Comprehensive Legal and Policy Analysis of the Draft Law on Personal Data Protection of the Kingdom of Cambodia

Professor Abu Bakar Munir

Chairman, Data Protection Expert Asia (DPEX) Sdn. Bhd.

President, Malaysian Association of Cybersecurity and Privacy Professionals (MACPP)

Founder, Asosiasi Profesional Privasi Data Indonesia (APPDI)

1. Introduction

This report presents a comprehensive legal and policy analysis of the Draft Law on Personal Data Protection of the Kingdom of Cambodia. It aims to support the Ministry of Post and Telecommunications (MPTC) in refining and strengthening the draft to ensure that the final law achieves its intended objectives of safeguarding personal data, promoting responsible data governance, and facilitating Cambodia's transition toward a trusted digital economy.

The analysis examines each substantive provision of the draft law in detail, identifying its alignment with international data protection principles and best practices—particularly those reflected in the EU General Data Protection Regulation (GDPR), ASEAN frameworks, and comparative legislation from regional jurisdictions. For each article, the report highlights potential legal, policy and implementation challenges, followed by specific recommendations to improve clarity, coherence, enforceability, and consistency with Cambodia's constitutional and institutional context.

Where appropriate and necessary, the report proposes revised drafting language to enhance legal precision and practical applicability. Special attention has been given to issues such as legal certainty, proportionality of obligations, institutional coordination, enforcement mechanisms, and the balance between data protection and innovation.

This analysis is submitted in the spirit of constructive engagement and collaboration. It is intended to assist the MPTC and relevant stakeholders in finalizing a robust, transparent, and future-proof legal framework that not only protects the rights and freedoms of individuals but also promotes public trust and investor confidence in Cambodia's digital transformation.

2. Article-by-Article Analysis and Recommendations for Improvement

2.1 Article 2 – Scope of Application

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.*

2.2 Key Observations

This article describes the law as a "basic law", implying it is foundational or primary legislation for the regulation of personal data. This suggests it sets fundamental principles, rights, and obligations rather than detailed procedural rules.

The law applies to the processing of personal data. The key term, "processing" as defined in the glossary, 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." This is in line with most modern data protection frameworks like GDPR.

In term of means of processing, the law covers automated and non-automated means. Automated means is digital processing, computer systems, online storage, and cloud services. Non-automated means refers to manual filing systems, paper records, handwritten forms. This broad language ensures the law applies not only to digital contexts but also to traditional paper-based systems. This is in-line with the Government's 2024-2035 agenda, ASEAN Digital Masterplan 2025 and ASEAN Digital Economy Framework Agreement (DEFRA).

The term of "personal data" is defined in the draft law as "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."

There are several issues with this definition. Firstly, the opening clause ("who identifies or can be identified by that natural person") reads incorrectly — an individual cannot be identified *by that natural person*. Likely intended: "identified or identifiable." Secondly, the phrase "and one or more specific information relating to…" could be read to mean that *personal data must include an identifier AND one or more 'identity' attributes* — which would wrongly narrow the

definition. Thirdly, inconsistent terminology - “Account name” / “online identifier” / “identifier” need consistent categories (usernames, device IDs, cookies, etc.). Fourthly, the list mixes identifiers (name, ID) with characteristics (genetic, mental) without distinguishing special categories/sensitive data that usually require higher. Lastly, over-broad / vague phrases like “economic, cultural or social identity.” It is unclear whether this means status, characteristics or simply behaviour (e.g., purchase history).

The phrase “which form the filing system” is significant - it indicates that the law targets data organized in a structured manner, allowing for retrieval. In GDPR terms, this is similar to “structured filing systems,” which are covered even if the data is on paper. The implication is that if data exists but cannot be systematically retrieved, it may fall outside the law’s scope. Sole proprietors, small companies processing unstructured data would be excluded from the law.

2.2.1 “Personal Data”

The term “personal data” should be clearly defined as it is the core of the subject matter in determining whether or not an entity will be subjected to the law.

The proposed replacement text is as follows:

“*personal data” means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*.”

2.2.2 “filing system”

It is vague and could cause confusion about what kinds of manual data are covered. The draft law defines “filling system” as to any structured set of personal data which is accessible according to specific criteria. There is a need to give special emphasis on the method of processing. The proposed complete definition: **“…** *structured set of personal information that is accessible by criteria relating to an individual, even if it's not processed automatically*.”

2.2.3 “basic law”

It is stylistically weak and legally imprecise. “Basic law” doesn’t carry clear legal weight unless it’s a defined category. Rephrase to make the clause more direct and authoritative: “*This Law governs the processing of personal data, whether carried out by automated or non-automated means forming part of a structured filing system*.”

2.2.4 Unclear Coverage

It is unclear whether the law covers *all* processing activities or only those forming filing systems. If the policy intent is to ensure broad protection, clarify explicitly: "*This Law applies to all processing of personal data, whether by automated or non-automated means. For non-automated means, it applies only where the data form part of a structured filing system*." This wording mirrors GDPR Article 2(1) and prevents interpretive loopholes.

2.3 Non-applicability

Article 2 provides, *"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*.

2.3.1 Exemption (a) - Public authorities performing functions within their jurisdiction

The Human Rights Committee's interpretation of the right to privacy in General Comment 16 explains that laws protecting personal data should apply to public and private entities alike. Exceptions to privacy protections should be written into law in a way that is clear and accessible (legality principle), should be necessary to achieve one of the legitimate purposes outlined in the ICCPR (legitimacy principle), and should be an appropriate and proportionate response and directly related to that legitimate aim (proportionality principle).

Instead of blanket exemption, specify that the exemption applies only when processing is for a function that is lawful, necessary, proportionate, and subject to oversight. Maybe require that even for public authorities there must be compliance with key principles (transparency, data subject rights, security) when not damaging official functions.

The rational for this is that the law does not obstruct essential state functions such as law enforcement, national security, taxation, or public administration. It avoids conflict between data protection obligations and constitutional or statutory duties of public agencies.

2.3.2 Exemption (b) - Natural person acting only for personal or household activities

This mirrors common exemptions found in international data protection regimes — but how it is worded matters greatly for accountability and enforceability.

Individuals using personal data only for private, non-commercial purposes (e.g., maintaining personal contacts, family photos, or social media for private use) are exempt. The rational for this exemption is to protects privacy of everyday life; avoids over-regulating private citizens. For example, someone keeping a contact list or sending invitations should not fall under compliance obligations.

The exemption must be strictly confined to purely personal activities. If an individual uses data in ways that are public, commercial, or systematically shared (e.g., running a social media page with

public access), they should not be exempt. The draft law defines "personal and household activities" as activities directly related to a natural person, household work, or family, and not to professional or business activities. This mirrors the GDPR provision.

2.4 Recommendations for Improvement and Proposed Revised Text

2.4.1 Narrow the exemption — specify that it applies only when the processing is necessary for lawful governmental or public interest functions and subject to appropriate safeguards (e.g., oversight, proportionality).

2.4.2 Clarify the exemption – it applies only to processing "exclusively for personal or household purposes and not for professional, commercial, or public activities."

"This Law shall not apply to:

(a) The processing of personal data by public authorities solely for the performance of their lawful functions, where such processing is subject to other legal safeguards; and

(b) The processing of personal data by a natural person solely for personal or household activities that are not connected with professional, commercial, or public purposes."

3. 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.

The MPTC's broad statutory powers demonstrate Cambodia's commitment to formal data protection governance. However, structural dependence, unclear safeguards, and limited enforcement powers weaken its regulatory credibility. Moving toward an independent,

transparent, and rights-based authority would align Cambodia with global and ASEAN data protection standards, reinforcing both citizen trust and international digital trade confidence.

More importantly, these are critical factors or pre-requisites to achieve the broad purposes of the law, "To establish 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."

3.1 Recommendations for Improvement

3.1.1 Establish an Independent Data Protection Commission (DPC) with legal personality, budgetary autonomy, and independent leadership.

3.1.2 Strengthen enforcement capacity — authorize binding decisions and corrective orders.

3.1.3 Ensure transparency — require annual public reporting, publication of enforcement outcomes, and audit of regulatory performance.

4. 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.

4.1 Recommendations for Improvement and Proposed Revised Text

Article 6 appropriately adopts the six fundamental principles recognized in international data protection frameworks (lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, and integrity/security). This alignment indicates Cambodia's intention to harmonize with global norms (GDPR, OECD Privacy Guidelines, APEC Privacy Framework). The final paragraph—requiring the controller to demonstrate compliance—is crucial. It establishes the accountability principle, which transforms these principles from abstract values into enforceable duties. However, several substantive and drafting weaknesses may undermine enforceability, accountability, and coherence with the rest of the law.

4.1.1 Purpose limitation exceptions are too open

(b) - The wording "in accordance with relevant data protection guidelines" delegates exceptions to future guidelines, not law. This undermines legal certainty and could allow broad administrative discretion. The exceptions should be narrowly defined and subject to safeguards, especially for secondary uses by the public sector.

Define "compatible purpose" criteria in the law (e.g., reasonable link, context of collection, consequences, safeguards). Ensure exceptions for research and archiving are subject to anonymization or pseudonymization.

4.1.2 Storage limitation clause confusingly refers to "Data Protection Directive"

(e) - Reference to a "Data Protection Directive" is technically incorrect, likely copied from EU text. Cambodia should not refer to EU legal instruments but to "this Law or relevant regulations". Replace "in accordance with the Data Protection Directive" with: "*in accordance with this Law or any implementing regulation*." Additionally, simplify exceptions and ensure storage is limited to necessary periods with retention policy requirements.

4.1.3 Security principle lacks clarity

(f) - It merely refers to Article 39, without summarizing integrity and confidentiality obligations. There is no mention of protection against unauthorized access, loss, or destruction. The principle should explicitly state “integrity and confidentiality” as part of the obligation.

Strengthen the security principle and make reference to confidentiality, integrity, and resilience explicitly.

Rephrase the provision to: “*Personal data shall be processed in a manner ensuring appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical and organizational measures*.”

5. Article 7 Legal Basis for Processing Personal

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.

5.1 Key Observations

This provision establishes the legal bases for processing personal data, a central component of data protection regimes globally. The listed bases broadly align with Article 6(1) of the EU General Data Protection Regulation (GDPR), which serves as an international benchmark. Here are commendable pints about the Article:

Comprehensive Scope: The article appropriately covers the six traditional legal bases—consent, contract, legal obligation, vital interests, public interest, and legitimate interests—ensuring a broad justification framework.

Flexibility: It allows data controllers to identify appropriate legal grounds depending on context, supporting diverse operational realities.

I**nclusion of legitimate interest**: Recognizing legitimate interests of controllers or third parties provides operational flexibility, particularly for private entities.

5.2 Weaknesses and Gaps

However, a closer analysis reveals several gaps that merit refinement to enhance clarity, accountability, and alignment with global best practices.

5.2.1 Ambiguity in consent requirements

The text merely mentions "consent of the data subject" without defining the nature of consent (e.g., freely given, specific, informed, and unambiguous). This leaves room for coercive or implied consent, weakening data subjects' control.

5.2.2 Lack of hierarchy or guidance on application

The provision treats all legal bases equally. In best practices (e.g., GDPR Recitals 40–43), consent is not always the preferred basis—controllers are encouraged to select the most appropriate basis before processing, with clear documentation. This text does not specify such responsibility.

5.2.3 Public interest and legitimate interest not adequately delimited

"Task carried out in the public interest" and "legitimate interest" are potentially broad and subject to misuse. No balancing test or safeguards (e.g., assessing impact on data subjects' rights) are mentioned.

5.2.4 No requirement for documentation or transparency

Modern data protection laws (e.g., GDPR Article 30) require controllers to document the chosen legal basis for accountability. The absence of such duty limits enforceability.

5.3 Recommendations for Improvement

5.3.1 Define "consent" clearly — Require that consent be freely given, specific, informed, and unambiguous, with explicit consent for sensitive data. The definition of the term in the draft law is too general. It says "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. Meanwhile "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.

5.3.2 Introduce accountability obligations — Mandate that data controllers document the

chosen legal basis prior to processing.

5.3.3 Insert balancing and necessity tests — For legitimate interests and public interest processing, require that processing not override the rights and freedoms of the data subject.

5.3.4 Clarify hierarchy of bases — Specify that consent should be used only when no other lawful basis applies, to prevent overreliance.

5.3.5 Enhance transparency — Require that data subjects be informed of the specific legal basis relied upon at the time of collection.

6. 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.

6.1 Key Observations

The clause correctly mirrors the general principle found in international data protection regimes (e.g., GDPR Art. 6(1)(b)), which allows processing when it is necessary for the performance of a contract. However, the phrasing “based on point (b) of Article 7 of this law” is overly internal and could hinder readability for external users. Laws typically restate the legal basis for clarity.

The phrase “such necessity shall be applied strictly” is commendable as it prevents broad interpretation, ensuring proportionality. However, the law does not specify how to assess or demonstrate necessity (e.g., distinguishing between necessary and merely useful data). This could create ambiguity for controllers. There is a need for this issue to be addressed in the law and not regulations.

The statement that “processing shall terminate in accordance with the terms and conditions agreed by the parties to contract” is problematic. Data processing rights and obligations should not depend solely on private contracts but on statutory principles, including data minimization, retention limits, and legal obligations.

There is no mention of the data subject’s rights once the contract ends (e.g., erasure, restriction, or retention period). There is also no reference to secondary uses (e.g., billing or dispute resolution) which might lawfully continue beyond contract performance under other

legal bases.

6.2 Proposed Revised Text

Rephrase the article so it stands on its own without referring back to Article 7 for meaning, add objective criteria for necessity, clarify post-contractual processing, and strengthen accountability requirements.

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

"Processing of personal data shall be lawful where it is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into such a contract. The assessment of necessity shall be limited strictly to what is required to fulfil the contractual purpose and shall comply with the principles of personal data processing set out in Article 6 of this law."

"In determining necessity, the data controller shall ensure that the personal data processed are directly relevant and proportionate to the contractual purpose, and that processing unrelated to the performance of the contract shall require a separate legal basis. Processing based on contractual necessity shall cease upon the completion or termination of the contract, except where continued retention is required by law, for legitimate business interests such as dispute resolution, or for compliance with legal obligations. The data controller shall be responsible for documenting the assessment of contractual necessity and for ensuring that any continued processing after contract termination is supported by a separate legal basis and retention policy."

7. 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.

7.1 Key Observations

This clause reflects a common lawful basis found in major data protection frameworks such as the EU General Data Protection Regulation (GDPR) Article 6(1)(c). It recognizes that processing is lawful when it is "necessary for compliance with a legal obligation to which the controller is subject." However, the draft law uses slightly imprecise language: The phrase "performance of a legal obligation required by law" is redundant; "performance" and "required by law" express the same idea. Additionally, it does not specify the source of such legal obligations — for example, whether it must arise from national laws, regulations, or court orders. This ambiguity

could lead to inconsistent interpretation.

The clause correctly imposes a burden of demonstration on the data controller. This is important to ensure accountability and prevent the overuse of the "legal obligation" ground. However, the provision lacks procedural detail — it does not specify how or when the data controller must demonstrate the existence of the legal obligation (e.g., to the data protection authority or upon request by the data subject). It also omits any requirement for documentation or record-keeping, which is essential for accountability and compliance audits.

The clause refers to processing "necessary" for compliance, but there is no mention of the principle of proportionality — ensuring that only data strictly required to meet the legal obligation are processed. Without this safeguard, controllers may process more data than needed.

Although Article 6 (Principles of Processing) presumably governs all processing, this clause would be stronger if it expressly reiterated that processing under legal obligation must still comply with the principles of fairness, purpose limitation, and data minimization.

7.2 Proposed Revised Text

Rephrase the article to address all the issues:

"The processing of personal data based on point (c) of Article 7 shall be lawful only where it is necessary to comply with a legal obligation arising from laws, regulations, or official orders to which the data controller is subject. The processing shall be limited to what is strictly necessary and proportionate to achieve compliance with that obligation. The data controller shall maintain records identifying the specific legal provision relied upon and shall be able to demonstrate compliance to the supervisory authority upon request. Such processing shall remain subject to the principles of processing of personal data as set out in Article 6 of this law."

8. 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.

8.1 Key Observations and Recommendations for Improvement

The article attempts to define the conditions under which personal data may be processed in the public interest, aligning conceptually with Article 6(1)(e) GDPR. However, it lacks precision and clear safeguards against potential misuse.

The draft law defines 'public authority" as ministries and institutions of the executive, legislative, and judicial branches; sub-national administration; and similar public entities. However, the phrase "national interest or public interest" is undefined and can be interpreted broadly. Without specific criteria or a mechanism for determination, it opens the door to arbitrary or excessive data processing by public authorities or other entities claiming a "public interest" justification.

The inclusion of publicly accessible data (point b) does not automatically make processing lawful — even publicly available data remains protected under data protection law. Simply put, the fact that the data is publicly available and accessible does not mean that anyone can collect and process the data without data subject's consent. A data controller must ensure that it has a lawful basis for processing and comply with all data protection principles.

