ICNL

www.icnl.org
info@icnl.org

Summary Analysis

Cambodia's Draft Law on Personal Data Protection

Introduction

In June 2025, Cambodia's Ministry of Post and Telecommunications (MPTC) circulated a revised Draft Law on Personal Data Protection (Draft PDP Law). The Draft PDP Law regulates the processing (i.e., the collection, use, and disclosure) of personal data and aims to protect the right to privacy of natural persons in Cambodia.

ICNL shared inputs on the previous version of Draft PDP Law. At the request of partners, ICNL is pleased to share a summary analysis on the Draft PDP Law to assist civil society, the MPTC and other stakeholders to better understand international human rights law and global norms and principles on data protection. This comment analyzes the English version of the Draft PDP Law shared by the MPTC when requesting inputs from civil society and development partners. Rather than addressing every aspect of the Draft PDP Law, ICNL's analysis summarizes key issues and best practices in data protection regimes to aid in revising the draft law.

International Law

Cambodia ratified the International Covenant on Civil and Political Rights (ICCPR) in 1992. The right to privacy is guaranteed by Article 17 of the ICCPR, which bars arbitrary or unlawful interference with "privacy, family, home, or correspondence." Restrictions on privacy must meet the legality, legitimacy, and necessity standards,[1] meaning that the government's ability to interfere with an individual's privacy rights must be clearly written into law, for a valid purpose, and both proportional in scope and directly related to that purpose. Government surveillance that is broad, indefinite, or secretive is a violation of international law.

In General Comment 16, the Human Rights Committee stipulated that the ICCPR not only prevents States from violating the right to privacy in ways inconsistent with Article 17, but also requires States to institute a legal framework to prohibit violations of privacy by private individuals and entities.[2] Such law must give individuals the right to know "what personal data is stored in automatic data files, and for what purposes," and "which public authorities or

[1] Electronic Freedom Foundation and Article 19, "Necessary and Proportionate: International Principles on the Application of Human Rights Law to Communications Surveillance," (May 2014), https://www.article19.org/data/files/medialibrary/37564/N&P-analysis-2-final.pdf.

[2] "States parties are under a duty themselves not to engage in interferences inconsistent with article 17 of the Covenant and to provide the legislative framework prohibiting such acts by natural or legal persons. . .. The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law." UN Human Rights Committee (HRC), *CCPR General Comment No. 16: Article 17 (Right to Privacy)* (1988) para. 10.

private individuals or bodies control or may control their files." They should also have the right to request correction of incorrect data and elimination of the data altogether. This framework forms the basis of the rights that are included in modern data protection laws, such as the European Union's General Data Protection Regulation (GDRP): the right to be informed, right of access, the right to rectification, and the right to erasure (also referred to as the right to be forgotten).[3]

Although the focus of this analysis will be on Article 17 of the ICCPR, it is relevant to note that the UN Human Rights Council has also stated that the right to privacy is closely linked to Article 19's right to freedom of opinion and expression because individuals who know or fear that their communications are being monitored by the government are less likely to express themselves freely for fear of reprisal. Similarly, when information that an individual privately communicates online is used against them in judicial proceedings or extra-judicial recrimination, the effect is to curtail speech and deter others from freely communicating their thoughts and opinions through online sites and applications.[4] Thus, a state's failure to adequately protect the right to privacy, whether online or offline, can also pose grave risks to an individual's right to freedom of expression.

Children – those under 18 years of age – are also protected by international law and have rights to privacy,[5] to access information, and to impart information online. Cambodia acceded to the Convention on the Rights of the Child (CRC) in 1992, which obligates the state to protect children's rights in close conformity with the ICCPR, with consideration to the maturity and age of the child.[6]

Positive Developments

DATA LOCALIZATION

The Draft PDP Law removes the requirement that data controllers store all collected personal data in Cambodia. Under Article 23, data controllers can send data outside of Cambodia when at least one of the enumerated conditions are met.[7] This better aligns with international best

[3] It should be noted that the GDPR includes additional rights, such as the right to data portability (the ability to obtain personal data in a format that can be used in other contexts), the right to restrict or object to the processing of personal data, and the right not to be subject to a decision based solely on automated processing of personal data. Data Protection Commission, *Your Rights Under the GDPR*, https://www.dataprotection.ie/en/individuals/rights-individuals-under-general-data-protection-regulation.

