions agreed by the parties to contract.

Article 10.- Necessity for Compliance with a Legal Obligation

The processing of personal data based on point (c) of Article 7 of this law shall be necessary for the performance of a legal obligation required by law. In such case, the data controller shall bear the burden of demonstrating the legal provisions with which it is required to comply.

Article 11.- Necessity to Protect the life

The processing of personal data based on point (d) of Article 7 of this law shall be necessary for the protection of the life of the data subject or of other natural persons who are seriously affected. In such cases, the data controller shall be required to demonstrate that there is a reasonable basis to believe that a threat exist to the health or safety of the data subject or other affected natural persons who are seriously affected.

Article 12.- The necessity for the purposes of the performance of a task carried out in the public interest

The processing of personal data based on point (e) of Article 7 of this law shall comply with one of the following conditions:

a- The exercise of rights under the laws or regulations that authorize the data controller to fulfill a duty in the national interest or the public interest.
b- The processing of personal data which is publicly accessible.
c- The processing of personal data solely for artistic, literary, archival, or historical purposes.
d- The processing of personal data by news entities solely for the purpose of news broadcasting.

Article 13.- The necessity for the Purposes of the Legitimate Interests

The processing of personal data based on point (f) of Article 7 of this law shall require a legitimate interest assessment before processing the personal data.

The legitimate interest assessment shall demonstrate that the legitimate interest pursued by a data controller or a third party outweighs the fundamental rights and freedoms of the data subject. The data controller shall provide special care and attention in protecting the best interests of the data subject that is under the age of 16 (sixteen).

Article 14.- The protection of Sensitive Personal Data

The processing of sensitive personal data shall be prohibited.

The first paragraph above shall not apply if the data controllers process personal data in compliance with legal bases as stipulated in Article 7 of this law and at least one of the following additional conditions:

a- Explicit consent of the data subject.
b- The necessity for the purposes of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection as determined by law.

c- The necessity for the protection of the vital interests of the data subject or of other natural persons where the data subject is physically or legally incapable of giving consent.
d- In the course of its legitimate activities by a not-for-profit body with a political, philosophical, religious or trade union related to the members or to former members of the body or to persons who have regular contact with it. In this case, the not-for-profit body shall have appropriate safeguards for the processing of personal data and shall not disclose the personal data outside that body without the consent of the data subjects.
e- Personal data has manifestly been made public by the data subject.
f- The necessity for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity.
g- The necessity for reasons of substantial public interest as determined by laws. In this case, the processing of personal data shall be proportionate to the purpose of the processing, respect the essence of right, shall be subject to suitable and specific measures to safeguard the fundamental rights and freedoms of the data subject.
h- The necessity for the purpose of preventive or occupational medicine or for reason of public health as determined by laws and shall be subject to suitable and specific measures to safeguard the fundamental rights and freedoms of the data subject.
i- The necessity for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes as shall be determined by laws. In this case, the processing of personal data shall be proportionate to the purpose of processing, respect the essence of right, shall be subject to suitable and specific measures to safeguard the fundamental rights and freedoms of the data subject

CHAPTER 4
DATA CONTROLLER AND DATA PROCESSOR

Article 15.- Personal data protection by design and by default

The data controller shall implement technical design measures for the protection of personal data by integrating the necessary security safeguard solely for the specific purposes of personal data processing. These measures shall be applied both at the time of determining the means for processing personal data and at the time the processing itself is carried out.

The data controller shall implement data protection measures by default in the processing of personal data, ensuring that only personal data necessary for a specific purpose is processed. These measures shall be applied by determining the amount of personal data collected, the scope of the processing, the period of storage and the accessibility of the personal data.

Article 16.- Representative of the Data Controller or Data Processor

A data controller or data processor located outside the Kingdom of Cambodia, whose activities related to the offering of goods or services to or the monitoring of behavior of data subjects within the Kingdom of Cambodia, shall appoint a representative and provide the representative's name and contact information to the Ministry of Post and Telecommunications.

The conditions, formalities and procedures for appointing such a representative and submitting their name and contact information to the Ministry of Post and Telecommunications shall be determined in the Common Guidelines on Personal Data Protection.

Article 17.- Contract between the Data Controller and Data Processor

A data controller and a data processor shall enter into a written contract specifying the subject matter of the contract, duration of personal data processing, nature and purpose of the processing, types of personal data, categories of data subject, notification procedure for personal data protection breach, as well as the obligations and rights of the data controller.