Under Singapore's Personal Data Protection Act (PDPA), organizations can collect, use, and disclose publicly available personal data without consent, but they must still comply with other PDPA obligations, such as the purpose limitation rule. This means the purpose must be one that a reasonable person would consider appropriate, and organizations cannot use the data for clearly unreasonable purposes like those that violate a law or harm an individual. Additionally, the data may be subject to terms and conditions imposed by the data source, and organizations must handle it responsibly.

This Article combines public interest tasks (point a) with special categories of processing such as journalistic, artistic, or historical purposes (points c and d), which under international standards (e.g., GDPR Articles 85 and 89) are subject to separate exemptions and balancing tests, not grouped under "public interest."

There is no mention of proportionality, necessity, or data minimization tests, which are crucial to justify processing under public interest. The Article lacks procedural safeguards, such as prior authorization, impact assessments, or oversight by a data protection authority (DPA). Points (c) and (d) omit the requirement to balance freedom of expression and information against the right to privacy.

It is unclear who qualifies as a data controller in the context of "public interest." The today's reality is that there are private entities providing services for public interest or performing public functions (e.g., hospitals, contractors, transportations, universities). Lack of clarity may

lead to inconsistent application.

8.1.1 Clarify the scope of "public interest", separate artistic, literary, journalistic, and historical purposes into a distinct article, add proportionality and necessity requirements, strengthen accountability, and Add safeguards for publicly accessible data.

8.1.2 The public interest purpose must be clearly established by law or regulation and proportionate to the aim pursued.

8.1.3 The data controller shall ensure compliance with the principles of data minimization, necessity, and transparency, and shall document the legal basis for such processing.

8.1.4 The processing of publicly accessible personal data shall remain subject to this law and must be compatible with the original purpose for which the data was made available.

8.2 Proposed Revised Text

Rephrase the provision**:**

"Processing of personal data based on point (e) of Article 7 shall be lawful only where it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller."

9. 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).

9.1 Key Observations and Recommendations for Improvement

The article appropriately mirrors the principle found in GDPR Article 6(1)(f), which allows processing when it is necessary for legitimate interests pursued by the controller or a third party. However, unlike the GDPR, this provision: (i) does not specify what qualifies as a "legitimate interest", (2) lacks procedural detail on how the legitimate interest assessment (LIA) should be conducted and documented, and it does not mandate transparency, such as notifying

the data subject that the processing is based on legitimate interests.

Requiring a legitimate interest assessment before processing is a strong safeguard. However, the article does not define the components of the assessment. There is no requirement to document or retain the assessment for accountability purposes. There is no supervisory oversight—the controller is not obliged to submit or make the LIA available to the Data Protection Authority (DPA) upon request.

The clause regarding special care for data subjects under 16 is commendable and aligns with child data protection principles. However, the article does not define what "special care and attention" entails. Furthermore, it does not indicate whether consent from a parent or guardian is required for minors when relying on legitimate interests.

The age threshold (16) is relatively high. For examples, Singapore's PDPA sets the age of consent at 13 years old. China's PIPL sets the age of consent at 14 years old. Under the GDPR, the default age of consent is 16 years old, however it allows EU member states to lower this threshold to as young as 13 years old if they choose. Majority of countries governed by GDPR set the age of consent between 13 – 15 years old.

9.1.1 Define "Legitimate Interest" Clearly

Add a definition or illustrative examples, such as:

"Legitimate interest" means a lawful, specific, and proportionate interest pursued by the controller or a third party, including fraud prevention, network security, or direct marketing, provided that such interest does not override the rights and freedoms of the data subject.

9.1.2. Structure and Document the Legitimate Interest Assessment (LIA)

Specify that the assessment must include at least:. A purpose test identifying the legitimate interest pursued. A necessity test demonstrating that processing is essential to achieve that purpose. A balancing test showing that the controller's interest outweighs the potential impact on the data subject. The controller shall document the assessment and make it available to the supervisory authority upon request.

9.1.3 Require Transparency to Data Subjects

Add a provision such as:

"*The data controller shall inform the data subject that the processing is based on legitimate interests, including the nature of such interests, and shall clearly communicate the data subject's right to object to such processing"*

9.1.4. Strengthen Protection for Minors

Clarify obligations for processing children's data:

"*When processing data of a data subject under the age of 16, the controller shall ensure that the processing is strictly necessary, proportionate, and conducted with additional safeguards such as parental involvement, minimal data collection, and clear communication suitable to the child's understanding*."

9.1.5 Add Reference to the Right to Object

Add:

"*The data subject shall have the right to object, at any time, to the processing of their personal data based on legitimate interests, unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the data subject*."

9. 2 Proposed Revised Text

Article 13 – Necessity for the Purposes of Legitimate Interests

"The processing of personal data based on point (f) of Article 7 shall require the controller to conduct and document a Legitimate Interest Assessment (LIA) prior to processing.
(2) The LIA shall include a purpose test identifying the legitimate interest pursued;
a necessity test demonstrating that the processing is essential to achieve that purpose; and a balancing test showing that such interest does not override the rights and freedoms of the data subject.
(a) The controller shall document the LIA and make it available to the supervisory authority upon request.
(b) The controller shall inform the data subject that processing is based on legitimate interests and provide a clear means to exercise their right to object.
(c) When processing data of persons under the age of 16, the controller shall implement additional safeguards to ensure protection of their best interests, including parental involvement and age-appropriate transparency."

10. 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.

10.1 Key Observations, Weaknesses and Gaps

This article reflects the core principle of "Data Protection by Design and by Default" under Article 25 of the EU GDPR, which requires data controllers to integrate data protection measures from the earliest stages of processing activities. However, it is less comprehensive and lacks key accountability elements found in the GDPR and similar global frameworks The gaps and weaknesses are:

10.1.1 "**Technical design measures"** – The provision focuses only on technical safeguards but omits organizational measures, which are equally essential (e.g., policies, training, risk assessment).

10.1.2 "Solely for the specific purposes" – This wording could unintentionally restrict lawful multi-purpose processing or compatible use under data minimization principles.

10.1.3 Lack of reference to risk assessment – There is no requirement to consider the risks to data subjects' rights and freedoms, which is a crucial foundation of "privacy by design."

10.1.4 No accountability or documentation requirement – The article does not oblige the data controller to demonstrate or document the implementation of these design and default measures.

10.1.5 No reference to data processor obligations – Only the controller is mentioned, but processors also play a key role in implementing protective design features.

10.1.6 No link to data protection impact assessments (DPIAs) – The article should reference DPIAs as a method to ensure design compliance where high-risk processing occurs.

10.2 Recommendations for Improvement

10.2.1. Expand the scope to include both technical and organizational measures

"The data controller shall implement appropriate technical and organizational measures, designed to implement data protection principles effectively and to integrate necessary safeguards into the processing…"

10.2.2. Include risk-based and accountability elements

"*Such measures shall take into account the state of the art, the cost of implementation, the*

nature, scope, context, and purposes of processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons." This ensures proportionality and risk awareness.

10.2.3. Strengthen the 'by default' obligation

Add explicit wording to emphasize data minimization and access control:

"By default, personal data shall not be made accessible to an indefinite number of persons without the data subject's intervention, and only data necessary for each specific purpose shall be processed." This ensures compliance with necessity and proportionality"

10.2.4. Require documentation and demonstrability

"*The data controller shall be able to demonstrate compliance with this Article, including documentation of the measures adopted and their effectiveness."*

This ensures accountability and regulatory auditability.

10.2.5. Include reference to processors

"*Where processing is carried out by a data processor, the data controller shall ensure that the processor implements equivalent technical and organizational measures by design and by default*."

This harmonizes controller–processor responsibility.

10.2.6. Encourage linkage with DPIA and continuous review

"*When conducting a Data Protection Impact Assessment (DPIA), the data controller shall assess whether the measures adopted meet the requirements of data protection by design and by default and review them periodically*."

This strengthens integration with risk assessment mechanisms.

10.3 Proposed Revised Text

Article 15 – Personal Data Protection by Design and by Default

"The data controller and data processor shall implement appropriate technical and organizational measures, both at the time of determining the means for processing and at the time of the processing itself, designed to effectively implement data protection principles and

integrate necessary safeguards into the processing."

(*a) Such measures shall take into account the state of the art, the cost of implementation, the nature, scope, context, and purposes of processing, as well as the risks to the rights and freedoms of data subjects.*

(b) By default, the data controller shall ensure that only personal data necessary for each specific purpose of the processing is processed, including limitations on the amount of data collected, the scope of processing, the period of storage, and the accessibility of the data.

(c) The data controller shall be able to demonstrate compliance with this Article, including through appropriate documentation and review of the measures adopted.

(d) Where processing is carried out by a data processor, the data controller shall ensure that the processor implements equivalent data protection by design and by default.

(e) The data controller shall, where appropriate, assess these measures within the framework of a Data Protection Impact Assessment (DPIA) and periodically review their adequacy and effectiveness".

11. 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.

11. 1 Key Observations

This provision intends to extend Cambodia's data protection jurisdiction to foreign entities that target or monitor Cambodian data subjects—mirroring the GDPR's extraterritorial scope (Article 3). It rightly ensures that foreign organizations remain accountable, even without physical presence in Cambodia. However, several weaknesses reduce its practical and legal clarity.

The draft does not define whether the representative is a natural person, legal entity, or business service provider. It is unclear whether the representative must reside or be established in Cambodia, or may operate cross-border (e.g., within ASEAN). Without definition, enforcement will be inconsistent and businesses will face uncertainty. The provision does not specify the extent of the representative's responsibility or liability. Under GDPR (Article 27(5)),

the representative may be held jointly liable for non-compliance within the Union.

Also, the draft law seems to apply universally, even to small foreign businesses or occasional data transfers. There is no risk-based threshold to exempt low-volume or incidental processing activities. This may deter foreign investment or digital service entry into Cambodia.

11.2 Recommendations for Improvement

11.2.1 Define the Representative Clearly

Add a legal definition:

"Representative" means a natural or legal person established within the Kingdom of Cambodia who is authorized in writing by a foreign data controller or processor to act on its behalf with regard to its obligations under this Law and to cooperate with the Ministry of Post and Telecommunications and data subjects."

11.2.2 Require Local Establishment

Mandate that the representative: Must be physically or legally established in Cambodia, and be reachable for communications, enforcement actions, and data subject requests. This ensures local accountability and mirrors international practice (GDPR, Singapore PDPA's agent model).

11.2.3 Clarify Responsibilities and Liability

Insert a new clause:

"*The representative shall act as the contact point for the Ministry and for data subjects on all issues related to personal data processing, and may be held jointly liable for non-compliance of the foreign data controller or processor with this Law*."

This balances accountability and enforceability.

11.2.4 Introduce Risk-Based Exemptions

Exempt small or incidental operators:

"*The requirement to appoint a representative shall not apply to occasional processing that does not include large-scale processing or sensitive personal data and is unlikely to result in risks to the rights and freedoms of data subjects*."

This aligns with proportionality principles used in EU and ASEAN models.

11.2.5 Mandate Transparency and Public Register

Require MPTC to: Maintain a public registry of representatives for transparency and provide online submission and verification mechanisms for representative information.

11.2.6 Clarify Role in Enforcement and Cooperation

Add:

"*The representative shall facilitate communication between the foreign data controller or processor and the Ministry and ensure timely compliance with enforcement notices or data subject complaints*."

This builds practical bridges for regulatory cooperation.

11.3 Proposed Revised Text

Article 16 – Representative of Foreign Data Controller or Processor

(1) A data controller or data processor located outside the Kingdom of Cambodia, whose activities relate to the offering of goods or services to, or monitoring the behavior of, data subjects within the Kingdom, shall appoint a representative established in Cambodia.

(2) The representative shall act on behalf of the foreign data controller or processor regarding their obligations under this Law and shall serve as a contact point for the Ministry and data subjects.

(3) The representative may be held jointly liable with the data controller or processor for non-compliance under this Law.

(4) The requirement to appoint a representative shall not apply to occasional or low-risk processing activities.

(5) The Ministry shall issue a Prakas specifying detailed conditions, formalities, and exemptions related to the appointment and registration of representatives.

12. 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.

12.1 – Key Observations and Recommendations for Improvement

This Article requires a written contract between data controllers and processors, ensuring that personal data is processed only under agreed and lawful conditions. This is an important safeguard that aligns Cambodia with international standards such as the EU GDPR (Article 28) and the ASEAN Model Contractual Clauses.

However, several important details are missing that could weaken accountability, security, and cross-border interoperability.

12.1.1 Scope of the Contract is Too Limited

The article lists key contractual elements — subject matter, duration, type of data, categories of data subjects, breach notification, and obligations of the controller — but omits essential processor obligations such as: confidentiality of personnel handling data; sub-processing authorization and oversight; data security measures; cooperation with the controller on audits and data subject rights; assistance in breach management and regulatory compliance.

This makes the contractual safeguards weaker than ASEAN and EU standards, potentially undermining accountability and data security.

Recommendation: Expand the minimum content of contracts to include these obligations to ensure full accountability.

12.1.2 Lack of Express Duties on the Processor

The provision mentions that processors must act "in accordance with contractual obligations and the law," but it does not: require processors to follow the controller's documented instructions; mandate security measures appropriate to risk; Clarify whether processors may engage other processors (sub-processors) and under what conditions. This risks creating legal ambiguity if processors act independently or delegate tasks without control.

Recommendation: Insert a clause mirroring international practice—requiring processors to

follow written instructions and protect data confidentiality.

12.1.3 No Minimum Content for the "Common Guidelines"

The article defers "detailed conditions" to future Common Guidelines, but it does not set any minimum legal baseline. This leaves excessive discretion to future regulations, creating uncertainty and possible inconsistency in enforcement.

Recommendation: Establish a baseline in the Law itself, requiring the Common Guidelines to include model contractual clauses aligned with ASEAN and international best practices.

12.1.4 No Explicit Audit or Inspection Rights

Unlike GDPR Article 28(3)(h), the provision does not mention that controllers should have the right to audit, inspect, or verify the processor's compliance. This omission weakens accountability and limits the controller's ability to ensure data protection compliance.

Recommendation: Include a clear audit right for data controllers to verify compliance and data protection measures.

12.1.5 Unclear Treatment of Data After Processing

While it requires processors to "delete and/or return" personal data after processing, it does not clarify: whether the processor must also delete backups or residual copies; and the timeline or verification procedure for such deletion. This could lead to disputes or retention of personal data beyond its lawful purpose.

Recommendation: Include a clear provision to require data processor to delete backups or residual copies and sets the timeline and verification procedure. This can be included in Common Guideline.

12.2 Proposed Revised Text

Article 17 – Contract Between the Data Controller and Data Processor

"(1) A data controller and a data processor shall enter into a written contract before any processing of personal data. The contract shall specify: the subject matter and duration of the processing; the nature and purpose of the processing; the type of personal data and categories of data subjects; the obligations and rights of the data controller; the data security measures to be applied; procedures for notification and management of personal data breaches; and conditions for engaging sub-processors, if any.

(2) The data processor shall process personal data only on the documented instructions of the

data controller, ensure confidentiality of persons authorized to process data, and implement appropriate technical and organizational measures to protect personal data.

(3) Upon completion of processing, the data processor shall delete or return all personal data to the controller and confirm such deletion or return.

(4) The data controller shall have the right to audit and verify the data processor's compliance with this Law and the contract.

(5) The Common Guidelines on Personal Data Protection shall prescribe detailed conditions and model contractual clauses to ensure compliance with this Article."

13. Article 18 - Records of Processing (RoPA)

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.

13.1 Key Observations and Recommendations for Improvement

This article requires data controllers and processors to prepare and maintain records of personal data processing activities under their control. This obligation forms the backbone of an accountability-based data protection regime — allowing both regulators and organizations to verify compliance, assess risks, and respond effectively to complaints or breaches. However, the current draft provision is too general and may not ensure consistent or meaningful implementation in practice.

13.1.1 Lack of Minimum Record Content Requirements

The article simply requires maintaining records but does not specify what information must be included. International and regional frameworks (e.g., GDPR Article 30, ASEAN Model Contractual Clauses) typically require records to include: name and contact details of the controller/processor and DPO; purposes of processing; categories of data subjects and personal data; categories of recipients; details of cross-border transfers; data retention periods; and general description of security measures. Without specifying minimum content, records may be incomplete or inconsistent across organizations.

Recommendation: Include a clause listing the minimum elements that must appear in the record of processing activities (RoPA).

13.1.2 No Distinction Between Controller and Processor Responsibilities

The draft merges both controllers and processors under the same obligation but does not clarify what each must record. Controllers should document all processing under their control, including data sharing and legal bases. Processors should document processing carried out on behalf of controllers, including subcontractors. Without distinction, the law may cause confusion and overlapping obligations.

Recommendation: Add separate sub-articles specifying what controllers and processors must record.

13.1.3 Over-Reliance on Future Guidelines

The article leaves all details to the "Common Guidelines," offering no legal certainty on how or when records should be prepared, maintained, or updated. This may delay implementation and reduce compliance readiness for organizations.

Recommendation: Establish a basic obligation in the law itself, leaving only technical specifications to the Guidelines (e.g., templates, format).