[4] U.N. Human Rights Council, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue," A/HRC/23/40 (April 2013), para. 30, 47-49.

[5] Article 16 of the Convention on the Rights of the Child state, "1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation. 2. The child has the right to the protection of the law against such interference or attacks."

[6] UN General Assembly, "Convention on the Rights of the Child" (Nov. 1989), Art. 13.

[7] Draft PDP Law, Article 23: Data Transfer outside the Kingdom of Cambodia. A data controller shall not transfer personal data outside the Kingdom of Cambodia unless one of the following conditions is fulfilled: a- The Ministry of Post and Telecommunications grants permission for the transfer of personal data. b- The data controllers assess that appropriate safeguards are in place to protect the personal data being transferred outside the Kingdom of Cambodia.
c- The transfer of personal data outside the Kingdom of Cambodia is based on specific circumstance, including but not limited to: 1. Written consent of the data subject. 2. The necessity for the performance of a contract between the data subject and the data controller. 3. Protection of public interests. 4. Protection of life of the data subject or another natural persons. 5. Protection of legitimate interests of the data subject. 6. Establishment, exercise, or defense of a legal claim or whenever courts are acting in their judicial capacity.

practices. For example, this approach seems to align with the European Union's General Data Protection Regulation (GDPR). The GDPR permits international data transfers where the receiving country has adequate data protection measures in place. Factors such as the country's adherence to the rule of law and human rights, among others, are relevant to this adequacy determination.[8]

EXEMPTION FOR NOT-FOR-PROFIT ENTITIES

Article 14 (d) allows not-for-profit bodies to process sensitive personal data of a data subject when doing so in the normal course of business and with appropriate safeguards.[9] This exemption will enable not-for-profit bodies, including civil society organizations (CSOs), trade unions and religious organizations, to utilize data of their members to carry out their lawful activities in furtherance of their goals. This exemption requires appropriate safeguards and prevents the disclosure of data to entities outside of the organization. This provision strikes the correct balance between protecting privacy and protecting the right to freedom of association.

Key concerns

OVERBROAD EXEMPTIONS FROM CERTAIN PROTECTIONS OF PERSONAL DATA

ISSUE: The Draft PDP Law establishes the rights of data subjects and the responsibilities of data controllers and data processers. These responsibilities include obtaining consent from data subjects prior to processing their personal data, ensuring the integrity and accuracy of personal data, only retaining personal data that is necessary for a specific purpose, giving data subjects access to their personal data when requested, and observing appropriate security safeguards. Despite strong language about data protection, however, the Draft PDP Law also includes broad exceptions to the requirements that undermine its stated goal of safeguarding privacy.

Article 7 provides that the processing of personal data can only occur when based on: consent of the data subject; necessity to perform a contract; necessity to perform legal obligations; necessity to protect "the vital interests of the data subject or another natural person;" necessity to "perform a task carried out in the public interest;" or necessity for the "legitimate interests pursued by the data controller or a third party."[10]

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.

[8] GDPR, Article 45(1)-(2).

[9] Draft PDP Law, Article 14(d): The processing of sensitive personal data shall be prohibited. The first paragraph above shall not apply if the data controllers process personal data in compliance with legal bases as stipulated in Article 7 of this law and at least one of the following additional conditions: In the course of its legitimate activities by a not-for-profit body with a political, philosophical, religious or trade union related to the members or to former members of the body or to persons who have regular contact with it. In this case, the not-for-profit body shall have appropriate safeguards for the processing of personal data and shall not disclose the personal data outside that body without the consent of the data subjects.