The data processor shall not process personal data prior to entering into a contract on processing of personal data with the data controller. The data processor shall process personal data in accordance with its contractual obligations and the provisions of this law, and shall delete and/or return the personal data to the data controller upon the completion of personal data processing.

The detailed conditions of the contract between data controllers and data processors shall be determined in the Common Guidelines on Personal Data Protection.

Article 18.- Records of Processing

A data controller and data processor shall prepare and maintain records of all personal data processing activities under their responsibility or control.

The conditions, formalities, and procedures of preparing and maintaining a record of all processing activities shall be determined in the Common Guidelines for Personal Data Protection.

Article 19.- Personal Data Impact Assessment

If the data controller determines that the processing of personal data may pose a high risk to the rights and freedoms of the data subject and/or other natural persons, the data controller is required to conduct a personal data impact assessment. This impact assessment shall take into account the type, scope, context, and purpose of the personal data processing and the data controller shall submit impact assessment report to the Ministry of Post and Telecommunications**.**

The personal data impact assessment report shall include:

a- Description of the purposes and means of the personal data processing.
b- The assessment of the risk affecting the rights and freedoms of the data subject and/or other natural persons.
c- Measures in response to those risks.
d- Security measures and other mechanisms to ensure the protection of personal data.

The conditions, formalities, and procedures of a personal data impact assessment shall be determined in the Common Guidelines for Personal Data Protection.

Article 20.- Security of Personal Data Processing

Data controllers and data processors shall implement technical and organizational measures for ensuring the security of the personal data processing and to prevent the following activities:

a- The Risks of unauthorized access, collection, use, disclosure, copy, modification, or destruction, as well as other potential risks.
b- The loss of any storage medium or device on which personal data is stored.

In the arrangement of technical and organizational measures as stipulated in paragraph 1 above, the data controllers and data processors shall assess the following conditions:

a- The risks of personal data processing that may impact the rights and freedoms of a data subject.
b- The type, scope, context, and purpose of personal data processing.
c- The current state-of-the-art technology.
d- Costs of implementing measures taking into account the circumstances and risks of processing.

After assessing the conditions as stipulated in paragraph 2 above, the data controllers and data processors shall implement the following appropriate measures:

a- Pseudonymization and encryption of personal data where, necessary.
b- Ensuring the confidentiality, integrity, and availability, and resilience of personal data processing systems and services.
c- Ensure the timely restoration of access and retrieval of personal data in the event of an incident.
d- Regular testing, assessing, and evaluating the effectiveness of the technical and organizational measures for ensuring the security of the personal data processing.

Article 21.- Notification of Data Breach to the Personal Data Protection Regulator of Cambodia

In the case of a personal data breach, where the breach may pose a risk to the data subject and/or other natural persons, the data controller shall notify the Ministry of Post and Telecommunications immediately, but no later than 72 (seventy-two) hours from the time of becoming aware of the personal data breach. In case where the data controller cannot notify the Ministry of Post and Telecommunications within 72 (seventy-two) hours, the data controller shall provide the valid reasons for the delay.

Conditions, formalities, and procedures of notification of personal data breach to the Ministry of Post and Telecommunications shall be determined in the Common Guidelines for Personal Data Protection.

Article 22.- Notification of Data Breach to the Data Subject

In the case of a personal data breach, where the breach may pose a high risk to the rights and freedoms of the data subject, the data controller shall notify the data subject immediately upon becoming aware of the personal data breach.

The provision of paragraph 1 above shall not apply in any of the following conditions:

a- The data controller has implemented proper technical and organizational measures to ensure security measure of the personal data affected by the breach such as encryption or data anonymization.

b- The controllers have taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects.

c- Notification of a personal data breach to each data subjects would involve a misappropriate burden or cost for the data controller or would be impossible to carry out by any other means. In such case, the data controller may issue a public notice or use similar method to inform the data subject in manner that is equally effective as a notification to each data subject.

If the data controller does not notify the data subject of the personal data breach on the grounds that there is no high risk as stated in paragraph 1 or under any of the conditions stated in paragraph 2 above, the Ministry of Post and Telecommunications may require the data controller to notify the data subject in case where it considers that the personal data breach present a high risk to the rights and freedoms of the data subject.