13.1.4 No Requirement for Accessibility or Submission

There is no mention of: whether records must be readily available to the Ministry of Post and Telecommunications (MPTC); how long they must be retained; or whether they can be requested during inspections. This limits MPTC's ability to audit or investigate compliance.

Recommendation: State that records must be kept in written or electronic form and be made available to MPTC upon request.

13.1.5 No Risk-Based Exemption

Small enterprises or low-risk processors might face a disproportionate administrative and financial burden if required to maintain complex records.

Recommendation: Introduce an exemption or simplified requirement for small-scale or low-risk processing (similar to GDPR Article 30(5)).

Under article 30(5) of GDPR, organizations with fewer than 250 employees are exempted unless their processing is risky or involves sensitive data. But that rule reflects the EU's economic structure (large corporate sector) — and may not fit Cambodia's SME-dominated digital economy directly.

Cambodia's economy consists overwhelmingly of micro, small, and medium enterprises

(MSMEs) — over 98% of all firms. A threshold of 250 employees would exclude nearly all Cambodian organizations, undermining accountability entirely. Most data processing risks come not from size, but from nature and sensitivity of processing (e.g., health, biometrics, financial, surveillance). A direct numerical exemption could unintentionally create a compliance vacuum, excluding almost all domestic entities.

For Cambodia, the effective exemption should balance proportionality, risk management, and regulatory practicality. The exemption can be based on three combined criteria: processing scale (volume), risk profile (nature of data) and organisational size.

Recommendation: The exemptions from the record-keeping obligation be defined on a risk-based and proportionality basis, taking into account enterprise size and nature of processing. A threshold of 50 employees, combined with exclusions for sensitive or high-risk processing, would ensure practical compliance while maintaining robust accountability for entities most likely to impact individual privacy.

13.2 – Proposed Revised Text

Article 18 – Record of Processing Activities

"(1) A data controller and a data processor shall prepare and maintain a record of all personal data processing activities under their responsibility or control.

(2) The record shall contain at least the following information:

(a) the name and contact details of the data controller, data processor, and, where applicable, their representative;
(b) the purposes of the processing;
(c) a description of the categories of data subjects and of the categories of personal data;
(d) the categories of recipients to whom personal data have been or will be disclosed;
(e) information on cross-border data transfers, if any; and
(f) a general description of technical and organizational security measures.

(3) The obligation under paragraph (1) shall not apply to organizations that:
(a) employ fewer than 50 employees; and
(b) engage only in occasional or low-risk processing of personal data, which does not involve:
(i) the processing of sensitive personal data;
(ii) processing that is likely to result in a risk to the rights and freedoms of data subjects; or
(iii) large-scale or systematic monitoring of data subjects.

(4) Notwithstanding paragraph (3), the Ministry of Post and Telecommunications may require any organization to maintain such a record where the nature, scope, or purpose of its processing

activities so warrants.

(5) The conditions, formalities, and procedures for preparing and maintaining records of processing activities shall be determined in the Common Guidelines on Personal Data Protection."

14. 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.

14.1 Key Observations and Recommendations for Improvement

The inclusion of a Data Protection Impact Assessment (DPIA) requirement in the draft law is a positive step that aligns Cambodia with leading global and regional data governance frameworks. DPIAs serve as a preventive risk management tool, requiring organizations to assess and mitigate privacy risks before launching high-risk processing activities.

However, the current drafting of the DPIA provision presents several implementation and compliance challenges:

14.1.1 Lack of a Defined "High Risk" Threshold

The trigger for conducting a DPIA is stated as processing that "may pose a high risk", yet there is no mechanism for determining what constitutes high risk. Without clear criteria: SMEs may

struggle to understand their obligations and regulators may face inconsistent and subjective compliance practices. A defined threshold would support predictability and regulatory certainty.

14.1.2 Mandatory Submission of Every DPIA to MPTC

Requiring all DPIAs to be submitted to MPTC is not practical for either industry or the regulator. High volume of submissions will overwhelm MPTC's capacity. Business innovation and service deployment may be delayed. International practice (e.g., GDPR) requires submission only when high residual risk remains. A more proportionate approach would preserve MPTC's oversight while supporting a pro-innovation environment.

14.1.3 Absence of Prior Consultation Mechanism

Current text does not empower MPTC to intervene before harmful processing occurs. Introducing a prior consultation mechanism for unresolved high-risk activities would: safeguard data subjects' rights; strengthen regulatory supervision; and encourage preventative compliance culture.

14.1. 4 Insufficient Coverage of Processor Responsibilities

Data processors may design or operate systems that create significant risk, but the draft provision assigns no obligations to them. Requiring processors to assist controllers in conducting DPIAs aligns with accountability principles across ASEAN.

14.1.5 Need for Clear Procedural Guidance

While Common Guidelines are referenced, the provision should set out minimum DPIA content, including: scope of processing; necessity and proportionality analysis; measures to mitigate risks; and security safeguards. This ensures foundational consistency from the outset of enforcement.

Recommendations: Strengthen the Article by: defining high-risk processing categories, limiting MPTC submission to situations where risks remain high after mitigation, enabling prior consultation, imposing support obligations on processors, and establishing minimum DPIA content within the statute.

14.2 Proposed Revised Text

Article 19 – Data Protection Impact Assessment

"(1) Where a type of personal data processing is likely to result in a high risk to the rights and freedoms of data subjects, the data controller shall conduct a Data Protection Impact

Assessment prior to the processing.

(2) A DPIA shall at minimum include:
(a) description of the processing operations and purposes;
(b) an assessment of the necessity and proportionality of the processing;
(c) an assessment of the risks to the rights and freedoms of data subjects; and
(d) the measures envisaged to address and mitigate such risks, including safeguards and security measures.

(3) Where a DPIA identifies that the processing continues to present a high residual risk in the absence of measures taken by the data controller, the data controller shall submit the DPIA report to the Ministry of Post and Telecommunications and seek guidance prior to commencing the processing.

(4) The data processor shall provide the data controller with all necessary assistance to fulfil DPIA obligations under this Article.

(5) The Ministry of Post and Telecommunications may issue a list of processing operations for which a DPIA is required, and a list for which a DPIA is not required.

(6) The detailed conditions, formalities, and procedures for conducting a DPIA and for prior consultation with the Ministry of Post and Telecommunications shall be determined in the Common Guidelines on Personal Data Protection."

15. 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 rsks 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.

15.1 Key Observations and Recommendations for Improvement

The draft provision rightly establishes a general obligation for data controllers and processors to implement technical and organizational measures to ensure security in personal data processing. By incorporating a risk-based approach, the draft aligns conceptually with international frameworks such as the GDPR and the ASEAN Data Management Framework.

However, the current wording remains too broad and is insufficiently operationalized to drive strong and consistent security practices across different sectors and organization sizes. Without clearer standards or mechanisms of accountability, compliance risks becoming minimalistic and reactive, ultimately exposing data subjects to significant harm from unauthorized access, data leaks, and cybercrime.

The draft also places limited emphasis on oversight of data processors, such as cloud service providers and external vendors, even though many cybersecurity incidents originate from these third parties. Clear obligations on contractual safeguards and supervision would significantly improve system-wide security.

Additionally, to support enforcement and compliance, especially among SMEs, the law should require controllers and processors to document their security measures and demonstrate that they are appropriate to the risks. Clear guidance from the Ministry should set minimum standards and provide practical tools.

16. 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.

16.1 Key Observations

The draft breach notification clause represents a significant step toward accountability in Cambodia's emerging data protection ecosystem. Requiring notification to the Ministry of Post and Telecommunications (MPTC) within 72 hours mirrors global norms and promotes transparency when data incidents may harm individuals.

However, the provision in its current form remains structurally incomplete and risks low compliance, regulatory overload, and limited protection for data subjects.

16.1.1 Need for clearer risk thresholds

The draft applies notification obligations where a breach "may pose a risk," but lacks clarity on risk level (low vs. high). International best practice distinguishes: Low-risk breaches → internal documentation only and High-risk breaches → notify regulator and affected individuals. Without this distinction, businesses — especially SMEs — may over-report, overwhelming MPTC and diluting focus from serious incidents.

16.1.2 Practicality: initial notice vs. full report

A single detailed notification within 72 hours is often unrealistic. Organisations frequently need time to investigate scope, severity, and root causes. Singapore PDPA, GDPR, Malaysia PDPA and Thai PDPA all allow: An initial notice with essential facts, and A follow-up detailed report after investigation

This staged model encourages early transparency without penalising operators for lack of immediate complete information.

16.1.3 Integrity of the 72-hour rule depends on a defined trigger

The provision does not define “becoming aware” of a breach. This creates legal uncertainty about when the countdown begins, potentially undermining enforceability. A “reasonable diligence” test would align Cambodia with ASEAN standards and mitigate disputes.

16.1.4 Processors must be included

The draft law imposes the breach notification obligation to data controller only. Most Cambodian operators outsource key data functions to processors — cloud storage, payroll vendors, loyalty systems. Unless processors are legally obligated to notify controllers promptly: controllers may fail to detect breaches; reporting deadlines become unworkable; and accountability gaps widen.

16.1.5 Accountability and learning require internal record keeping

A mandatory breach register is missing but essential for: organisational self-governance, trend analysis by MPTC, and proportionate, and regulatory action.

16.2. Recommendations for Improvement

16.2.1 Adopt a “Notifiable Breach” Standard

Define a notifiable breach as one likely to result in harm to individuals, reducing unnecessary reporting and focusing enforcement on impactful breaches.

Two-Tier Notification System (Regulator + Individuals) - Medium risk → regulator notified. High risk → regulator and affected individuals notified. Require controllers to notify data subjects when there is a high likelihood of harm such as identity theft, financial loss, or reputational damage.

Allow Staged Reporting: Initial Notice + Full Report - Many laws allow an initial notice followed by a detailed submission once investigation is complete (EU, UK, Australia). Permit preliminary notification within 72 hours and supplemental reports when full facts become available — promoting early transparency.

16.1.6 Define the Trigger for the 72-Hour Deadline

EU guidance ties the reporting time-frame to when a controller becomes aware of the breach — preventing ambiguity. Draft law adopted the similar approach but there is a need to clarify that the countdown starts when reasonable certainty of a breach is established, not merely suspicion.

16.1.7 Place Explicit Duties on Data Processors

ASEAN countries, South Korea, Australia. Canada. etc require processors to inform controllers promptly so reporting deadlines can be met. This is crucially important when a data breach occurs when the data under the control of data processor or the data is in the system of the data processor. Require contractual and legal obligations for processors to notify controllers without delay.

16.1.8 Introduce Mandatory Breach Record keeping

Many countries, including ASEAN and others require breach logs even when notification isn't triggered. This will support audits and trends analysis by the regulator and data controller/processor. Require controllers and processors to maintain a Breach Register available for regulator inspection.

16.1.9 Specify the Key Facts

The draft law should specify key facts to be included in the notification rather than leaving everything to the Common Guidelines. For example, under the General Data Protection Regulation (GDPR), Article 33(3) states that the notification to the supervisory authority "shall at least" include: (a) nature of the breach (including categories & approximate numbers of data subjects and records), (b) contact details of the Data Protection Officer or other contact point, (c) likely consequences, (d) measures taken or proposed. By doing so, it achieves a balance: the law sets the mandatory baseline, while the guidelines can offer flexibility (template, format, channel) and adapt over time.

16.1.10 Publish Standard Templates and Digital Reporting Portal

Many countries including ASEAN, New Zealand, Brazil, etc provide prescribed formats to ensure complete and consistent submissions. MPTC should issue standardized reporting forms and a secure digital portal to streamline submissions and analytics.

17. 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 2above, 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.

17.1 Key Observations, Weaknesses and Gaps

A credible personal data protection framework must ensure that individuals are promptly informed when their personal data is exposed to risks that could lead to tangible harm. The current draft provision establishes a commendable foundation by adopting a risk-based notification requirement, which aligns with international standards such as the GDPR and regional peers.

However, there are gaps that risk undermining requires controllers to notify "immediately," which is subjective and unenforceable. This ambiguity may encourage delay or inconsistent practices, making enforcement difficult.

17.1.1 No clear assessment criteria for "high risk"

Without statutory guidance on what constitutes high risk, data controllers could interpret the threshold narrowly and avoid notification even in serious incidents.

17.1.2 Content of breach notification not specified

Data subjects may be informed—but without actionable details. A notification that cannot help them mitigate harm offers little value.

17.1.3 Public notice exception too broad

Certain groups such as domestic violence victims, children, persons with disabilities—may be put at additional risk if notice is not directly delivered to them.

17.1.4 Excessive reliance on future Guidelines

Key elements are deferred to administrative guidelines. This creates uncertainty and weakens rights protection until the guidelines are issued.

17.2 Recommendations for Improvement

Implementing these changes would: enhance the credibility of Cambodia's enforcement regime; improve trust among citizens and international investors; align Cambodia with ASEAN & international best practices, and provide clearer compliance expectations for data controllers. This also contributes to broader digital economy goals — because responsible data stewardship fuels user confidence, business innovation, and cross-border data flows, the objectives of the law.

17.2.1 Strengthen Transparency + Accountability

Establish explicit timelines: Notify affected individuals without undue delay once high risk is confirmed, and require controllers to demonstrate how they assessed the level of risk

17.2.2 Define "High Risk" to Support Consistent Application

Include criteria such as: nature and sensitivity of data (e.g., financial, health, children's data), number of individuals affected, likelihood of identity theft, discrimination, physical danger, or reputational damage, and vulnerability of impacted groups. This ensures both industry certainty and meaningful protection.

17.2.3 Minimum Notification Content

Mandate that notices provide: Description of breach and what was compromised, actual or potential consequences, steps the controller has taken to mitigate, practical steps subjects can take to protect themselves, and contact point of controller or DPO. This empowers individuals to respond proactively to harm.

17.2.4 Narrow the Public Notice Exception

Public disclosure should only be allowed if: direct contact is truly impossible or creates isproportionate cost; and measures are adopted to avoid eexposing vulnerable individuals (e.g., argeted supplementary notifications)

18. Article 23 - Data Transfer outside the Kingdom of Cambodia

A data controller shall not transfer personal data outside the Kingdom of Cambodia unless oneof

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 person,

5. Protection of legitimate interests of the data subject.

6. Establishment, exercise, or defence 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.

18.1 Key Observations, Weaknesses and Gaps

The proposed cross-border transfer regime demonstrates a clear state intention to safeguard personal data that leaves the country. This aligns with emerging ASEAN practices and supports Cambodia's digital sovereignty agenda. However, the current provision governing transfers of personal data outside the Kingdom of Cambodia creates a regulatory structure that is too discretionary, highly centralized, and operationally unclear. Without significant refinement, it risks deterring digital investment, impeding ASEAN interoperability, and weakening personal data protection in practice.

18.1.1 Permission requirement (condition a) is overly broad and vague

Requiring explicit Ministry permission for all or most transfers can raise excessive administrative burdens, slow down legitimate business flows, and create unpredictability. Unless the criteria, timelines, scope and process are clearly defined, this can be a barrier rather than a protector.

18.1.2 "Appropriate safeguards" (condition b) undefined

What counts as "appropriate"? Are standard contractual clauses, binding corporate rules, codes of conduct, certification mechanisms allowed? The draft law does not specify. Without clarity, controllers may interpret too loosely (weak safeguards) or too conservatively (hindering innovation). International guidance emphasises that safeguards must be enforceable, offer rights, and have strong contractual or organisational commitments.

18.1.3 Derogation-based transfers (condition c) risk becoming the norm

Many transfers are based on consent, contractual necessity, public interest etc. But if derogation bases are used too widely, they dilute the baseline standard of protection. For example, relying on consent in a situation of imbalance (consumer vs big platform) may not offer genuine protection. Also "legitimate interest" basis needs careful guardrails.

18.1.4 Lack of structured documentation/assessment requirement

The draft says "controller shall be able to provide evidence" but doesn't require a prior documented assessment (a "transfer impact assessment") of the receiving jurisdiction, risks, onward transfers, safeguards. Without this, enforcement becomes reactive and weak.

18.1.5 Too much left to Guidelines

The core mechanics (what is "safeguard", how Ministry permission works, record-keeping obligations) are all delegated to future Guidelines. This risks delay, uncertainty and possibly weaker practical protections until the Guidelines are issued.

18.1.6 No mention of adequacy decision or "safe list" concept

Many mature frameworks include a concept of "adequate protection" in recipient country (a whitelist) so that transfers to those countries can proceed with less oversight. The draft law lacks this, which limits flexibility and may hamper international business. For example, the EU regime includes adequacy decisions.

18.1.7 "Protection of legitimate interest of data subject" (condition 5)

Typically, international frameworks use legitimate interest of the data controller as a narrow basis for processing NOT for data transfer. Putting "user interest" as justification for

transferring their data overseas flips accountability and weakens protection.

18.2 Recommendations for Improvement

18.2.1 Introduce a legal "adequacy / safe list" mechanism

Add a clause: "Transfers may proceed to a foreign country or international organisation that the Ministry has determined provides an adequate level of protection." Publicly publish list of such countries/organisations. Transfers to these countries may proceed under simpler requirements (with safeguards) without separate Ministry permission each time.