[10] Draft PDP Law, Article 7: Legal Basis for Processing Personal Data. The processing of personal data shall be based on one of the following legal basis: a- Consent of the data subject. b- The necessity of performing a contract to which the data subject is a party, or at the request of the data subject prior to entering into a contract. c- The necessity of the data controller to perform legal obligations as required by law. d- The necessity for the

Similarly, Article 14 allows for the processing of "sensitive personal data,"[11] when done in compliance with one of the bases outlined in Article 7 and with any of the nine bases contained in Article 14.[12]

There are several problematic bases for the processing of personal data or sensitive personal data under Articles 7 and 14. These include: the vital interests of the data subject or another natural person (Article 7(d) and Article 14(c)), when in "the public interest" (Article 7(e) and Article 14(g)), necessity for the "legitimate interests" of a data controller or a third party (Article 7(f)), and for "archiving purposes in the public interest, scientific or historical research purposes or statistical purposes" (Article 14(g)).

Under these provisions a data controller may process personal data or sensitive personal data *without* the consent of the data subject. These broad, wide-ranging exemptions, which remove the requirement to obtain the consent of the data subject, do not meet international best practices.

ANALYSIS: 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.[13] 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),[14] and should be an appropriate and

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.

[11] In the Annex to the Draft PDP Law, "Sensitive Personal Data" is defined as: "Refer[ing] to personal data revealing racial origin, political opinions, religious or philosophical beliefs, or trade union membership, biometric data, genetic data, health data, and data concerning the sex life or sexual orientation of a natural person."

[12] Draft PDP Law, Article 14: The protection of Sensitive Personal Data. The processing of sensitive personal data shall be prohibited. The first paragraph above shall not apply if the data controllers process personal data in compliance with legal bases as stipulated in Article 7 of this law and at least one of the following additional conditions: a- Explicit consent of the data subject. b- The necessity for the purposes of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection as determined by law. c- The necessity for the protection of the vital interests of the data subject or of other natural persons where the data subject is physically or legally incapable of giving consent. d- In the course of its legitimate activities by a not-for-profit body with a political, philosophical, religious or trade union related to the members or to former members of the body or to persons who have regular contact with it. In this case, the not-for-profit body shall have appropriate safeguards for the processing of personal data and shall not disclose the personal data outside that body without the consent of the data subjects. e- Personal data has manifestly been made public by the data subject. f- The necessity for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity. g- The necessity for reasons of substantial public interest as determined by laws. In this case, the processing of personal data shall be proportionate to the purpose of the processing, respect the essence of right, shall be subject to suitable and specific measures to safeguard the fundamental rights and freedoms of the data subject. h- The necessity for the purpose of preventive or occupational medicine or for reason of public health as determined by laws and shall be subject to suitable and specific measures to safeguard the fundamental rights and freedoms of the data subject. i- The necessity for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes as shall be determined by laws. In this case, the processing of personal data shall be proportionate to the purpose of processing, respect the essence of right, shall be subject to suitable and specific measures to safeguard the fundamental rights and freedoms of the data subject.

[13] UN Human Rights Committee (HRC), *CCPR General Comment No. 16: Article 17 (Right to Privacy)* (1988) para. 10.

[14] Legitimate purposes are those that protect the rights or reputations of others, have national security or public order aims, or pursue the interest of public health or morals.

proportionate response and directly related to that legitimate aim (proportionality principle).[15]

It is considered good practice to limit exemptions from protecting personal data to circumstances where the public interest outweighs the interests of the data subject. The GDPR allows data controllers to exercise exemptions to certain data protections when there is a national or public interest that is greater than the interests of the individual. General guidance for the GDPR emphasizes that a data controller may only rely upon an exemption if it would otherwise be unfeasible to uphold the rights and principles under the GDPR.[16]