Conditions, formalities, and procedures of notification of data breach to the data subject shall be determined in the Common Guidelines for Personal Data Protection.

Article 23.- Data Transfer outside the Kingdom of Cambodia

A data controller shall not transfer personal data outside the Kingdom of Cambodia unless one of the following conditions is fulfilled:

a- The Ministry of Post and Telecommunications grants permission for the transfer of personal data.

b- The data controllers assess that appropriate safeguards are in place to protect the personal data being transferred outside the Kingdom of Cambodia.

c- The transfer of personal data outside the Kingdom of Cambodia is based on specific circumstance, including but not limited to:

1. Written consent of the data subject.
2. The necessity for the performance of a contract between the data subject and the data controller.
3. Protection of public interests.
4. Protection of life of the data subject or another natural persons,
5. Protection of legitimate interests of the data subject.
6. Establishment, exercise, or defense of a legal claim or whenever courts are acting in their judicial capacity.

The data controller shall be able to provide evidence to the Ministry of Post and Telecommunications in the case of conditions (b) and (c) of paragraph 1 above.

Conditions, formalities, and procedures of personal data transfer outside the Kingdom of Cambodia shall be determined in the Common Guidelines for Personal Data Protection.

CHAPTER 5
PERSONAL DATA PROTECTION OFFICER

Article 24.- Requirement to have Personal Data Protection Officer

The data controllers and the data processors shall appoint a personal data protection officer who possesses the qualifications to practice the personal data protection.

The data controllers and the data processors shall notify the Ministry of Post and Telecommunications of the name and information of the personal data protection officer within 30 (thirty) working days from the date of appointment.

The provision in paragraph 2 above also applies in the event of a change of the personal data protection officer. The notification shall be made within 15 (fifteen) working days from the date of the change.

The criteria for determining the types of the data controllers and the data processors that are required to have a personal data protection officer shall be determined by a Prakas of the Minister of the Ministry of Post and Telecommunications.

Article 25.- Duties and qualifications of the Personal Data Protection Officer

The personal data protection officer is responsible for monitoring the compliance of personal data processing as stipulated by this law.

Any natural persons who practice personal Data Protection Officer shall have adequate qualifications for practicing personal data protection officer and possess a personal data protection profession certificate.

The conditions, procedures, and formalities for obtaining the personal data protection profession certificate shall be determined by a Prakas of the Minister of the Ministry of Post and Telecommunications.

CHAPTER 6
DATA SUBJECT RIGHTS

Article 26.- General Rules

In order to ensure the exercise of the data subject's right as stipulated in this Chapter, the data controllers shall fulfill the following conditions:

a- Provide information to the data subject in a form that is easily understandable and clear.
b- Facilitate the exercise of the data subject's rights and shall not reject the data subject's request, unless the data controller is unable to identify the data subject.
c- Provide information on the actions to be taken relating to the data subject's right without undue delay and within 1 (one) month from the date of the receipt of the data subject's request. This period may be extended by up to 2 (two) additional months, if necessary, due to the number and the complexity of requests. In such cases, the data controllers shall inform the data subject of the request for an extension within one (1) month from the date of receipt of the request, including the reasons for the requested extension.
d- Provide information to the data subject free of charge. In cases where the data subjects make a request more than 2 (two) times within one quarter, the data controllers may charge a reasonable fee to cover the administrative costs related to providing such information.

Article 27.- Right to Information

Prior to processing personal data, the data controller shall provide the following information to the data subject:

a- Identity and contact information of the data controller.
b- Legal basis and purpose of the processing of personal data.
c- Type of personal data related to the data subject.
d- The recipient of personal data.
e- The right to file a complaint to the Ministry of Post and Telecommunications.
f- The procedure for exercising the rights of the data subjects as stated in this Chapter.
g- Other necessary information that ensures that personal data has been processed fairly and transparently.

The information as stated in points (a) to (g) in paragraph 1 above shall also be applied in the case where the data controllers obtain the personal data of data subject from a person who is not the data subject. In such case, the data controller shall provide the information to the data subject immediately and no longer than 1 (one) month from the date of personal data is received.

Article 28.- Right to Access

The data subject shall have the right to access or obtain a copy of their personal data from the data controller, including information related to the processing of their personal data.