18.2.2 Define "appropriate safeguards" in law

Specify that acceptable safeguards include: (i) standard contractual clauses approved by the Ministry; (ii) binding corporate rules for intra-group transfers; (iii) codes of conduct & certification mechanisms. Require enforceable rights and remedies for data subjects under those safeguards. Require contractual or binding commitments with foreign recipients.

18.2.3 Require Transfer Impact Assessment (TIA) and record-keeping

Insert requirement: "Before a transfer under condition (b), the controller shall conduct, document and retain a transfer impact assessment which assesses: the receiving jurisdiction's legal & regulatory regime; risks to data subjects; safeguards adopted; onward transfer risks." The assessment shall be made available to the Ministry on request. Require controllers to maintain a register of outbound transfers: date, recipient, country, legal basis, safeguards, TIA summary.

18.2.4 Narrow derogation bases and set prioritisation

Make clear that derogation bases (consent, contract, vital interests etc) are exceptions, not the default. Impose additional conditions: e.g., consent must be explicit, informed, free, and data subject told of risk. Legitimate interest basis only if transfer is necessary and benefits outweigh risks. Require that if a safer basis (adequacy or safeguards) is possible, it should be preferred.

18.2.5 Limit Ministry permission to high-risk cases

Revise condition (a) so that Ministry permission is only required when: (i) the destination country is not assessed as adequate; and/or (ii) the category of data is sensitive; and/or (iii) the volume or nature of transfer is high-risk (children's data, health, biometric). Define timeline: "Ministry shall decide permission within X days (e.g., 60) or permission deemed granted/denied". Provide right of appeal or administrative review.

18.2.6 Ensure the Guidelines development and regulatory powers are clear

Law should mandate that the Ministry publish standard contractual clauses, codes of conduct, certification processes, TIA templates in guidelines within specified timeframe (e.g., 12 months). Ministry should have enforcement powers: audit, fine, stop transfers, require remedial action.

18.2.7 Remove Condition 5

Cross-border restrictions exist to ensure equivalent protection abroad, not to facilitate convenience-driven transfers. Condition (5) shifts the law's priority: from protecting rights to accommodating business preferences under a user-benefit narrative. Legitimate beneficial situations are already covered by other clauses – thus, condition 5 is redundant.

19. 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.

19.1 Key Observations and Recommendations for Improvement

The draft law's provision mandating data controllers and processors to appoint a Personal Data Protection Officer (DPO) is a positive step toward strengthening Cambodia's data protection framework. This aligns with international practices recognizing the importance of designated personnel overseeing data protection, as seen in the EU GDPR, Singapore PDPA, Malaysia PDPA, Thailand PDPA, etc.

Here are the gaps and recommendations to be considered:

19.1.1 Delegation to Prakas

Prakas will determine which entities must appoint a DPO. Without legislative guidance on

criteria, there is risk of inconsistent or delayed implementation. GDPR requires DPOs only for public authorities, large-scale processing, or sensitive data processing. Meanwhile, Singapore PDPA requires all individuals and organisations, regardless of size, to appoint DPO. There is a need to Include broad criteria in the law while leaving technical thresholds to the Prakas.

19.1.2 Qualification and Expertise

The current draft law states that DPO must "possess qualifications to practice personal data protection." Ambiguous language may lead to inconsistent appointments; no minimum standards or required expertise are specified. Define minimum knowledge or skill requirements to ensure competence and credibility.

20. 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 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.

20.1 – Key Observations, Weaknesses and Gaps

The DPO regime is a central compliance mechanism within modern data protection laws. Its inclusion in the draft Cambodian legislation demonstrates a commitment to accountability and alignment with international standards. However, in its current form, the framework lacks several core elements required to ensure feasibility, effectiveness, and consistency with global best practices.

20.1.1 DPO Functions Are Too Narrowly Defined

Currently, the draft law says the DPO is responsible for monitoring compliance. This is necessary but not sufficient. Missing essential duties include: advising the organization on obligations, managing data breach notifications, conducting/overseeing Data Protection Impact Assessments (DPIAs), training and awareness-raising, cooperating with the authority and serving as the contact point. fostering a data protection culture, and auditing.

Without defining these, organizations may treat DPOs as symbolic roles and internal auditor, weakening accountability. Under GDPR, Singapore PDPA, Malaysia PDPA, Thailand PDPA, etc.

the functions of DPO include all those above-mentioned matters.

20.1.2 Independence and Protection Not Guaranteed

There is no assurance that DPOs: are free from conflicts of interest, have authority and resources to perform their tasks, report directly to senior leadership, are protected from dismissal or retaliation for performing their duties. The risk is DPO may be appointed merely as a "figure-head" with no real oversight power. GDPR, ASEAN legislations/regulations, etc provide these elements to ensure DPO can function effectively without fear or favour.

20.1.3 Certification and Qualification Rules Are Overly Rigid

The certificate-only pathway: May create supply shortages, elevates cost barriers, risks delaying implementation, fails to recognize international expertise. Competence should be defined through multiple pathways (training, experience, recognized qualifications), with transitional measures.

20.1.4 "Any natural persons"

By specifying "natural person", the draft law creates a strict requirement that: a DPO must be an individual human being. A legal person (company) cannot be appointed as DPO, DPO-as-a-service providers cannot be appointed in corporate form, and a team-based DPO model is legally excluded.

So even if a company has a fully qualified privacy compliance department, they could not serve collectively as the DPO. This is misalignment with ASEAN regional and international practices allowing DPO as a service or DPO to be outsourced. The draft law is unrealistic and Cambodia would be an outlier and less business-friendly.

20.1.5 "Practicing" and "Personal Data Protection Certificate"

Practicing usually refers to regulated professional activities (e.g. lawyers, doctors, accountant, etc). Employing this term in the draft law: suggests that being a DPO is an independently licensed profession, which is not the norm internationally, may create uncertainty as to the position of DPO, internally as an employee or externally as a consultant or both? GDPR treats DPO as a compliance governance role, not a professional practice like law or medicine. DPOs do not "practice" — they perform or carry out duties. This may unintentionally imply personal liability similar to licensed professions, discouraging individuals from accepting the role.

The term "Personal Data Protection Certificate" seems to suggest that there will a special certificate created by the law and issued by the MPTC. This diverges from international norm and standard – no law specifically requires certificate. GDPR does not mandate a formal certificate. It requires that the DPO have "expert knowledge of data protection law and

practices, UK guidance similarly does not require a specific certificate; it expects professional experience and knowledge proportionate to the organization's processing.

20.2 Recommendations for Improvement

20.2.1 Clarify appointment criteria in the Law

Limit mandatory DPOs to: public bodies, high-risk processing (biometrics, children's data, large-scale surveillance) and operators of essential services (health, finance, telecom).

20.2.2 Strengthen DPO responsibilities

Include explicit duties: advisory on compliance and DPIAs, training and awareness programs, handling complaints and breach coordination, and reporting misconduct to MPTC.

20.2.3 Ensure DPO independence

Include provisions that: DPO cannot be dismissed/penalized for performing duties, DPO must avoid conflicts of interest (e.g., not head of legal/IT/security).

20.2.4 Allow DPO to be outsourced

The term "natural person" needs to be removed or reframed.

20.2.5 Provide regulatory certainty

Core principles should be in the law, with Prakas used only for technical procedures.

21. Article 26 - General Rules

In order to ensure the exercise of the data subjects right as stipulated in this Chapter, the data controllers shall fulfil 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.

21.1 Key Observations, Weaknesses and Gaps

This provision is a positive step toward ensuring data subjects can meaningfully exercise their rights. By requiring clear communication, timely action, and accessibility, the draft aligns itself with global norms and demonstrates Cambodia's commitment to responsible digital governance.

However, several elements of the current wording introduce significant risks to both effective rights protection and regulatory practicality. Here are the gaps and weaknesses:

21.1.1 Lack of Abuse Safeguards

The draft allows refusal only when a controller cannot identify the data subject. This is too restrictive and will: encourage malicious, spam, or vexatious requests, divert limited compliance resources away from legitimate queries, and increase burden on SMEs and public authorities.

International standards (EU GDPR, Thailand PDPA, Singapore PDPA) explicitly permit controllers to reject requests that are manifestly unfounded or excessive, particularly were repetitive. Without safeguards, cost of compliance could become extremely high for Cambodian organizations, discouraging digital innovation and lawful data use.

21.1.2 Arbitrary Fee Threshold

The rule allowing fees after "more than two requests per quarter" is: not tied to the nature of the request, misaligned with international models, and potentially punitive for individuals in prolonged disputes or urgent situations. More importantly, this may undermine accessibility and fairness of data rights, especially for vulnerable populations.

21.1.3 No Protection of Other Rights & Interests

The provision does not require controllers to consider: confidential business information, trade secrets, privacy of other individuals appearing in records, and national security or public interest concerns. This could expose businesses and individuals to unintended harm, creating legal contradictions with other sectors.

21.1.4 Weak Transparency in Time Extensions

The law requires controllers to notify of extensions but not to specify the new deadline. This dilutes accountability and opens the door to delaying tactics. It decreases trust and weakens enforceability.

21.1.5 Lack of Procedural Guarantees

There is no requirement for: acknowledgment of receipt, secure and accessible communication formats, and documentation for enforcement and dispute resolution. This raises uncertainty about when obligations begin and how compliance will be verified.

22.2 Recommendations for Improvement

The current draft provision requiring data controllers to facilitate the exercise of data subject rights is a valuable foundation for Cambodia's emerging data protection system. It promotes fair access, transparency, and timely responses. However, several operational gaps may unintentionally create compliance burdens, legal uncertainty, and weakened enforcement outcomes. Clarifying and strengthening the provision will help ensure both the protection of individual rights and the practical needs of Cambodia's growing digital economy. It is recommended that the law:

- Permits refusal for requests that are manifestly unfounded or excessive,
- Aligns fee policy with international best practice: fees only where requests are excessive or repetitive,
- Includes limitations to protect rights/freedoms of others,
- Requires confirmation of receipt and clear extension deadlines, and
- Mandates accessible, secure formats for response.

Refining this provision creates a balanced regulatory framework where data subjects' rights are genuinely protected without imposing disproportionate compliance burdens. This ensures Cambodia's Data Protection Law becomes a growth enabler in the digital transformation agenda. At the same time adopting these improvements will: strengthen enforcement credibility, support SMEs and digital economy competitiveness, increase legal clarity for both regulators and business, build public trust in the national data governance regime, and promote ASEAN and international alignment (GDPR, PDPA Singapore, PDPA Thailand).

23. 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.

23.1 – Key Observations, Weaknesses and Gaps

The draft provision requiring data controllers to provide information to data subjects prior to the processing of personal data represents a foundational step toward embedding transparency and accountability into Cambodia's emerging data protection regime. The intent is aligned with international norms — particularly the principles of fairness, transparency, and purpose limitation recognized under global frameworks such as the GDPR, Singapore's PDPA, Malysia's PDPA, etc.

This provision operationalizes transparency by requiring data controllers to proactively inform data subjects of how their personal data is processed. In practical compliance terms, this means: data controllers must maintain a privacy notice (sometimes branded as a "Privacy Policy" or "Personal Data Protection Notice"), the notice must contain all minimum elements listed in the provision (identity, purpose, legal basis, rights, complaints mechanism, etc.), the notice must be presented before any collection or processing begins, and the requirement applies both to personal data collected directly and indirectly. Here are the gaps and weaknesses of the draft law:

23.1.1 Conceptual Alignment vs. Fragmented Drafting

The provision borrows from international norms like GDPR Articles 13–14. However, some key transparency elements are missing or diluted. Without including full disclosure requirements, transparency becomes partial and risks weakening data subjects' ability to understand or exercise their rights. Right now, transparency is treated as a procedural task rather than a core

data protection principle embedded throughout the lifecycle of processing.

23.1.2 Weak Purpose Specification Requirement

The clause states "legal basis and purpose for processing" but doesn't require the purpose to be: specific, explicit, and legitimate. Controllers could rely on vague categories such as "business improvement," turning this into a box-ticking exercise rather than limiting function creep This could undermine trust and violate global purpose limitation standards.

23.1.3 Lack of Storage Limitation Transparency

No requirement to inform data subjects of: how long data will be kept; retention criteria; and deletion schedules. This creates a compliance loophole. Controllers could keep data indefinitely without disclosure or scrutiny. Almost every modern law GDPR, Brazil LGPD, Thailand PDPA, etc mandates retention transparency.

23.1.4 Insufficient Accountability Indicators

The provision provides information on rights and complaints to MPTC but doesn't require an internal accountability contact, such as: Data Protection Officer contact; internal grievance channels; and responsible business unit.

23.1.5 Recipient Identification Could Be Too Broad

"Recipient" is undefined. The controller could simply say "third parties" without: identifying category; specifying location; clarifying if cross-border transfers are involved. This conceals risk exposure from the data subject.

23.1.6 International Transfers Omitted

Not informing data subjects about transfers outside Cambodia: hinders informed consent; prevents data subjects from assessing risk; and undermines cross-border safeguard mechanisms.

23.1.7 Automated Decision-Making Not Addressed

Modern digital governance requires clarity on: profiling; automated scoring; and decisions with legal effects. Transparency is key to fairness, especially in biometrics, fintech, hiring, and public service delivery.

23.1.8 Indirect Data Collection Rule Too Rigid

The 1-month timeline is good but impractical if: huge datasets are acquired; subjects are

unknown; notification is impossible or disproportionate; and law enforcement confidentiality applies. GDPR builds in multiple exceptions to prevent regulatory overload and operational infeasibility.

23.1.9 Ambiguous “Other necessary information” Clause

While flexible, it creates uncertainty for businesses and inconsistent enforcement. Controllers need certainty. Regulators need clarity. Subjects need comprehensibility. Vague catch-all rules don’t satisfy any party.

23.2 Recommendations for Improvement

23.2.1 Expand Mandatory Information Elements

Include the following in the required disclosure list: data retention period or the criteria used to set it; contact details of the Data Protection Officer (if appointed); international transfers and safeguards applied; categories and sources of personal data for indirect collection; and automated decision-making and profiling that produce legal or significant effects. This closes information gaps and aligns with GDPR Articles 13–14, and ASEAN regulations.

23.2.2 Strengthen Purpose Limitation Language

Clarify that processing purposes must be: specific, explicit, and legitimate. This prevents vague justifications like “business needs” that allow excessive data reuse.

23.2.3 Add Proportionality and Feasibility Exceptions

In cases of indirect collection, allow exceptions where: identifying the data subject is impossible; notification requires disproportionate effort; confidentiality or secrecy obligations apply; information is already available to the data subject. This minimizes administrative burden and prevents over-notifying.

23.2.4 Require Layered & Accessible Communication

Specify that privacy notices must: be easily understandable (avoid legal jargo be delivered through accessible formats (digital, audio, local languages, etc.); and be tailored to vulnerable groups where applicable (children, disabled individuals). This directly supports fairness and inclusivity.

23.2.5 Introduce Internal Redress Channels Before Regulatory Complaints

Provide: a contact point for concerns or rights requests; a structured internal response procedure; and the option to escalate to MPTC only if unresolved. This eases regulator burden

and encourages effective resolution.

23.2.6 Clarify "Recipient" and Disclosure Scope

Replace broad references with: specific entities where possible; categories of recipients; whether they are located inside or outside Cambodia; and the purpose and legal basis for disclosure. This increases transparency around data sharing risks.

23.2.7 Link Transparency to Accountability Obligations

Explicitly state that controllers must: document compliance with transparency requirements; and update notices when processing purposes or recipients change. This makes transparency living, not static.

23.3 – Proposed Revised Text

Article 27 – **Transparency and Information to Data Subjects**

"1. Prior to or at the time of collecting personal data directly from a data subject, the data controller shall provide the data subject with clear, easily understandable, and accessible information including:
a. The identity and contact details of the data controller, and where applicable, the contact details of the Data Protection Officer.
b. The specific, explicit, and legitimate purposes of processing the personal data, and the legal basis relied upon.
c. The categories of personal data to be processed.
d. The recipients or categories of recipients to whom the personal data will be disclosed, including whether such recipients are located within or outside the Kingdom of Cambodia.
e. The period for which the personal data will be retained, or the criteria used to determine such period.
f. The rights of the data subject under this Law and the procedures for exercising such rights, including the right to withdraw consent where processing is based on consent.
g. The right to lodge a complaint with the data controller and with the Ministry of Post and Telecommunications.
h. Where applicable, information regarding transfers of personal data outside the Kingdom of Cambodia and the safeguards applied for such transfers.
i. Where applicable, the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the potential consequences of such processing for the data subject.

2.Where the personal data has not been obtained directly from the data subject, the data controller shall additionally inform the data subject of:
a. The source from which the personal data originates; and

b. The categories of personal data involved.

3.The information referred to in paragraph (2) shall be provided to the data subject within one (1) month from the date on which the personal data is obtained or at the time of the first communication with the data subject, whichever is earlier.