While there is no definitive list of legitimate interests that justify exemptions to personal data protections, the GDPR mentions examples of legitimate interests including marketing, fraud prevention, and IT security, among others.[17] Similarly, the United Kingdom (UK)'s GDPR defines "fraud prevention," "ensuring network and information security," and "indicating possible criminal acts or threats to public security" to constitute a "legitimate interest" that may justify an exemption to a protection of personal data.[18] The UK's GDPR also grants data controllers an exception to the general prohibition on processing special categories of data if there is a "substantial public interest" in doing so. The UK's GDPR sets out twenty-three "public interest conditions" in detail, which the UK's Information Commissioner's Office (ICO) explains are "narrowly drawn" and require data controllers to meet specific criteria.[19] These limitations from both the EU and UK make clear that exemptions from processing personal data are to be narrowly interpreted.

Unlike in the GDPR or the UK's GDPR, the exemptions in Articles 7 and 14 of the Draft PDP Law are vaguely worded and thus may encourage violations to the rights to privacy because they could allow a data controller to unilaterally process data. These restrictions on the right to privacy do not meet the legality test because they are so broadly worded that they grant a data controller broad discretion to determine that an exemption applies, which harms the privacy of individual.

> *Article 7(d) and Article 14(c)*: Without a definition of "vital interest," a data controller could argue that profits are a vital interest, thus enabling a social media company to undertake and justify all types of processing.
>
> *Article 7(e) and Article 14(g):* Without a definition of "public interest," data controllers are empowered to claim that knowing the number of adherents to a certain religion or ethnicity is in the "public interest" and it would then be allowed to process personal and sensitive personal data without consent of the data subject.

[15] Electronic Freedom Foundation and Article 19, "Necessary and Proportionate: International Principles on the Application of Human Rights Law to Communications Surveillance," (May 2014), https://www.article19.org/data/files/medialibrary/37564/N&P-analysis-2-final.pdf.
[16] Net Lawman Limited, "Exemptions," available at https://www.netlawman.co.uk/know-your-privacy-rights/exemptions.
[17] GDPR EU, "GDPR Legitimate Interests," https://www.gdpreu.org/the-regulation/key-concepts/legitimate-interest/.
[18] Information Commisioner's Office, "What is the 'legitimate interests' basis?" https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/legitimate-interests/what-is-the-legitimate-interests-basis/#article_61f.
[19] Information Commissioner's Office, "What are the substantial public interest conditions?," https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/what-are-the-substantial-public-interest-conditions/.

Article 12's clarifications of when a data controller can use this exception is not clear enough to meet the legality test.[20]

Article 7(f): Without further guidance on grounds that are "legitimate," a data controller could find a wide range of reasons to process a data subject's data. Article 13's clarifications of when a data controller can use this exception is not clear enough to meet the legality test.[21]

Article 14(g): This broadly-worded article would allow a data controller to deem any type of research or archive to be in the "public interest" thus enabling processing sensitive personal data without the data subject's consent.

While there is no definitive list of legitimate interests that justify exemptions to personal data protections, the GDPR mentions examples of legitimate interests including marketing, fraud prevention, and IT security, among others.[22] Similarly, the United Kingdom (UK)'s GDPR defines "fraud prevention," "ensuring network and information security," and "indicating possible criminal acts or threats to public security" to constitute a "legitimate interest" that may justify an exemption to a protection of personal data.[23] The UK's GDPR also grants data controllers an exception to the general prohibition on processing special categories of data if there is a "substantial public interest" in doing so. The UK's GDPR sets out twenty-three "public interest conditions" in detail, which the UK's Information Commissioner's Office (ICO) explains are "narrowly drawn" and require data controllers to meet specific criteria.[24] These limitations from both the EU and UK make clear that exemptions from processing personal data are to be narrowly interpreted.

These exceptions to the consent requirement are concerning because they enable the data controller to unilaterally process protected data based on undefined concepts of legitimate and operational interests. Taken together, these exemptions do not afford individuals or legal entities in Cambodia with any meaningful data protections for either private or public sector processing of data. In effect, they serve to invalidate the data protection principles of the Draft PDP Law and disempower data subjects.