In case where the personal data is transferred outside the Kingdom of Cambodia, the data subject shall have the right to obtain information about appropriate safeguard as stated in point (b) of Article 23 of this law.

Article 29.- Right to Rectification

The data subject shall have the right to obtain the rectification of their inaccurate personal data from the data controller without undue delay. In such cases, the data subject also has the right to have their incomplete personal data completed, including by providing a supplementary statement.

To ensure the exercise of the rights mentioned in Paragraph 1 above, the data controller shall notify the data subject about the restriction of personal data processing, unless there is a justified reason indicating that such notification is impossible or exceeds the capacity to provide it.

Article 30.- Right to Erasure

A data subject has the right to erase his or her personal data from the data controller based on any of the following reasons:

a- The personal data is no longer required for the purposes for which the personal data was processed.
b- The data subject withdraws consent to the processing of personal data as stipulated in point (a) of Article 7 of this law, and the data controller has no other legal basis for processing personal data.
c- The data subject objects to the processing of personal data in accordance with Article 33 of this law.
d- The personal data is processed contrary to this law or other laws and regulations in force.
e- Other laws or regulations require the erasure of such personal data.

In cases where the data controller has made the personal data publicly avialable that is required to be erased, as stated in paragraph 1 above, the data controller shall tak appropriate measures to erase that publicly disclosed personal data by notifying other data controllers to delete any links to, or copies of, the personal data that has been requested for erasure. In taking such appropriate measures, the data controller may taking into account consider the use of available technology and the cost of erasing such personal data.

The provisions specified in paragraph 1 and paragraph 2 above shall not apply to any of the following conditions:

a- The exercise of the right of freedom of expression and information.
b- The performance of a legal obligation by the data controller, or for the fulfillment of a task carried out in the public interest, or the exercise of official authority under the laws or regulations vested in the data controller.
c- Processing is necessary for the purpose of public health.
d- Processing is necessary for archiving purposes in the public interests, scientific or historical research purposes or statistical purposes in accordance with the Common Guidelines for Personal Data Protection.
e- Processing is necessary the establishment, exercise or defense of legal claims.

To ensure the exercise of the rights mentioned in Paragraph 1 above, the data controller shall notify the data subject about the restriction of personal data processing, unless there is a justified reason indicating that such notification is impossible or exceeds the capacity to provide it.

Article 31.- Right to Restriction

A data subject has the right to restrict the processing of his or her personal data by requesting the data controller to restrict such processing of personal data in any of the following cases:

a- The data subject disagrees with the accuracy of the personal data and the data controller is verifying the accuracy of the personal data;
b- The processing of personal data is contrary to laws and regulations in force, but the data subject opposes the erasure of the personal data and requests to restrict the use of the personal data instead;
c- The data controller no longer needs the personal data for the purposes of the processing of personal data, but the data subject requests for retention of such data for the establishment, exercise, or defense of legal claims.
d- The data subject exercises the right to object as specified in paragraph 1 of Article 33 of this law.

When the processing of personal data is restricted as stipulated under paragraph 1 of this Article, the data controller only has the right to retain such personal data. The processing of such personal data is restricted during the restricted period, except in any of the following conditions:

a- The personal data is processed with explicit consent from the data subject;
b- The processing of personal data is necessary for the establishment, exercise, or defense of legal claims;
c- The processing of personal data is necessary for the protection of the rights of other natural or legal persons;
d- The processing of personal data is necessary for national interests.

To ensure the exercise of the rights mentioned in Paragraph 1 above, the data controller shall notify the data subject about the restriction of personal data processing, unless there is a justified reason indicating that such notification is impossible or exceeds the capacity to provide it.

Article 32.- Right to Personal Data Portability

The data subject shall have the right to request the data controller holding their personal data to transmit their personal data to another data controller. The requested data controller is obliged to transmit the personal data in a machine-readable format to the receiving data controller at the request of the data subject, without any obstruction, subject to the following conditions:

a- The processing of personal data is carried out with consent of the data subject in accordance with this law or pursuant to a contract;
b- The processing of personal data is carried out by automated means.

In the case where the data subject exercise the right in accordance with paragraph 1 above, the data subject has the right to have their personal data transmitted directly from one data controller to another data controller, if technically feasible.

The exercise of the right to data portability as stated in paragraph 1 above shall not affect the right to erasure of personal data as stated in Article 31 of this law, nor the rights and freedoms of others.