4.Paragraph (3) shall not apply where:
a. The data subject already possesses the information referred to in paragraphs (1) and (2);
b. The provision of such information is impossible or would require disproportionate effort, taking into account the number of data subjects, age of data, or cost of communication;
c. Obtaining or disclosing the personal data is expressly required by law and appropriate safeguards are in place to protect the data subject's legitimate interests; or
d. The personal data must remain confidential subject to an obligation of professional secrecy or legal confidentiality.

5.Where the purposes of processing or the recipients of personal data change after the information has been provided to the data subject, the data controller shall inform the data subject of such changes before processing for the new purpose takes place."

24. 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.

24.1 Key Observations

The right of access is one of the foundational mechanisms for ensuring that personal data protection laws are not merely symbolic. Article 28 establishes this right but currently takes a narrow approach that limits its practical effectiveness. Strong access rights empower individuals to understand how their data is used, challenge misuse, and meaningfully exercise other related rights such as correction, deletion, portability, or objection. Without robust access provisions, broader data subject protections become harder to realize and enforce. The current draft has several strengths: it affirms a clear right to obtain a copy of personal data held by the controller; it acknowledges access rights in the context of cross-border data transfers; and. it reinforces transparency and accountability obligations outlined elsewhere in the law. These are important pillars in strengthening public trust and enabling rights-based data governance in Cambodia.

24.2 Weaknesses and Gaps

Despite its strong starting point, several critical components are missing:

24.2.1 Scope of the right is too limited

The provision does not require controllers to confirm whether processing is taking place or to provide essential contextual information such as processing purposes, categories of data, recipients, or retention periods. Access without context prevents informed decision-making.

24.2.2 No timeline or procedural safeguards

There is no legal deadline for responding to access requests, no requirement to provide access in a clear or accessible format, and no standard for identity verification. These omissions risk delays, inconsistent practice, or even accidental disclosure of data to the wrong person.

24.2.3 No balance between transparency and legitimate restrictions

The draft does not address situations where disclosure might infringe the privacy of others, conflict with secrecy obligations, or jeopardize investigations. Controllers need legal clarity on when redaction or refusal is permitted. In many jurisdictions, the laws allow data controllers to refuse access in certain limited circumstances.

24.2.4 Limited clarity on cross-border safeguards

The reference to Article 23 is helpful but vague. Individuals should be able to obtain meaningful information about the specific protection m mechanisms for their data, especially if transferred to jurisdictions with weaker privacy regimes.

24.3 Recommendations for Improvement

24.3.1 Expand the right to include confirmation of processing and a list of required supplementary information (purposes, categories, recipients, retention period/criteria, DPO contact, automated decision-making, transfer safeguards).

24.3.2 Set a clearer procedural rule - how to make a request, proof of identity, etc. apart from matters provided for in Article 26. This makes this foundational right of access operational.

24.3.3 Provide balanced exemptions - allow refusal or redaction when disclosure would adversely affect others' rights, public security, confidentiality obligations, or ongoing investigations — but require the controller to give reasons and appeal route.

24.3.4 Require transfer safeguards to be disclosed concretely - when applicable (e.g., name of third-country recipient category, legal basis for transfer, safeguards such as adequacy/contractual clauses). Tie this to the existing transfer rules in Article 23 for

consistency.

23.3.5 Add portability and rectification linkage - access should be coupled with clear routes to request rectification, portability, or restriction where appropriate. Many regional laws combine these rights to promote active data subject control.

23.4 Proposed Revised Text

Article 28 – Right to Access

"1. The data subject has the right to obtain from the data controller confirmation as to whether personal data concerning them is being processed, and, where that is the case, access to such personal data.

2. Upon request, the data controller shall provide the data subject with the following information in a clear and accessible form:
a. the purposes of the processing
b. the categories of personal data being processed
c. the recipients or categories of recipients to whom the personal data has been or will be disclosed, including where recipients are located outside the Kingdom of Cambodia
d. the data retention period, or if not possible, the criteria used to determine such period
e. the source of the personal data, if it was not collected directly from the data subject
f. information on the existence of automated decision-making, including profiling, and the significance and consequences for the data subject
g. the rights of the data subject to request rectification, erasure, restriction of processing, and to file a complaint to the supervisory authority

3. The data controller shall provide a copy of the personal data undergoing processing free of charge for the first copy. A reasonable fee may be charged for additional copies where requests are manifestly excessive or repetitive.

4. Where personal data is transferred outside the Kingdom of Cambodia, the data subject shall have the right to obtain information regarding the appropriate safeguards applied to the protection of such data in accordance with this law.

5. A data controller may refuse to act on a request that is manifestly unfounded or excessive. In such cases, the data controller shall notify the data subject of the reasons for refusal and provide information on the right to lodge a complaint with the supervisory authority."

24. 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.

24.1 Key Observations and Recommendations for Improvement

The current draft provision establishes an important right for individuals to rectify inaccurate personal data. This supports trust in digital services and aligns with international data protection principles. However, the current text combines rectification with restriction of processing in a way that creates ambiguity and may weaken enforceability. Targeted improvements are necessary to ensure legal clarity, protect individuals effectively, and provide business-friendly compliance obligations. Several key gaps and weaknesses have been identified.

24.1.1 Lack of transparency in broader data ecosystems

There is no requirement to inform third-party recipients of corrected data, reducing the practical benefit of rectification. This is a common element in every data protection law.

Recommendation – require notification to recipients. Ensure that rectified data propagates to all third parties who have received the inaccurate data.

24.1.2 Ambiguous notification exemption

The current wording “impossible or exceeds the capacity” is too broad and could allow unjustified avoidance of compliance duties.

Recommendation - Clarify the condition for non-notification. Use internationally recognized language such as “disproportionate effort” to balance burdens with accountability.

24.1.3 No rules for refusal

The provision does not address excessive requests, identity verification, or notification of rights when a request is rejected.

Recommendation - Introduce refusal safeguards. Mandate justification for any refusal and inform individuals of their right to complain to MPTC.

25. 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 available that is required to be erased, as stated in paragraph 1 above, the data controller shall take 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 take 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 fulfilment 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 defence 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.

25.1 Key Observations

The Article establishes the right of individuals to request the erasure of their personal data under specific circumstances. This right is a cornerstone of modern data protection law and reflects global principles, including the GDPR's "right to be forgotten" (Article 17). It is intended to give data subjects control over personal data that is no longer necessary, processed unlawfully, or when consent is withdrawn. The provision also addresses public disclosure and exceptions to the right, highlighting awareness of complex data ecosystems and competing public interests.

There are several strengths of the provision: Firstly, comprehensive triggers for erasure - the article correctly identifies key scenarios where erasure is warranted: data no longer necessary, withdrawal of consent, objection to processing, unlawful processing, or legal obligations. This aligns with international best practice and supports fairness and accountability. Secondly, recognition of public disclosure challenges - including measures for publicly available data demonstrates awareness of modern data environments, such as social media and online repositories, where erasure may require coordination with other controllers. Thirdly, inclusion of legitimate exceptions - the listed exceptions (freedom of expression, legal obligations, public health, research, archival, legal claims) balance the right to erasure with other societal, legal, and economic interests, mirroring GDPR Article 17(3) and ASEAN regulations.

25.2 Weaknesses and Gaps

Several gaps and areas for improvement have been identified.

25.2.1 Vague obligations for publicly disclosed data

The clause on notifying other controllers is imprecise. Phrases like "may taking into account and consider the use of available technology and cost" are open to interpretation and could undermine compliance.

Recommendation - Use clear, enforceable language: "The controller shall take reasonable steps to notify other controllers to remove links or copies within a reasonable timeframe, taking into account proportionality and available technology."

25.2.2 Procedural gaps

The law does not specify how identity verification, refusal of unfounded requests, or communication of reasons for denial should occur. These procedural elements are critical to

both enforceability and fairness.

Recommendation - Include identity verification, handling of manifestly unfounded requests, communication of refusal with reasons, and the right to lodge complaints with the supervisory authority.

25.2.3 Ambiguous exceptions language

Exceptions do not specify that they only apply "to the extent necessary," potentially allowing overbroad interpretations that could undermine the erasure right.

Recommendation - Specify that exceptions apply "only to the extent necessary" to balance erasure rights with other legal, public interest, and research purposes.

26. 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.

26.1 Key Observations

The right to restriction of processing serves as an intermediate safeguard between full processing and complete erasure of personal data. Its purpose is to allow a data subject to temporarily limit how their personal data is used while disputes over accuracy, legality, necessity, or objection are resolved. In policy terms, this right operationalizes the principles of: (1) Fairness and accountability — preventing misuse of contested data, (2) Accuracy and proportionality — ensuring processing reflects verified, lawful, and necessary data, and (3) Data subject empowerment — enabling individuals to pause data use without losing it entirely (especially important for evidence or legal claims).

This right is critical in balancing competing interests: the data subject's privacy rights versus the data controller's need to retain information for legitimate business, legal, or public purposes.

26.2 Weaknesses, Gaps and Recommendations for Improvement

26.2.1 Procedural Weakness

No duty to mark or label data as restricted within internal systems. No guidance on communication — whether restriction requests must be written, signed, or electronic. No clarity on duration — how long data may remain restricted and when it should revert to active or be erased.

Mandate written or electronic request forms standardized by the MPTC and require notification to data subject upon restriction, activation, or lifting of restriction.

26.2.2 Oversight and Accountability Gaps

No reporting or recordkeeping requirement for controllers to document restrictions. No obligation to notify processors or third parties who previously received the data. Broad exceptions ("national interest," "rights of others") risk misuse, especially without proportionality tests or MPTC oversight.

The law must require controllers to record and justify all restriction requests and any decision

to override restriction for national interest or others' rights. It must also require periodic review (e.g., every six months) of restricted data to determine whether continued retention is justified, and MPTC should issue technical and procedural guidelines

26.2.3 Substantive Weakness

Unclear relation to data retention policies. Controllers may retain restricted data indefinitely, defeating the purpose. No right to be informed of refusal. If the controller rejects a restriction request, there is no obligation to explain or provide recourse. No link to remedies or complaint process. The article does not mention the right to file a complaint to the Ministry or supervisory authority if the controller fails to comply.

Clarify interaction with right to erasure (Article 30) and right to object (Article 33) — for instance, restriction may evolve into erasure if the basis for retention no longer applies. Add remedy clause: data subjects should have the right to complain to the MPTC and seek judicial review. Include penalties for non-compliance such as failure to notify, misuse of restricted data, or neglecting restriction requests.

Other recommendations: (1) controllers should mark restricted data (e.g., digital "flagging" or tagging systems), (2) require notification to third-party recipients so that restriction applies downstream, (3) "National interests" and "rights of others" should be limited by necessity and proportionality tests, require written justification and possible MPTC notification when relying on those exceptions.

27. 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 exercises 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.

27.1 Key Observations

The Right to Data Portability is one of the most forward-looking rights in modern data protection law. It empowers individuals to retrieve and reuse their personal data across different services and platforms. This right enables:

- User autonomy — letting data subjects control their own information beyond the confines of one organization;
- Market competition — reducing data lock-in and promoting innovation by making it easier to switch between digital service providers;
- Transparency and fairness — ensuring individuals can access their data in usable formats; and
- Trust in digital ecosystems — allowing individuals to exercise mobility over their digital identity and records.

At its core, data portability bridges data protection and digital economy policy. It is both a privacy right and a competition enabler — encouraging open, interoperable markets while strengthening personal control.

The strengths of article 32 are:

- Recognition of a progressive data right — Cambodia joins other jurisdictions that see data portability as a key enabler of both digital trust and market innovation.
- Consent and contract-based limitation — aligning with global standards by limiting the right to situations where data subjects actively participated in data collection or use.
- Inclusion of direct transmission possibility — reflects the most advanced portability model (akin to EU and Singapore), promoting digital interoperability.
- Safeguard for rights of others — ensures balance between individual rights and protection of third-party data or confidentiality.

27. 2 Weaknesses and Gaps

The weaknesses and gaps of this provision:

27.2.1 Undefined scope of "personal data" — unclear whether the right applies only to data "provided by" the subject (like names, uploaded files) or also to observed data (usage logs, behavioral data) and derived data (profiles, analytics).

27.2.2 Broad "technical feasibility" caveat — allows controllers to deny direct transfers too easily without oversight.

27.2.3 No mention of trade secrets or IP — missing safeguards for legitimate business interests and confidential algorithms.

27.2.4 No cross-border portability provision — unclear if data can be ported to a controller outside Cambodia and what safeguards would apply.

27.3 Recommendations for Improvement

27.3.1 Limit to personal data provided by or observed from the data subject, excluding purely inferred or algorithmic data unless otherwise decided by the regulator.

27.3.2 Ensure portability does not undermine intellectual property, trade secrets, or public interest.

27.3.3 Protect third-party data — permit redaction or aggregation where other individuals' data are intermingled.

27.3.4 Portability requests involving foreign data controllers should comply with cross-border transfer rules (adequacy, contractual clauses, or explicit consent).

27.3.5 Require controllers to disclose if data is being transmitted abroad and what safeguards are used.

28. 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- 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.

28.1 – Key Observations

The right to object empowers individuals to challenge the processing of their personal data when such processing is not based on consent but instead relies on public interest or legitimate interest grounds It reflects the broader policy principle of "accountability through justification" — requiring data controllers to explain why processing is necessary despite an individual's opposition. This right serves to:

- Protect individual autonomy and privacy;
- Reinforce fairness and transparency in data processing; and
- Ensure checks and balances on broad legal bases like "public interest" or "legitimate interest," which are otherwise easily invoked by data controllers.

The provision has the following policy strengths:

- Alignment with global standards — The provision mirrors GDPR and ASEAN regulations and best practices.
- Recognition of contextual objection ("particular situation") — Protects individuals whose circumstances make processing harmful or unjustified.
- Inclusion of balancing clause — Allows data controllers to continue processing if they prove "compelling legitimate grounds," ensuring proportionality.
- Absolute right for direct marketing — Strong protection of personal autonomy against intrusive commercial profiling.
- Reference to legal claims exception — Consistent with due process principles and practical necessity.

28.2 Weaknesses and Gaps

28.2.1. Procedural and Operational Ambiguity

- No requirement to notify the data subject of the outcome (accepted or rejected).
- No obligation to temporarily restrict processing while an objection is under review — weakening effectiveness.
- No explicit linkage to Article 31 (Restriction of Processing), though they are functionally related rights.

28.2.2 Substantive Uncertainty

- Undefined "reasons related to particular situation" — may confuse both data subjects and controllers. Needs examples (e.g., risk of discrimination, harm to dignity, or personal safety).
- Broad "compelling legitimate grounds" exception — gives controllers too much discretion without regulatory oversight.
- Direct marketing scope unclear — should include profiling, targeted advertising, and automated decision-making for marketing purposes.

28.2.3 Enforcement and Oversight Deficit

- No requirement for the controller to document the balancing test or notify the regulator.
- No clear burden of proof rule — under best practice, the controller should prove its grounds override the individual's interests.
- No regulatory power to audit or verify that "compelling legitimate grounds" were properly assessed.

28.3 Recommendations for Improvement

28.3.1 Add Clear Procedure and Timelines

- Acknowledgment within 7 days of receiving an objection.
- Decision within 30 days, extendable once with justification.
- Temporary restriction of processing during review, unless processing is legally required or necessary for vital interests.
- Written notification of the outcome and the reasons for acceptance or refusal.

28.3.2 Clarify Substantive Standards

- Define "reasons related to the data subject's particular situation" — e.g., risks to safety, discrimination, or moral harm.
- Require that any "compelling legitimate grounds" be:
    - Documented,
    - Proportionate, and
    - Demonstrably overriding the data subject's rights and freedoms.
- Specify that the burden of proof rests on the data controller.
- Clarify that the right to object covers all forms of direct marketing, including:
    - Targeted advertising;
    - Profiling for marketing purposes; and
    - Data sharing with marketing affiliates.

28.3.3 Enhance Oversight and Accountability

- Require controllers to record and retain objection requests and their assessment outcomes.
- Empower the MPTC to audit objection decisions.
- Provide complaint and appeal mechanisms for rejected objections.

28.3.4 Integrate with Related Rights

- Cross-reference Article 31 (Right to Restriction) to ensure interim protection when an objection is raised.
- Clarify interaction with other rights (e.g., access, erasure, portability).
- Ensure consistent language regarding legitimate interest and public interest.

28.3.5 Strengthen Transparency

- Controllers must inform data subjects of their right to object at the time of first communication and in the privacy notice.
- Require periodic publication of aggregate statistics on objection outcomes for accountability.

28.4 – Proposed Revised Text

Article 33 –The Right to Object Processing

"(*1) A data subject shall have the right, at any time and on grounds relating to their particular situation, to object to the processing of their personal data where such processing is based on:*
a) The performance of a task carried out in the public interest or in the exercise of official authority; or
b) The legitimate interests pursued by the data controller or a third party.

(*2) Upon receiving an objection, the data controller shall temporarily restrict processing pending assessment, and shall within 30 days decide whether to uphold or reject the objection, providing written reasons.*

(3) The data controller shall cease processing unless it demonstrates compelling legitimate grounds that override the interests, rights, or freedoms of the data subject, or that the processing is necessary for the establishment, exercise, or defense of legal claims.