The right to personal data portability shall not be applicable in cases where the data controller processes personal data in accordance with point (e) of Article 7 and Article 12 of this Law.

Article 33.- Right to Object

The data subject shall have the right to object at any time to the processing of their personal data, based on reasons related to their particular situation, if one of the following conditions applies:

a- The processing of personal data is based on necessity for the performance of a task carried out in the public interest, as specified in point (e) of Article 7 and Article 12 of this Law.
b- **(b)** The processing of personal data is based on necessity for the purposes of the legitimate interests pursued by the data controller or a third party, as specified in point (f) of Article 7 and Article 13 of this Law.

In such cases as mentioned in paragraph 1 above, the data subject may exercise their right to object in order to stop or prevent the processing of their personal data. However, the data controller may continue to process the personal data if the controller can demonstrate compelling legitimate grounds for the processing personal data which override the fundamental rights and freedoms of the data subject, or if the processing of personal data is necessary for the establishment, exercise, or defense of legal claims.

Furthermore, the data subject shall have the absolute right to object to the processing of their personal data if it is used entirely for direct marketing purposes.

Article 34.- Automated individual decision-making, including profiling

The data subjects shall have the right to request human involvement in cases where an automated decision produces legal effects that impact their legitimate interests or similarly affects them.

The right to request human involvement in automated decisions, as stated in paragraph 1 above, shall not apply if the automated decision:

a- is necessary for the performance of a contract or to initiate entering into a contract;
b- is authorized by specific legal provisions; or
c- is based on the explicit consent of the data subject.

In the cases referred to in points (a) and (c) of paragraph 2 above, the data controllers shall implement appropriate measures to protect the rights, freedoms, and legitimate interests of the data subject. These measures shall include the right to request human intervention, as well as the right of the data subject to express their views or object to the automated decision.

Article 35.- Right to Remedy

The data subjects shall have the right to obtain an appropriate legal remedy when their rights, as provided in this chapter, have been infringed.

The data controllers shall establish rules and mechanisms to receive complaints and resolve issues within their Internal regulations on Personal Data Protection.

Article 36.- Conditions, Formalities, and Procedures of Exercising Data Subject Rights

The conditions, formalities, and procedures of exercising data subject rights as stipulated in this Chapter shall be determined in the Common Guidelines for Personal Data Protection.

CHAPTER 7
COMMON GUIDELINES ON PERSONAL DATA PROTECTION

Article 37.- Common Guidelines on Personal Data Protection

The Ministry of Post and Telecommunications shall prepare the Common Guidelines on Personal Data Protection in order to request a decision from the government.

The Common Guidelines on Personal Data Protection shall be determined by Sub-Decree.

Article 38.- Supplementary Guidelines for Sectoral Personal Data Protection

The line ministries/institutions may, if necessary, develop Supplementary Guidelines for Sectoral Personal Data Protection. The development of Supplementary Guidelines for Sectoral Personal Data Protection shall comply with the Common Guidelines on Personal Data Protection and be consulted with the Minister of Ministry of Post and Telecommunications.

Supplementary Guidelines for Sectoral Personal Data Protection shall be determined by a Prakas of the Minister of the line ministry or the Head of the line institution.

Article 39.- Internal Regulations on Personal Data Protection

Data controllers and data processors shall develop Internal Regulations on Personal Data Protection in accordance with the Common Guidelines on Personal Data Protection and any Supplementary Guidelines for Sectoral Personal Data Protection, if applicable.

The Internal Regulations on Personal Data Protection shall be approved by the management board or senior leaders of the data controllers and data processors.

The Internal Regulations on Personal Data Protection shall include technical and organizational measures for the protection of personal data, taking into account the security framework of the personal data, the type, scale, context, and purpose of the processing, as well as the risks that may impact the rights and freedoms of data subjects.

Data controllers shall be able to demonstrate that the technical and organizational measures comply with this law.

Data controllers shall regularly review and update their technical and organizational measures based on the changes in their business operations, technological developments, legal amendments, and requirements set by the Ministry of Post and Telecommunications.

CHAPTER 8
PERSONAL DATA INSPECTION

Article 40.- Personal Data/Ministry of post and Telecommunications Inspectors

The Minister of the Ministry of Post and Telecommunications shall appoint personal data/ Ministry of post and Telecommunications inspectors to oversee, investigate, gather evidence, and strengthen the enforcement of this law.

Personal data/ Ministry of post and Telecommunications inspectors receive legal status as judicial police to oversee offenses as stated in this law and shall act in accordance with the provisions of the Criminal Procedure Code.

Formalities and procedures for granting of legal status as judicial police to personal data/ Ministry of post and Telecommunications inspectors shall be determined by an inter-ministerial Prakas by the Minister of the Ministry of Justice and the Minister of the Ministry of Post and Telecommunications.

Article 41.- Uniform, Insignia, and Rank symbol of Personal Data/Ministry of post and Telecommunications Inspectors

During the law enforcement operations, personal data Personal Data/Ministry of post and Telecommunications inspectors shall wear a uniform with an insignia and rank symbol, and shall have a mission order letter.

The uniforms, insignias, and Rank symbol of personal data/Ministry of post and Telecommunications inspectors shall be determined by Sub-Decree.

Article 42.- Duties and Rights of personal data/Ministry of post and Telecommunications Inspectors

Personal data inspectors shall have the following duties and rights:

a- Oversee, investigate, and suppress offenses related to personal data;
b- Take measures in accordance with this law and related regulations in force;
c- Seize evidence and preparing the case file related to offenses under this law;
d- Perform other duties and take other measures within the framework of implementing this law or as assigned by the Minister of the Ministry of Post and Telecommunications.

The formalities and procedures for personal data inspection shall be determined by Prakas issued by the Minister of the Ministry of Post and Telecommunications.

Article 43.- Personal data inspection operations

All personal data inspection operations conducted in the course of investigate offenses shall comply with the Criminal Procedure Code.

Personal data/Ministry of post and Telecommunications inspectors may seek assistance from any local authorities at all levels and armed force unit or other relevant competent authorities to assist in the suppression of offenses as stated in this law.

In case of an *in flagrant delicto*, the relevant competent authorities shall immediately provide information to the nearest personal data/Ministry of post and Telecommunications inspectors to measures according to the procedures.

Article 44.- Complaint Against the Actions of the personal data/Ministry of post and Telecommunications Inspector

Any person who does not agree with any measure taken by the personal data/Ministry of post and Telecommunications inspectors may file a complaint to Ministry of Post and Telecommunications within 30 (thirty) days from the date of receiving the decision.

The Minister of the Ministry of Post and Telecommunications shall issue a decision on the complaint within 45 (forty-five) days from the date of receiving the complaint.

In the event that such a person does not agree with the decision of the Minister of the Ministry of Post and Telecommunications, that person may file a complaint to other mechanisms of the Royal Government or to the courts according to the procedures.

CHAPTER 9
DISPUTE RESOLUTON

Article 45.- Dispute Resolution Related to Personal Data Protection

Besides criminal offenses, any disputes related to personal data protection, a disputing party shall file a complaint to the Ministry of Post and Telecommunications for resolution in according with existing procedures. The Minister of the ministry of Post and Telecommunications shall appoint a conciliator within 48 (forty-eight) hours from the time receiving the complaint for conciliation or resolution.

In the event that no disputing parties file a complaint to the Ministry of Post and Telecommunications, the Minister of the ministry of Post and Telecommunications may also conciliate or resolve the disputes if necessary.

The conciliation or resolution of a dispute related to personal data protection shall be conducted within 15 (fifteen) days from the time receiving the instruction from the Minister of the ministry of Post and Telecommunications.

The results of the conciliation shall be recorded in a conciliation report. This conciliation report shall specify the conciliated or non-conciliated points and shall be signed by the disputing parties and an officer of the Ministry of Post and Telecommunications.

Ministry of Post and Telecommunications shall provide a copy of the conciliation report to the disputing parties.

The conciliated points shall be enforceable immediately or within a timeframe specified in the conciliation report.

Conditions, formalities, and procedures of personal data dispute resolution shall be determined by a Prakas of the Minister of the Ministry of Post and Telecommunications.

Article 46.- Public service fees for dispute resolution

Public service fees for dispute resolution shall be determined by an inter-ministerial Prakas between the Minister of the Ministry of Economy and Finance and the Minister of the Ministry of Post and Telecommunications.