(4) The data subject shall have an absolute right to object at any time to the processing of personal data for direct marketing purposes, including profiling related to direct marketing.

(5) The data controller shall inform the data subject of the right to object clearly and separately

at the time of first communication and in its privacy notice.

29. 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.

29.1 Key Observations

The provision grants data subjects the right to request human involvement where automated decisions produce legal or similarly significant effects. This right aims to safeguard individual autonomy, fairness, and accountability in an era where automated or algorithmic decision-making systems increasingly affect access to employment, credit, insurance, education, and public services. This provision is one of the most technically complex and ethically significant aspects of modern data protection law.

29.2 Weaknesses and Gaps

The intention aligns with global data protection principles—EU GDPR, OECD Guidelines and many national legislations. However, several weaknesses and gaps exist:

29.2.1 Scope and Conceptual Clarity

- No definition of “automated decision” or “profiling”: The text assumes their meaning but does not define them. In GDPR Article 4(4), profiling is explicitly defined as automated processing to evaluate personal aspects (e.g., performance, behaviour, location, preferences).
- “Legal effects” and “similarly affects” are vague: The terms are not operationalized. For

example, does rejection of a job application by an automated system qualify? How about algorithmic credit scoring or social media content moderation?

Without definitional precision, both data subjects and controllers will face uncertainty about the scope of the right and the compliance obligations.

29.2.2 Limited Right to Human Involvement

The article states that the data subject has the right to request human involvement only when an automated decision produces legal or similar effects.

- This is weaker than the GDPR approach, which provides a general prohibition on such decisions unless specific safeguards are met.
- "Right to request human involvement" is a reactive mechanism, placing the burden on the individual rather than obligating controllers to ensure human oversight proactively.
- It lacks reference to transparency duties (e.g., informing the individual when an automated decision occurs, what logic is used, and what data influences it).

Individuals may not know that an automated decision has been made at all—rendering the right meaningless in practice.

29.2.3 Exemptions Too Broad and Insufficiently Safeguarded

Paragraph 2 provides three exemptions: a) contractual necessity, b) legal authorization, and c) explicit consent. These mirror GDPR Article 22(2), but the safeguards are weaker in implementation:

- Under (a) and (c), the text only requires "appropriate measures" without specifying their nature or enforceability.
- There is no obligation of risk assessment, impact evaluation, or human oversight during system design (as seen in GDPR Articles 25 & 35).
- The inclusion of (c) – consent – can be problematic, since consent in automated systems is often illusory or coerced (e.g., "click-to-accept" without understanding algorithmic consequences).

The safeguards may be too soft to prevent algorithmic harms such as bias, discrimination, or opacity.

29.2.4 Absence of Transparency and Accountability Measures

The provision is silent on:

- Notification to the data subject when such automated decision-making is applied.
- The obligation to explain the underlying logic, decision parameters, or the significance of profiling results.
- Documentation and audit requirements for automated systems.

Without mandatory transparency, the right to human involvement cannot be exercised effectively.

29.3 Recommendations for Improvement

29.3.1 Define Key Concepts

Add a dedicated definitions clause or cross-reference to general definitions:

- "Automated decision-making": processing that occurs without human involvement and produces legal or similar effects on an individual.
- "Profiling": automated processing to evaluate or predict aspects of a person's performance, preferences, behavior, or location.
- "Legal or similarly significant effects": include rejection of services, differential pricing, denial of credit, or employment-related decisions.

29.3.2 Strengthen the Right and Shift from "Reactive" to "Preventive"

Reformulate paragraph 1 as follows:

"*Data subjects shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects them, unless specific safeguards apply*."

This mirrors GDPR Article 22(1) and creates a prohibition-first model. Human involvement should be built-in by default, not only upon request.

29.3.3 Clarify Safeguards and Human Oversight Obligations

Amend paragraph 3 to include explicit safeguards:

- The right to obtain meaningful information about the logic involved in the decision.
- The right to contest the decision and obtain human review.
- Obligation for controllers to ensure human oversight in system design and operation (accountability by design).
- Requirement to conduct a Data Protection Impact Assessment (DPIA) for high-risk automated systems.

29.3.5 Address Transparency and Information Duties

Insert a new clause:

"*Where a decision is made based solely on automated processing, the data controller shall inform the data subject, at the time of decision-making, of the use of such processing, the logic involved, and the significance and possible consequences for the data subject*."

This ensures informed participation and algorithmic accountability.

29.3.6 Narrow or Condition the Consent Exemption

Explicit consent (paragraph 2(c)) should be conditioned on:

- A clear explanation of the processing logic and consequences.
- Freely given and specific consent—not bundled into general terms.
- The ability to withdraw consent easily, triggering cessation of automated processing.

29.3.7 Introduce Oversight and Redress Mechanisms

- Require controllers to maintain records of automated decision systems.
- Empower the supervisory authority to audit and prohibit unfair algorithmic processing.
- Provide for administrative penalties for failure to implement safeguards.

29.4 Proposed Revised Text

Article 34 - Automated Decision-Making and Profiling

(1) A data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

(2) Paragraph (1) shall not apply if the decision:
(a) is necessary for entering into or performing a contract between the data subject and the controller;
(b) is authorized by law; or
(c) is based on the explicit consent of the data subject.

(3) In the cases referred to in (a) and (c), the controller shall implement appropriate safeguards to protect the rights, freedoms, and legitimate interests of the data subject, including:

- *the right to obtain human intervention,*

- *the right to express their point of view,*
- *the right to contest the decision, and*
- *the right to receive meaningful information about the logic involved and the significance of such processing.*

(4) Controllers shall notify data subjects whenever an automated decision-making process is used and shall ensure transparency, fairness, and accountability consistent with applicable law and ethical principles.

30. 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.

30.1 Key Observations

The right to an "appropriate legal remedy" is a cornerstone of any effective data protection regime. It operationalizes the principle of accountability by ensuring that individuals can enforce their rights and hold data controllers responsible for breaching the law.

At its core, this article seeks to promote responsible internal governance among data controllers, while offering a pathway for data subjects to obtain redress when their rights are violated. Yet, as currently framed, it leans heavily toward internal self-regulation and provides insufficient assurance of independent or external oversight.

This article has several strengths:

- Recognition of the Right to Remedy - The provision correctly acknowledges that individuals must have legal recourse when their data protection rights are violated. This aligns with international human rights standards and global data protection frameworks.

- Encouragement of Internal Compliance Systems - By requiring controllers to develop internal complaint and redress mechanisms, the provision encourages proactive compliance, early resolution, and organizational accountability. This internal approach can reduce regulatory burdens on supervisory authorities by resolving minor or procedural grievances internally.
- Institutionalization of Complaint Mechanisms - Integrating complaint-handling procedures into internal data protection regulations fosters a culture of transparency, record-keeping, and continuous improvement within organizations.

30.2 Weaknesses, Gaps and Recommendations for Improvement

Despite these strengths, the provision's current drafting presents several policy and enforcement weaknesses that could undermine its intended protection.

30.2.1 Unclear Nature of "Appropriate Legal Remedy"

The phrase is too general. It should clarify whether remedies include:

- compensation (for material or moral harm),
- rectification or erasure of data,
- cessation of processing,
- public apology, or
- administrative sanctions.

Without this clarity, remedies may be symbolic rather than effective. Under GDPR, data subject has the right to lodge compliant with DPA, right to effective judicial remedy, right to compensation. In Malaysia, complaints can be filed with Commissioner; Commissioner can investigate & direct compliance as well as criminal prosecution. Similarly, in Thailand and Philippines, data subject may file complaint with the regulator and civil damages judicial review available.

The law should define "remedy" clearly to include compensation, correction, erasure, restriction of processing, injunctions, and non-pecuniary remedies (e.g., apologies or public corrections).

30.2.2 Absence of Independent Oversight or Escalation Route

The article does not explicitly mention the right to complain to an independent supervisory authority or to seek judicial review or compensation. Without this, internal remedies could become self-serving and non-transparent, as controllers effectively adjudicate their own misconduct.

The law should embed multi-level redress pathways to guarantee that the right to an "appropriate legal remedy" includes: (a) internal complaint to the controller, (b) external complaint to the supervisory authority, and (c) judicial remedy or civil action for damages, and ensure each path is complementary, not mutually exclusive.

30.2.3 No Procedural Safeguards

There are no acknowledgment requirements, or communication duties for how complaints should be handled internally. This omission risks making internal mechanisms slow,

inconsistent, or inaccessible, particularly for vulnerable or less informed individuals.

The law should require controllers to: acknowledge receipt of complaints (within 7 days), provide written response within specify time frame (30 days), offer reasoned decisions and escalation options, and preserve relevant records and evidence.

30.2.4 Lack of Transparency and Public Reporting

Controllers are not required to publish complaint procedures, report statistics, or demonstrate compliance. This lack of transparency impedes public confidence and prevents supervisory bodies from monitoring systemic issues.

The law should oblige controllers to publish complaint-handling procedures and submit annual statistics on received complaints and resolutions to the supervisory authority.

30.2.5 Limited Protection for Complainants

No mention is made of non-retaliation, confidentiality, or support for complainants. This discourages individuals from exercising their rights, particularly in employment or service-provider contexts.

The law should make provisions to prohibit retaliation or discrimination against complainants and ensure confidentiality of personal data related to the complaint.

31. 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.

31.1 Key Observations

This clause delegates the procedural implementation of data subject rights—such as access, correction, erasure, objection, and restriction—to a subordinate instrument called the Common Guidelines for Personal Data Protection. Such delegation is intended to provide administrative flexibility, enabling the supervisory authority or relevant ministry to issue technical guidance without constant legislative amendment. This can promote adaptability as technology, data practices, and compliance standards evolve.

The strengths of this clause are:

- Administrative Flexibility and Responsiveness - Delegating procedural detail to guidelines allows regulators to update requirements more easily in response to

technological and operational developments. This is valuable in the data protection field, where digital platforms, automation, and AI evolve rapidly.

- Consistency Across Sectors - A unified "Common Guideline" approach may help harmonize implementation across industries and government agencies, ensuring standardized handling of rights requests.
- Facilitates Technical Specificity - Certain procedural aspects—forms, verification methods, digital submission platforms, and timelines—are better suited for administrative guidance than rigid statutory text.
- Encourages Capacity Building and Best Practice Sharing - Common Guidelines can incorporate examples, templates, and step-by-step procedures, helping controllers (especially SMEs) comply more easily.

31.2 Weaknesses and Gaps

From a policy perspective, however, the provision also raises concerns about legal certainty, accountability, and effective access to rights. The balance between flexibility and the protection of fundamental rights must be carefully managed to ensure that delegation does not become a loophole for weakening enforceable rights.

31.2.1 "The conditions"

In legal drafting, "conditions" are substantive qualifiers — they define whether and when a right can be exercised. It refers to the circumstances or prerequisites under which a right may be exercised. They are not mere procedures; they determine the existence, scope, and limits of a legal entitlement. Leaving the determination of conditions to "Common Guidelines" means that a non-legislative instrument — issued by an administrative authority — could effectively define, limit, or suspend the exercise of data subject rights.

This raises serious policy and legal concerns: (a) undue administrative power, (b) erosion of legal certainty, (c) contradiction with international standards, and (d) potential for inequality and arbitrary implementation.

31.2.2 Excessive Delegation of Core Right

The exercise of fundamental data subject rights is a matter of substantive justice, not merely procedure. Leaving "conditions, formalities, and procedures" entirely to guidelines risks allowing administrative rules to redefine or restrict the scope of rights through secondary regulation—without legislative scrutiny or parliamentary oversight.

31.2.3 Legal Uncertainty

If the Guidelines are non-binding or lack legal clarity, both data subjects and data controllers may be uncertain about their legal obligations or entitlements. This undermines predictability

and enforceability, key pillars of the rule of law.

31.2.4 Potential Erosion of Rights through Bureaucratic Barriers

Without safeguards, guidelines could impose burdensome formalities—for example, excessive identity verification, fees, or restrictive timeframes—that effectively discourage individuals from exercising their rights.

31.3 Recommendations for Improvement

31.3.1 "Conditions"

This word should be removed from the clause to prevent unintended delegation of substantive rule-making power over data subject rights. The law itself should clearly prescribe the conditions under which these rights may be exercised, while the Common Guidelines should be confined to setting out formalities and procedural mechanisms for implementation.

This amendment will strengthen legal certainty, preserve the integrity of individual rights, and align the law with international best practice.

31.3.2 Mandate transparency and consultation in developing Guidelines

Public trust and legitimacy require consultation with stakeholders — including civil society, industry, and academia — before issuing the Guidelines.

This builds transparency, participation, and legitimacy, reduces future resistance and compliance disputes, and promotes a multi-stakeholder approach, consistent with international best practice.

31.3.3 Require periodic review and adaptation

Technology evolves; rules must too. Regular review ensures relevance without constant legal amendment.

32. 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.

32.1 Key Observations

The draft provision currently empowers line ministries or institutions to issue Supplementary Guidelines for Sectoral Personal Data Protection by Prakas, after consulting the Ministry of Post and Telecommunications (MPTC). While this approach ensures ministerial involvement, it reflects a top-down regulatory model that may prove rigid, fragmented, and ill-suited to Cambodia's fast-evolving digital economy.

Globally, jurisdictions with mature data protection frameworks — such as the EU GDPR Singapore, Malaysia, Thailand, and the Philippines — have adopted a co-regulatory approach, allowing industry associations or professional bodies to develop sectoral codes of practice, subject to review and approval by the central data protection authority. This ensures that sectoral practices remain consistent with national principles while reflecting the technical realities and needs of each industry.

The digital economy thrives on innovation, trust, and regulatory clarity. Relying solely on ministerial Prakas to operationalize privacy obligations risks creating multiple and inconsistent sectoral regimes, where similar data processing activities are governed by different interpretations across ministries.

By contrast, empowering industry associations to take the lead in developing sector-specific codes — under MPTC's supervision — can foster greater compliance ownership, practical standards, and adaptive governance aligned with international best practice. This model shifts the focus from government control to shared responsibility, enabling the private sector to act as a compliance partner rather than a passive rule-taker.

32.2 Weaknesses and Gaps

32.2.1 Fragmentation and Overlap

Multiple ministries issuing separate Prakas could lead to inconsistent obligations, particularly for cross-sector actors such as cloud service providers, fintech companies, and e-commerce platforms.

32.2.2 Limited Technical Expertise

Ministries may lack the sectoral insight and technological depth required to design nuanced data protection standards for complex digital systems.

32.2.3 Slow Regulatory Response

Formal regulatory processes are time-consuming and may not keep pace with technological and

business innovations.

32.2.4 Low Stakeholder Buy-in

Industry players are less likely to internalize or champion compliance with rules developed without their participation.

32.3 – Recommendations for Improvement

Cambodia's personal data protection framework must balance governmental oversight with industry expertise and agility. Entrusting line ministries alone with sectoral guidelines risks over-regulation, inconsistency, and low compliance culture.

Adopting an industry-led, MPTC-approved co-regulatory model would be a forward-looking reform — flexible, participatory, and innovation-friendly — ensuring that data protection standards are practical, consistent, and credible both domestically and internationally.

This model would strengthen trust, promote digital transformation, and demonstrate Cambodia's readiness to uphold internationally recognized data protection principles while fostering a vibrant and responsible digital economy.

To ensure consistency, efficiency, and adaptability, it is recommended that the current clause be revised to provide that:

Sectoral Codes of Practice on personal data protection may be developed by industry associations, professional bodies, or representative organizations, in consultation with relevant line ministries. These codes shall be submitted to MPTC for review, approval, and registration, to ensure alignment with the Common Guidelines and national data protection law.

33. 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.

33.1 Key Observations

The requirement for data controllers and processors to develop Internal Regulations on Personal Data Protection (IRPDP) is a vital mechanism for operationalizing compliance with the law.
It institutionalizes data protection within each organization by requiring senior-level approval and ongoing review of technical and organizational measures. The strengths of the draft law are:

- requires controllers/processors to adopt internal regulations and tie them to Common / Sectoral Guidelines.
- links measures to risk, scale, purpose — endorsing a risk-based approach.
- requires management approval and ongoing review.

This provision is the backbone of organizational accountability in Cambodia's data protection regime. However, in its current draft, the provision functions mainly as a statement of intent rather than a robust framework for demonstrable accountability.
It mandates internal rules but does not specify:

- the scope and minimum content of those rules;
- the documentation or evidentiary requirements to prove compliance;
- the review frequency, or
- the supervisory authority's role in oversight and enforcement.

Without these elements, implementation risks becoming uneven, symbolic, and difficult to audit.

33.2 Recommendations for Improvement

To serve its purpose, it must move beyond generality to prescribe minimum standards, documentation requirements, and oversight powers. The recommendations are:

33.2.1 Clarify the Minimum Content of Internal Regulations

Specify that Internal Regulations must include, at a minimum:

- risk assessment and mitigation measures;
- security controls (access control, encryption, logging, backups);
- breach detection and response procedures;
- data retention and deletion schedules;
- staff training and disciplinary provisions; and
- vendor and processor management policies.

This ensures uniformity and allows for sectoral tailoring through guidelines.