CHAPTER 10
PENALTIES

Article 47.- Penalties

Penalties under this law include:

a- Administrative penalties include written warnings, fine, restriction and other administrative penalties. The enforcement of administrative penalties shall be vested in the Ministry of post and telecommunications. Rules and procedures for the enforcement of administrative penalties shall be determined by a Prakas of the Minister of the Ministry of Post and Telecommunications.

b- Criminal penalties include criminal penalties as stated in Article 51 of this law.

Article 48.- Administrative Fines

Any person who does not comply with any of the provisions under Chapter 3, Chapter 4, Chapter 5, or Chapter 6 of this law shall be liable for administrative fines as follows:

- not exceed the maximum amount of 60,000,000 (sixty million) Riels for each natural person getting involved
- not exceed the maximum amount of 600,000,000 (six hundred million) Riels or 10% of a legal person’s annual turnover for each legal person involved.

The annual income of a legal person shall be determined based on the income stated in the financial statements audited by an independent auditor who is recognized by the Ministry of Economy and Finance.

Article 49.- Grounds for Administrative Fines

The decision on administrative fines as specified in Article 48 of this law shall be considered on the following grounds:

a- The nature, gravity, and duration of the non-compliance by the data controller;
b- The types and characteristics of personal data affected by the non-compliance by the data controller;
c- Gaining any financial benefit or avoiding any financial loss from the non-compliance by the data controller;
d- Timely and effective measures taken by the data controller to mitigate the effects and consequences of the non-compliance;
e- Efforts to implement adequate and appropriate measures have already been made by the data controller despite the non-compliance;
f- Previous non-compliance of the data controller;
g- Compliance with the order or guidelines of the Ministry of Post and Telecommunications or voluntary implementation of the data controller related to remedy or mitigating the effect of the non-compliance;
h- Administrative fines imposed are proportionate and effective to strengthen the law enforcement and prevent non-compliance by the data controller;
i- Impact of the imposition of the administrative fines on the data controller or regular operations of the data controller;
j- any other relevant grounds as prescribed by laws and regulations.

Article 50.- Fines for Non-Payment of Fines

Any person who has been administratively fined but fails to pay the fines for more than:

a- 30 (thirty) days from the date of receiving the order to pay the fine, shall be administratively fined twice the amount of the unpaid fine.
b- 60 (sixty) days from the date of receiving the order to pay the fine, shall be fined three times the amount of the unpaid fine.
c- 90 (ninety) days from the date of receiving of the order to pay the fine, there shall be a case filed to the competent courts of the Kingdom of Cambodia in order to take measures in accordance with the procedures.

Article 51.- Criminal Liability

A legal person shall be declared criminally liable in accordance with the conditions set forth in Article 42 (Criminal Responsibility of Legal Entities) of the Code of Criminal Procedures for the offenses as specified in Article 48 of this law.

A natural person who still commits the same offense shall be punishable by imprisonment from 6 days to 2 years and a fine up to 60,000,000 (sixty million) Riels.

A legal person who still commits the same offense shall be punishable by a fine up to 100,000,000 (one hundred million) Riels, and one or more additional penalties set forth in Article 168 (Additional Penalties Applicable to Legal Entities) of the Code of Criminal Procedure.

CHAPTER 11
TRANSITION PROVISIONS

Article 52.-

Regulations related to personal data protection that have previously been in force shall continue to apply until a new regulation replaces those regulations in accordance with the provisions of this law.

CHAPTER 12
FINAL PROVISIONS

Article 53.-

All provisions contrary to this law shall be abrogated.

Article 54.-

This law shall be implemented within 2 (two) years from the date of promulgation.

This law was approved by the National Assembly of the Kingdom of Cambodia.
on ... month ... year ...
at the National Assembly session... Legislature ...
Day ... month ... year ... ... year ...
Phnom Penh Date ... Month ... Year ...
President of the National Assembly