33.2.2. Establish Documentation and Evidentiary Requirements

Controllers and processors should be legally required to:

- maintain written records of processing activities,
- document Data Protection Impact Assessments (DPIAs) for high-risk operations, and
- retain audit logs and incident reports.

This converts “demonstrate compliance” into an enforceable and auditable duty.

33.2.3. Mandate Periodic Review and Updates

Include a minimum review frequency (e.g., annually) and specify that updates must be made upon material business, technological, or legal change. This ensures living compliance rather than static documents.

33.2.4. Strengthen Oversight by MPTC

Grant MPTC explicit power to:

- request copies of Internal Regulations,
- conduct audits or inspections, and
- issue corrective directions or administrative sanctions if internal controls are absent or inadequate.

This transforms the obligation into an enforceable compliance pillar.

33.2.5 Reference Recognized Standards and Sectoral Flexibility

Allow organizations to align their internal controls with recognized frameworks (e.g., ISO 27001, NIST, COBIT), while requiring conformity with the Common Guidelines. This balances international best practice with national regulatory coherence.

33.2.6 Support for SMEs

Provide simplified templates and proportional obligations for small and medium-sized enterprises to prevent compliance fatigue while maintaining minimum safeguards

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

Personal data inspection 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.

34.1 Key Observations

The provision establishing the duties and rights of personal data inspection inspectors represents a cornerstone of Cambodia's data protection enforcement regime. However, while the article intends to empower inspectors to ensure compliance, its current wording risks granting overbroad, loosely defined powers without sufficient legal safeguards, procedural clarity, or accountability mechanisms. This weakens both legal certainty and public trust in data protection enforcement.

While strong enforcement is essential, effective regulators act through administrative investigation and compliance monitoring, not criminal-style suppression. Comparable authorities in Singapore, Thailand, and Malaysia exercise investigative and corrective—not coercive—functions.
Leaving seizure powers undefined risks constitutional or procedural conflicts with law enforcement authorities.

Delegating the "formalities and procedures" entirely to a ministerial Prakas undermines legal predictability. Fundamental elements of inspection—such as authorization, confidentiality, and appeal—should be embedded in the primary law, while only technical details (inspection checklists, documentation formats) should be delegated.

34.2 Recommendations for Improvement

To align this provision with international norms and good governance principles, the following amendments are strongly recommended:

34.2.1 Refine the scope of powers

Replace “suppress” with “prevent and take enforcement action against” to clarify that inspectors act in an administrative capacity, not as criminal investigators.

34.2.2 Embed procedural safeguards in the law

Require written authorization for inspections; ensure proportionality and due process; and provide the right to receive inspection reports and to appeal enforcement decisions.

34.2.3 Impose confidentiality and integrity obligations

Mandate inspectors to maintain strict confidentiality over personal or business data obtained and to use such data solely for enforcement purposes.

34.2.4 Enhance transparency and accountability

Require inspectors to prepare written reports for each inspection and to submit them to the Ministry; include disciplinary sanctions for misuse of power or unauthorized disclosure.

34.2.5 Ensure professional standards

Require inspectors to undergo formal training in data protection law, digital forensics, and ethical conduct before exercising their powers.

34.2.6 Retain detailed procedural rules in the Prakas

While the Prakas should define the technical formalities and procedures, fundamental rights and principles must be enshrined in the law itself, ensuring legal force and protection against arbitrary exercise of power.

35. 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.

35.1 Key Observations

This provision seeks to establish coordination between the MPTC inspectors and other enforcement agencies — including local authorities and armed forces — during the investigation of offenses under the Personal Data Protection Law (PDPL). It also mandates that such operations comply with the Criminal Procedure Code (CPC) and outlines procedures for situations of in flagrante delicto (caught in the act).

It allows personal data inspectors — who are administrative officers under a civilian ministry — to engage in activities such as "suppression of offenses" and coordination with armed forces. This language implies quasi-policing or military functions beyond the MPTC's lawful administrative scope. In established data protection systems (e.g., EU, Singapore, Malaysia, Thailand), data inspectors do not conduct criminal suppression; they refer cases to law enforcement for prosecution.

Authorizing "armed force units" to assist in "suppression of offenses" raises profound rule-of-law and human-rights concerns. The armed forces are not designed for civilian data enforcement, and their involvement in administrative investigations — absent clear legal basis and safeguards — can intimidate citizens, disrupt businesses, and violate international human rights norms. Even in serious cyber or data crimes, military support should be limited to technical assistance and only upon judicial or ministerial authorization.

The term in flagrante delicto (caught in the act) is undefined. Without strict criteria, it could be misused to justify warrantless searches or seizures. International standards require that emergency powers be necessary, proportionate, time-limited, and subject to judicial review. The draft provision provides none of these guarantees.

The term "operation" in the clause is problematic and should definitely be reconsidered. The word "operation" is typically used in military, police, or security contexts — e.g., "military operation," "police operation," or "enforcement operation." Its use in a civilian regulatory law (like data protection) creates an unintended militaristic tone, implying the use of coercive or forceful measures. This contradicts the rights-based, administrative nature of data protection oversight.

Moreover, the term "operation" diverges from international standards, as no data protection or administrative enforcement law globally uses this expression. Jurisdictions such as the EU, Singapore, and Thailand use legally defined terms such as "inspection" or "investigation," reflecting a rights-based and procedural approach rather than a coercive or militaristic one.

35.2 Recommendations for Improvement

To align this provision with international norms and good governance principles, the following amendments are strongly recommended:

35.2.1 The term “operation”

It should be replaced, as it is not used in any international data protection legislation and conveys an enforcement tone inconsistent with the administrative and procedural character of data protection regulation. More appropriate alternatives include “inspection and investigation activities” or “investigation procedures.”

35.2.2 Restrict use of armed forces and set strict conditions for assistance

Prohibit routine use of armed forces except where constitutionally and legally authorised, and only with prior approval from the Minister and a judicial or executive emergency authorization where required. Prefer police or civilian law-enforcement for operational assistance.

35.2.3 Define and limit “in flagrante delicto”

Provide an objective, narrow definition (e.g., when a person is caught in the act committing an offence and immediate action is necessary to prevent loss of life, serious material harm, or destruction of evidence). Require written after-action justification and supervisory review.

35.2.4 Require written requests/authorisations and documentation for assistance

Any request for assistance from local authorities, police, or armed forces must be: (a) documented in writing (or contemporaneous written note if urgent), (b) include legal basis and scope, and (c) be logged and reported to MPTC within a fixed timeframe.

35.2.5 Specify warrant vs. exigent-circumstance rules for searches/seizures

Searches and seizures must follow the CPC and ordinarily require a judicial warrant. Allow exceptions only for narrowly defined exigent circumstances (e.g., imminent destruction of evidence) with mandatory later judicial validation.

35.2.6 Embed confidentiality, chain of custody, and limited use rules

Joint operations must include safeguards: sealed evidence, limited access lists, non-disclosure obligations, restricted retention and purpose limitation, and return or secure destruction protocols for non-relevant material.

35.2.7 Introduce oversight, reporting, and remedy mechanisms

Require MPTC to publish anonymised aggregate reports on joint operations annually. Provide inspected parties with written inspection/seizure recor.ds and a right to complain or seek judicial review if procedures were breached.

36. 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.

36.1 Key Observations

The current draft provision on Penalties provides that violations of the law may give rise to administrative and criminal sanctions. Specifically, administrative penalties include written warnings, fines, and restrictions, with enforcement authority vested in the Ministry of Post and Telecommunications (MPTC). Rules and procedures for enforcement are to be further prescribed by a Prakas of the Minister. Criminal penalties are stated to be governed by Article 51 of the law.

The provision distinguishes between administrative and criminal penalties but does not define criteria or thresholds for each. This lack of differentiation may result in inconsistent or arbitrary enforcement, where similar violations are treated differently depending on interpretation.

In a sound regulatory framework, administrative penalties are appropriate for minor or negligent violations, while criminal sanctions should be reserved for intentional, reckless, or large-scale data breaches that cause harm to individuals or national interests.

The phrase “administrative penalties” in the draft law conflates two distinct ideas:

- Administrative measures/sanctions — non-punitive regulatory actions (warnings, orders, suspensions, etc.) designed to ensure compliance; and
- Penalties or sanctions — punitive actions (fines, revocations, etc.) designed to punish wrongdoing.

In administrative law theory, “penalty” implies punishment, which presupposes legal guilt and due process similar to criminal law. This can conflict with constitutional and rule-of-law principles, which usually reserve punitive powers to the judiciary or legally independent

tribunals.

In contrast, **"**administrative measures," "enforcement actions," or "corrective measures**"** are broader, more flexible, and less punitive terms—making them better suited to regulatory contexts like data protection.

The law already provides for criminal penalties in Article 51. Keeping the word "penalties" under both administrative and criminal sections blurs the distinction between: (administrative enforcement (regulation and compliance); and (ii) Criminal prosecution (punishment and deterrence). This overlap weakens the principle of legal certainty, because it is unclear which forum or standard of proof applies. EU GDPR, laws in Indonesia, Thailand, Singapore, Malaysia, etc. deliberately avoid "administrative penalty" to ensure conceptual clarity and constitutional compatibility.

The draft law also states "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."

The use of the word **"**rules" in that clause is problematic — both **l**egally and institutionally. It seems minor at first glance, but in the context of a law on personal data protection, the term "rules" can create serious ambiguity and even constitutional or administrative inconsistencies. Therefore, giving a minister the power to determine "rules" by Prakas risks over-delegation of legislative authority, contrary to the principle of legality (nullum crimen sine lege and nulla poena sine lege). In short, A Prakas can set procedures**,** guidelines, or implementation measures — but not rules that create new rights, duties, or sanctions.

36.2 Recommendations for Improvement and Proposed Revised Text

To Improve the provision, it is recommended: (1) The title of the Article to be substituted with "Enforcement Measures and Sanctions", (2) Replace "Administrative Penalties" with "Administrative Measures and Fines" and (3) Remove the term "rules".

Here is a revised version to improve legal clarity and aligns with international norms:

Article 47 – Enforcement Measures and Sanctions

"(*1) Violations of this Law may result in enforcement measures and sanctions appropriate to the nature and seriousness of the violation.*

(2) Administrative measures may include:
(a) written warnings or reprimands;
(b) orders to rectify, delete, or restrict processing of personal data;

(c) suspension of data processing activities;
(d) administrative fines as prescribed by this Law and related regulations.

(3) The Ministry of Post and Telecommunications, or the designated Data Protection Authority, shall implement such measures in accordance with transparent and fair procedures, ensuring the right of the alleged violator to be notified, to respond, and to appeal.

(4) Detailed procedures and standards for enforcement shall be established by a Prakas of the Minister, consistent with the principles of legality, proportionality, and due process.

(5) Criminal sanctions shall apply only to intentional, reckless, or large-scale violations as specified in Article 51 of this Law."

37. 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.

37.1 Key Observations

This clause on administrative fines is one of the most critical parts of the law, because it determines the fairness, enforceability, and credibility of the entire data protection regime. It is one of the core enforcement tools of modern data protection regimes. The policy purpose is not to punish like criminal law, but to:

- Deter non-compliance by creating credible financial consequences;
- Promote accountability by encouraging compliance systems and risk-based controls; and
- Enable responsive regulation, allowing the supervisory authority to apply proportionate measures without resorting to the courts.

In this sense, fines are both economic regulators and compliance incentives**.** However, to serve that function effectively, the law must make them predictable, proportionate**,** and enforceable. Poorly drafted penalty clauses can lead to overreach, arbitrary enforcement, and legal challenges that weaken the credibility of the authority.

37.2 Weaknesses and Gaps

37.2.1 Overbroad scope and lack of differentiation

The clause penalizes “any person who does not comply with any of the provisions” in four full chapters of the law (chapters 3-6) -regardless of the seriousness of the offense. This collapses all violations (from minor administrative lapses to massive data breaches) into a single penalty class. The significant policy risks are: (i) violates principle of proportionality; (ii) creates uncertainty and enforcement discretion too broad to be legitimate; and (iii) makes judicial review difficult (courts lack clear benchmarks for reasonableness).

37.2.2 Ambiguity in the cap structure (fixed vs percentage)

The wording “not exceed 600,000,000 Riels or 10% of turnover” is ambiguous. It’s unclear whether the fine can reach the greater or lesser of the two, or if the authority must choose between them. 10% of turnover could vastly exceed 600 million Riel for large corporations, while being meaningless for small ones. Under GDPR, it is based on tiered by severity 10M EUR/20M EUR or 2per cent/4 per cent of global turn over. Singapore PDPA, up to IM SGD or 10 per cent of annual turnover, whichever is higher. Under Malaysia PDPA, flats fine up to 1M. Cambodia’s current draft law can lead to enforcement inconsistency; perception of unpredictability or unfair treatment; and potential conflict with constitutional requirements for clarity of sanctions.

37.2.3 Conceptual and practical confusion in “annual income” definition

The clause uses the terms “annual turnover” and “annual income”. It defines “annual income” based on audited statements recognized by the Ministry of Economy and Finance — but: “income” is not the same as “turnover”.” Income” commonly means net income/profit after expenses and taxes. Enforcement practice and international law use “turnover” (gross revenue) for fines because turnover better reflects economic capacity to pay. Requiring a “recognized auditor” introduces bureaucratic delay and politicization. Also, the law does not address cases where audited accounts are unavailable or falsified. Many SMEs or newly-formed entities may not have audited accounts. Requiring audits can stall enforcement or unfairly benefit non-compliant actors.

This confusion can lead to enforcement paralysis; disputes over financial figures; risk of manipulation.

37.2.4 Lack of procedural safeguards

The clause is silent on: the right to be notified, the right to respond before a fine is imposed, or the publication of decisions. This violates due process and fair administrative action principles,

exposes fines to annulment by courts, and damages the law's credibility internationally.

37.2.5 Structural risks: compliance costs and investor confidence

Foreign investors and tech companies require predictability. Unclear penalty structures discourage data localization, innovation, and investment in compliance. Predictable, transparent, tiered sanctions are viewed as hallmarks of a mature data protection regime, often used to assess cross-border data adequacy.

37.3 Recommendations for Improvement

To address these issues and enhance the provision, the following suggestions are strongly recommended**:**

37.3.1 Adopt a tiered approach

Proportionality principle requires monetary sanctions to be tied to the seriousness of the infringement:

- Minor / technical breaches → warning, corrective order, small fine.
- Material / negligent breaches → larger fines.
- Intentional / large-scale breaches → highest fines (percentage of turnover).

37. 3.2 Clarify the turnover calculation

- Use the legal person's most recent audited consolidated annual turnover for the preceding financial year.
- Permit alternative verifiable sources where audited statements are unavailable (tax filings), with statutory hierarchy.

37.3.3 Embed procedural safeguards

Procedural safeguards must be embedded in the same enforcement chapter: notice of alleged violation, right to be heard, right to appeal to an independent court/tribunal, possibility of administrative settlement, and ability to mitigate fines for cooperation.

37.3.4 Specify apportionment and cumulative rules

Clarify if fines are per violation/per day/per data subject, and impose an annual cap per legal person (to avoid ruinous multiplicative penalties).

37.3.5 Require publication and transparency

Require anonymized publication of enforcement decisions and a periodic enforcement report.

37.3.6 Define use of proceeds

Specify whether fines go to State budget or to a dedicated fund for data protection capacity building — transparency prevents political misuse.

38. 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.

38.1 Key Observations and Recommendations for Improvement

Article 49 seeks to guide the competent authority (the Ministry of Post and Telecommunications, MPTC) in determining the amount of administrative fines under Article 48. Its aim is to ensure that penalties are: (i) proportionate (not excessive compared to the

gravity of the violation), (ii) effective (capable of deterring misconduct), and (iii) consistent (applied on the basis of predictable criteria).

This reflects good international practice, similar to Article 83(2) of the EU GDPR, section 48 of the Singapore PDPA**,** and section 66 of the Thailand PDPA.

However, the drafting and structure of this Article can be improved for clarity, coherence, and enforceability**.**

38.1.1 Nature, gravity, and duration of non-compliance (para-a)

This is a standard and essential factor, aligned with international benchmarks. It ensures that more serious or prolonged breaches attract higher fines. However, no guidance is given on how to assess "gravity" — e.g., whether harm to individuals, number of data subjects affected, or volume of data are included. This could lead to inconsistent interpretations. There is a real need to add clarifying language such as:

"*The nature, gravity and duration of the infringement shall be assessed having regard to the number of data subjects affected, the volume and sensitivity of personal data involved, and the degree of harm or risk caused*."

38.1.2 Types and characteristics of personal data affected (para-b)

Para b recognizes the importance of data sensitivity (e.g. biometric, health, or financial data). However, the phrase "types and characteristics" is vague — "characteristics" could mean anything from format to sensitivity level. It is recommended that the provision to be replaced with:

"*The sensitivity and categories of personal data affected, including whether special categories of data were involved*."

38.1.3 Financial gain or avoidance of loss (para-c)

This aligns with the principle of disgorgement (ensuring no one profits from violations). It is fair and rational. However, the clause should specify that gaining benefit or avoiding loss may be an aggravating factor to justify higher fines. There is a real need to add clarity:

"*Any financial gain obtained or loss avoided as a result of the non-compliance shall be considered as an aggravating factor*."