Samdech Moha Rathsapheathika
Thipadei KHUON SUDARY

Annex to the Law on Personal Data Protection
Glossary

1	Encryption	Transformation of information or data into any special code that cannot be understood or used.
2	Processing	Refers to any operation or set of operations which may be performed on personal data, whether or not by automated means or non-automated means, including but not limited to collection, recording, organization, storage, alteration, retrieval, use, disclosure by transmission, dissemination, erasure, and destruction.
3	Pseudonymization	Refers to the processing of personal data in a way that cannot identify the data subject.
4	Data breach	Refers to an incident in which personal data was accessed, disclosed, or stolen without an authorization.
5	Consent	Refers to the expression of the data subject's will to agree with the processing of his or her data in accordance with the provisions of Article 8 in this law.
6	Explicit Consent	Refers to written or electronic consent that can be used as a basis for evidence in the event of an objection from the data subject.
7	Data anonymization	Refers to the process of transforming personal data in such a way that the natural person can no longer be identified. It means completely removing all information related to the natural person's identity, to the extent that even the data controller or data processor cannot identify such a natural person.
8	Legally Incapable	Refers to the condition of a natural person who is unable to make decisions or perform legal actions due to reasons such as being underage (minor), mental incapacity, or legal restrictions.
9	Management Board or Senior Executive	Refers to the board of directors, the chief executive officer, the head of a company or entity, or the head of a department who is responsible for the personal data management.
10	Common Guidelines on Personal Data Protection	Refers to the personal data protection rules that set the minimum requirements for all data controllers and data processors.
11	Supplementary Guidelines for Sectoral Personal Data Protection	Refers to additional personal data protection rules by sector developed by line Ministries/Institutions in the event that the minimum requirements determined in the Common Guidelines on Personal Data Protection are not sufficient for each sector.
12	Sensitive personal data	Refers to personal data revealing racial origin, political opinions, religious or philosophical beliefs, or trade union membership, biometric data, genetic data, health data, and data concerning the sex life or sexual orientation of a natural person.
13	Personal data	Refers to information relating to a natural person who identifies or can be identified by that natural person. Information relating to a natural person includes an identifier (name, identification number, location data), an online identifier (IP address, email address and account name) and one or more specific information relating to the

		physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
14	Biometric data	Refers to personal data resulting from technical processing relating to the physical, physiological or characteristics of an individual from which a natural person can be identified. For example: facial image or fingerprints.
15	Genetic data	Refers to personal data relating to the identity or genetic characteristics of a natural person from which that natural person can be identified.
16	Data concerning health	Refers to data related to the physical, mental health of an individual, such as information related to the health status of an individual, and that information can identify the individual.
17	Internal Regulations on Personal Data Protection	Refers to personal data protection rules developed by data controllers and data processors.
18	Data subject	Refers to a natural person whose information is processed in accordance with the provisions of this law.
19	Traditional Media	Refers to media systems that existed before the internet era, such as newspapers, magazines, books, radio, television, and movies.
20	New Media	Refers to new media that defines anything related to the Internet with interaction between publishers and users or users and users of new technologies, both visual and audio. The definition of this term is constantly changing with the development of science and information technology, both analog and digital, such as Facebook, YouTube, social networking sites, etc.
21	Filing system	Refers to any structured set of personal data which is accessible according to specific criteria
22	Person	Refers to a natural person or a legal person.
23	Data controller	Refers to a natural person or legal entity that determines the purpose and means of processing personal data. Legal entities that are considered as data controllers under this law include private legal entities, public establishments of administrative character, or public enterprises, not including Public Authorities acting within their jurisdiction. A data controller that is a Public Authority and governed by this law shall be based on a decision by the Royal Government or other laws.
24	Data processor	Refers to a natural person, private legal entity, public establishment of administrative character, or public enterprise that processes personal data on behalf of a data controller based on a contract.
25	Data Protection Officer	Refers to a natural person who is assigned to assist in the compliance of the processing of personal data as defined by this law. Such natural person may be an employee or a representative by mandate. When this law comes into force, the personal data protection officer must have a personal data protection profession certificate.
26	Data protection by default	Refers to the approach that requires data controllers to automatically set settings in devices or systems that

		make it easier for users to control their privacy when using or receiving services electronically.
27	Data protection by design	Refers to a mandatory approach for designing systems by incorporating personal data technical and organizational measures from the outset rather than adding measures later. This approach is intended to prevent the risk of data breaches.
28	Personal or household activities	Refers to activities directly related to a natural person, household work, or family, and not to professional or business activities.
29	News entity	Refers to a group of individuals or legal entities that disseminate information to the public through traditional and/or modern media.
30	Public Authority	Refers to ministries and institutions of the executive, legislative, and judicial branches; sub-national administration; and similar public entities.
31	Representative of data controller and data processor	Refers to a person who is represented by a mandate of the data controller or data processor. This person may be a lawyer or a person who has been legally authorized by the data controller or data processor.