38.1.4 Timely and effective mitigation measures (para-d)

This factor will encourage data controllers to act quickly and responsibly after breaches — a key compliance incentive. The term "timely and effective" is good, but the article should link it to mitigation of harm to data subjects rather than just "effects and consequences." It is recommended that the provision to be rephrased:

"*The promptness and effectiveness of measures taken to mitigate or remedy the harm caused to affected data subjects*."

38.1.5 Prior efforts to implement measures (para - e)

This para recognizes good-faith efforts, even if they fail — important for fairness and regulatory encouragement. But the phrase "adequate and appropriate measures" is undefined — should reference compliance programs, data protection officers, or risk assessments. To clarify and make it clearer, it is recommended for the clause to be replaced with:

"*The extent to which the data controller had implemented appropriate technical and organizational measures, policies, and training prior to the non-compliance*."

38.1.6 Previous non-compliance (para – f)

This a standard aggravating factor; ensures repeat offenders face heavier penalties. There is a need to consider frequency and similarity of past violations. It is suggested for the paragraph to be replaced with:

"*The history of prior violations, particularly repeated or similar non-compliance*."

38.1.7 Compliance with orders or voluntary remedial actions (para-g)

This para encourages cooperation and compliance after enforcement action. However, it is redundant with (d); also, "voluntary implementation" could overlap with "mitigation." Should consolidate with (d) or clarify distinct scope. Merge with (d) as part of "post-violation conduct," or rephrase as:

"*The degree of cooperation with the competent authority and voluntary implementation of corrective measures*."

38.1.8 Proportionality and effectiveness of fines (para-h)

This clause states that the fines imposed shall be proportionate and effective, which is not a "ground" for determining fines — it's a principle. It belongs in a separate paragraph or preamble, not as a factor within the same list. Move this clause to a new Article or sub-clause that states:

"*Administrative fines shall be proportionate, effective, and dissuasive in relation to the gravity of the infringement*."

36.1.8 Impact of fines on the data controller (para-i)

This para acknowledges the need to avoid excessive penalties that cripple legitimate business operations — promotes fairness. The phrase "Impact on regular operations" is vague. Should reference financial capacity and public interest (especially for public entities or SMEs). To make it clearer, it is recommended that the paragraph be replaced with:

"*The economic capacity of the data controller and the impact of the fine on its continued lawful operations, taking into account the need for deterrence*."

38.1.8 Any other relevant grounds prescribed by laws and regulations (para-j)

This is an overly broad catch-all clause. It undermines the predictability and legality of sanctions by allowing arbitrary additional factors. Courts could find this violates the principle of legality and certainty in administrative law. Limit its scope or replace with a procedural safeguard:

"*Any other relevant factors prescribed by Sub-Decree or Prakas issued under this Law, provided that such factors are consistent with the principles of proportionality, fairness, and legal certainty*."

38.1.9 "Grounds for Administrative Fines"

Clause 49 uses the phrase "Ground for Administration Fines." This suggests that the clause defines the circumstances in which an administrative fine may be imposed — i.e., the legal grounds (the "why") that justify imposing a fine. However, in substance, the article actually deals with the criteria or factors used to determine the amount of the fine once non-compliance has been established — i.e., the how much and based on what considerations. That is a very different legal concept.

Article 49 is about assessment criteria, not the legal basis for liability. This creates confusion for enforcement and interpretation. In many jurisdictions, they avoid the word "grounds"**;** instead use "criteria," "factors," "considerations," or "conditions." It is recommended that the title of the clause to be changed to – "**Criteria for Determining Administrative Fines**"

(or) "**Factors to be Considered in Imposing Administrative Fines.**"

39. 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.

39.1 Key Observations, Weaknesses and Gaps

The clause aims to ensure prompt payment of administrative fines imposed under the law by introducing automatic multipliers for late payment (doubling after 30 days, tripling after 60 days, and court referral after 90 days). While the intention—to strengthen deterrence and ensure compliance—is legitimate, the provision as currently drafted risks violating principles of legality, proportionality, and procedural fairness, which are essential components of administrative enforcement under both Cambodian constitutional principles and international regulatory norms. The key weaknesses or policy concerns are:

39.1.1 Disproportionate and Arbitrary Escalation

The automatic doubling and tripling of fines, regardless of the nature of the offense or the amount of the original penalty, can lead to excessive and punitive outcomes. For serious offenses with high fines, the multiplication could result in amounts that are unreasonable or unenforceable, particularly for small or newly established entities. In regulatory policy, penalties must be effective, proportionate, and dissuasive, not excessive or confiscatory.

39.1.2 Absence of Procedural Safeguards

The clause provides no clear process for:

- confirming when the fine becomes final and enforceable;
- determining valid service or receipt of the payment order; or
- allowing appeals or payment deferrals.

Without these safeguards, a person may face multiplied penalties even while an appeal is

pending or before being properly notified. This undermines due process and legal certainty.

39.1.3 Overreliance on Automatic Multipliers

Automatic mathematical escalation is a blunt instrument that does not account for the reasons behind non-payment—such as insolvency, technical delays, or legitimate dispute over liability. Internationally, regulators prefer interest accrual, surcharges, or enforcement actions, which reflect actual delay or cost rather than arbitrary multiplication. No other data protection law (EU GDPR, Singapore PDPA, Thailand PDPA, Malaysia PDPA, etc) employs automatic multipliers for late payment of fines. Instead, these frameworks use: Interest on overdue fines (usually at the legal or central bank rate); administrative enforcement measures (e.g., license suspension, seizure of assets); and judicial enforcement as a last resort, following due process.

39.1.4 Ambiguity of Judicial Referral

The final paragraph ("a case filed to the competent courts… to take measures") lacks clarity on what type of proceedings the court is expected to undertake—civil enforcement, criminal prosecution, or administrative review. This vagueness weakens enforceability and risks procedural conflict between administrative and judicial authorities.

39.2 Recommendations for Improvements

The current clause, though intended to enhance compliance, risks undermining proportionality, fairness, and legal certainty. Cambodia's data protection enforcement regime should adopt a rights-based and rule-of-law approach, emphasizing due process, proportional sanctions, and transparent enforcement. Replacing automatic multipliers with clearly defined, proportionate surcharges and judicial safeguards would bring the law into line with international standards and good regulatory practice, thereby enhancing its legitimacy and effectiveness. The recommendations to be considered:

39.2.1 Replace Multipliers with Proportionate Surcharges or Interest

Substitute the doubling/tripling mechanism with a fixed surcharge (e.g., 10–20%) or statutory interest accruing per day of delay. Ensure total penalties remain proportionate and capped.

39.2.2 Clarify Enforcement Sequence and Timing

Specify that escalation applies only after the fine becomes final and enforceable (i.e., after the appeal period or decision). Define what constitutes proper service or notification of the payment order.

39.2.3 Introduce Flexibility for Payment Plans

Allow data controllers or processors to apply for deferred or instalment payment, subject to Ministry approval.

39.2.4 Define Judicial Enforcement Clearly

Replace “case filed to the competent courts” with “the Ministry shall file an application to the competent court for enforcement of the administrative decision as a civil judgment.”

39.2.5 Add Transparency and Accountability

Require the Ministry to issue procedural by Prakas detailing enforcement timelines, notice formats, and appeal processes.

39.3 Proposed Revised Text

Article 50 - Fines for Non-Payment of Fines

“*If an administrative fine remains unpaid thirty (30) days after the decision becomes final, the fined party shall be subject to a surcharge not exceeding ten percent (10%) of the unpaid amount, and statutory interest shall accrue from that date.*

If the fine remains unpaid ninety (90) days after the decision becomes final, the Ministry of Post and Telecommunications may initiate judicial enforcement proceedings before the competent court to recover the unpaid amount and related enforcement costs.”

40. 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.

40.1 Key Observations

The draft imposes criminal liability on natural and legal persons for offences in Article 48, with imprisonment of “6 days to 2 years” and fines up to 60,000,000 Riels for natural persons, and fines up to 100,000,000 Riels plus additional penalties from the Code of Criminal Procedure for

legal persons.

As discussed at para 35, article 48 is about administrative penalties including fine for the breach of provisions in chapters 3 – 6 of the law. Article 48 defines the grounds and procedures for imposing administrative penalties (warnings, fines, restrictions, etc.). These are non-criminal sanctions, handled by the Ministry of Post and Telecommunications (MPTC) under administrative procedures. So, article 48 is about regulatory enforcement — not about crimes or prosecutions.

Meanwhile, Article 51 talks about criminal liability. The article begins:

"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."

So, it says that criminal liability applies to the "offences" as specified in Article 48. This is misleading, confusing and internally inconsistent because Article 48 does not create criminal offences — it only defines administrative infractions and fines.

40.1 Weaknesses and Gaps

40.1.1 Cross-reference mixes administrative wrongs and criminal offences.

For the following reasons, without amending, this could lead to the law unworkable.

Category confusion

Administrative offences (handled by MPTC) and criminal offences (handled by courts) belong to different legal regimes. Mixing them blurs the enforcement boundary.

No clear criminal provision

If Article 48 does not define criminal acts, then Article 51 has no operative basis — courts will have no defined offence to prosecute.

Due process violation

The Constitution and Criminal Procedure Code require that criminal offences be precisely defined by law (nullum crimen sine lege). Here, the "offence" is undefined or misplaced.

Conflict of enforcement authority

MPTC can't both fine administratively and prosecute criminally under the same article — it creates double jeopardy or overlapping jurisdiction.

Legislative drafting error

The reference to Article 48 likely reflects a drafting oversight — they intended to refer to an article listing criminal offences (perhaps a missing article or misnumbered provision).

Apart from those reasons, several other weaknesses and gaps have been identified.

40.1.2 Sentencing ranges — odd minimum and unclear rationale

A minimum prison term of 6 days is unusual and practically meaningless; courts or prisons typically have minimum months. A wide band (6 days–2 years) without criteria makes sentencing arbitrary.

Perception of arbitrariness; sentences not reflective of harm; difficulty for judges to calibrate penalties. Recommendation: Replace 6 days with a more standard minimum (e.g., 6 months) for offences that merit imprisonment; reserve short custodial terms for minor criminal provisions or convert to non-custodial penalties (community work/fines).

40.1.2 Corporate fines — fixed amounts not tied to capacity

Fines for legal persons are fixed at up to 100,000,000 Riels. For large companies this may be negligible; for SMEs it may be catastrophic. Modern best practice ties corporate fines to turnover or sets proportionate maxima to be effective and dissuasive (e.g., GDPR-style % of turnover). Ineffective deterrence for large offenders; disproportionate impact on small firms. Make corporate fines proportionate and, where necessary, turnover-based

40.1.3 Corporate liability conditions — unclear mechanics

Article refers to Article 42 of Criminal Procedure Code for liability, but the draft does not spell out how corporate liability is established (attribution via agents, vicarious liability, failure to supervise). Litigation on whether an act of an employee is imputable to the corporation; lack of clarity for prosecutors.

Recommendation: Spell out grounds for attributing criminal liability to corporations: acts by senior management, systemic failures, failure to supervise, or benefit from the offence.

40.2 Recommendations for Improvement

40.2.1 Correct the cross-reference

If the intent is to criminalize certain acts (e.g. unlawful disclosure, intentional destruction, obstruction, etc.), Article 50 should refer to the appropriate criminal article, not the one on

administrative fines.

Example:

"A legal person shall be declared criminally liable in accordance with Article 42 of the Code of Criminal Procedure for the offences specified in Article X of this law. A new **"Article X – Criminal Offences"** should be added to define clearly the criminal acts.

41. Article 52 – Transitional Provision

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.

41.1 Key Observations

This clause is intended as a transitional safeguard — to prevent a legal vacuum. It ensures that existing regulations, circulars, or ministerial orders on personal data protection remain effective until new ones are issued under the new law.

Such clauses are common and useful to maintain continuity and avoid regulatory gaps. However, the way this one is currently drafted is too broad and legally imprecise, which can create confusion or even conflict with the new law.

The intent of this transitional clause is sound — to avoid a legal vacuum during the shift from fragmented data protection practices to a unified framework under the new law. However, the current formulation undermines legal certainty**,** coherence, and the supremacy of the new law. Without safeguards, it could allow outdated or contradictory ministerial rules to persist, leading to confusion, inconsistent enforcement, and possible violation of data subjects' rights.

41.2 Weaknesses and Gaps

There are several weaknesses and gaps in the clause**.**

41.2.1 Ambiguity of the term "regulations"

The clause does not specify what type of regulations are covered: Are they sub-decrees, Prakas, Guidelines, or Ministerial Decisions? Do they include internal circulars or administrative instructions? The word "regulations" (in English) is ambiguous in the Cambodian legal hierarchy, which recognizes specific instruments — law → sub-decree →

Prakas → decision → circular. Without precision, any prior document — even one inconsistent with the new law — could claim continued effect.

41.2.2 Hierarchy and supremacy conflict

The clause risks allowing old regulations (often issued under different legal frameworks or ministries) to remain operative even if they contradict the new law's provisions. That could undermine legal certainty and legislative supremacy, since under the Cambodian hierarchy of norms, a law (Chbab) must override any inconsistent sub-decree or Prakas.

Example:
If a past Prakas allowed data sharing without consent, this clause could be interpreted to keep that rule alive until MPTC issues new regulations — directly contradicting the law's data protection principles.

41.2.3 Absence of temporal or substantive limitation

The clause does not set a time limit for how long old regulations remain valid. It also does not say only provisions consistent with the new law will remain in effect. This could result in prolonged coexistence of outdated and inconsistent rules.

41.2.4 Risk of fragmented enforcement

Different ministries may have issued their own circulars or decisions on data handling (e.g., finance, health, telecommunications). If all are "carried forward," overlapping or conflicting regimes could emerge — confusing data controllers and the public.

41.2.5 No clarity on interpretive authority

Who decides whether an old regulation remains "consistent" or is "replaced"? Ideally, this authority should rest with the Ministry of Post and Telecommunications (MPTC) or Council of Ministers, not individual minister.

41.3 Recommendations for Improvement

41.3.1 Add a consistency safeguard

Clarify that only provisions consistent with this Law continue to apply. Revised draft:

"*Regulations related to personal data protection that were in force prior to the promulgation of this Law shall continue to apply only to the extent that they are not inconsistent with the provisions of this Law, and until such time as new regulations are*

issued under this Law."

This ensures the primacy of the new law and aligns with standard legislative drafting practice in Cambodia.

41.3.2 Specify regulatory instruments

To avoid ambiguity, specify the types of instruments covered — e.g., sub-decrees, Prakas, or ministerial guidelines. **Example:**

"*Existing sub-decrees, Prakas, and ministerial decisions related to personal data protection shall remain in force, insofar as they are consistent with this Law*…

41.3.3 Add a sunset or review clause

Prevent outdated regulations from remaining indefinitely by setting a transition period (e.g., 12–24 months). **Example:**

"…*provided that such existing regulations shall be reviewed and harmonized with this Law within twenty-four (24) months from its entry into force*."

This creates a legal modernization timeline and an accountability mechanism for MPTC.

41.3.4 Clarify interpretive authority

Designate who determines whether old regulations remain valid.

Example:

"*The Ministry of Post and Telecommunications shall determine the continued applicability of existing regulations and issue necessary notifications to ensure consistency with this Law*."

41.3.5 Provide for coordination

Encourage cross-ministry harmonization:

"*The Ministry of Post and Telecommunications shall coordinate with other competent ministries and institutions to review and repeal or amend inconsistent regulations*."

41.4 Proposed Revised Text

Article 52 - Transitional Provisions

"*Existing sub-decrees, Prakas, and other regulations relating to personal data protection shall remain in force only to the extent that they are consistent with the provisions of this Law, and until they are repealed, amended, or replaced by new regulations issued under this Law.*

The Ministry of Post and Telecommunications, in coordination with relevant ministries and institutions, shall review and harmonize such regulations within twenty-four (24) months from the effective date of this Law."

42. Concluding Remarks

The author wishes to express sincere appreciation to the Ministry of Posts and Telecommunications for its leadership and commitment in advancing the development of Cambodia's Draft Law on Personal Data Protection. The Ministry's openness to consultation and expert input reflects a commendable commitment to ensuring that the law is comprehensive, well-informed, and responsive to Cambodia's evolving digital landscape.

This report has been prepared with the objective of providing constructive and evidence-based recommendations to support the Ministry in refining the draft law. The analysis takes into account Cambodia's legal and institutional context while drawing on comparative experiences from regional and international data protection frameworks.

The recommendations offered throughout the report are intended to enhance the clarity, consistency, and practical enforceability of the draft provisions. They seek to ensure that the law effectively balances the protection of individuals' personal data with the facilitation of responsible data use, digital innovation, and economic development.

It is hoped that this analysis will serve as a useful reference for the Ministry and other stakeholders as they move toward the finalization and implementation of the law. The author respectfully commends the Ministry's ongoing efforts to establish a modern, transparent, and rights-based data protection framework that will strengthen public trust and position Cambodia as a leader in the region's digital transformation.