---

[20] See, Draft PDP Law, 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.

[21] See, Draft PDP Law, 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).

[22] GDPR EU, "GDPR Legitimate Interests," https://www.gdpreu.org/the-regulation/key-concepts/legitimate-interest/.

[23] Information Commissioner's Office, "What is the 'legitimate interests' basis?" https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/legitimate-interests/what-is-the-legitimate-interests-basis/#article_61f.

[24] Information Commissioner's Office, "What are the substantial public interest conditions?," https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/what-are-the-substantial-public-interest-conditions/.

RECOMMENDATION: Review all exemptions to the processing of personal data and sensitive personal data in Articles 7 and 14, in consultation with human rights, privacy, and cybersecurity experts, and in consideration of legal frameworks for data protection in other jurisdictions, such as the United Kingdom and Brazil. Revise exemptions to ensure the exemptions are limited to those that are proportionate to a legitimate interest in order to ensure data subjects still have meaningful rights over the processing of their personal data.

PROCESSING OF SENSITIVE PERSONAL DATA WITHOUT CONSENT

ISSUE: A data controller may process sensitive personal data without the consent of the data subject when the sensitive personal data "has manifestly been made public by the data subject."[25] While this is an improvement from previous drafts of the law and follows the GDPR, it is necessary to narrowly interpret this exemption.

ANALYSIS: Many data privacy laws at the regional, national, and sub-national levels allow data controllers to process "publicly available" personal data without the data subject's consent. For example, the EU's GDPR exempts information that is "manifestly made public" by the data subject from general data protections. An EU data protection expert explains that this exemption should be narrowly interpreted, noting as an example that publishing personal data in a biography or article in the press is different from posting a message containing personal data on social media.[26] The UK's ICO similarly warns that data collectors should be careful about using information found on social media because it may be difficult to show that a person has manifestly made information public when posting on social media.[27] Social media users that post about their political opinions, beliefs, or other sensitive information with the intent of sharing with their friends and family may not be aware that their information is public and accessible to third parties to be processed in ways that they did not intend. Processing that data would be incompatible with the object and purpose of the data protection law.

RECOMMENDATION: Revise Article 14(e) to clarify that "manifestly publicly available" means that the data subject deliberately made the information public and does not include data published on social media.

LACK OF INDEPENDENT DATA PROTECTION OFFICE/AUTHORITY

ISSUE: The Ministry of Post and Telecommunications serves as the personal data protection office.[28]

ANALYSIS: Independence is widely regarded to be essential to the efficacy of data protection authorities. Accreditation to the International Conference of Data Protection and Privacy Commissioners (ICDPPC) requires that members have appropriate autonomy and independence," and a ICDPPC white paper details the characteristics of an independent authority, such as fixed terms for commissioners, removal of commissioners only for cause,

[25] Draft PDP Law, Article 14(e).
[26] European Data Protection Supervisor, "A Preliminary Opinion on Data Protection and Scientific Research" (Jan. 2020), pg. 19, https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.
[27] Information Commissioner's Office, "What are the conditions for processing?" (Aug. 2023), https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/what-are-the-conditions-for-processing/.
[28] Draft PDP Law, Article 4.

and a dedicated budget that is fully within the authority's control. The ICDPPC's Interpretation also references the United Nations' Paris Principles on national human rights institutions, which adds that adequate funding of such institutions is necessary for their independence. The EU's GDPR in Articles 53 and 54 on the independence of data protection supervisory authorities and the OECD's report on Being an Independent Regulator echo these indicators for independence.

Any law or policy that formally establishes the Data Protection Board should ensure that board is independent and that members from civil society and academia are part of it. Without independence, there is considerable risk that the Data Protection Board can be politically weaponized and used to target CSOs, human rights defenders, media outlets, political parties, or other entities that might criticize or threaten the government. Establishing an independent data protection office mitigates risks of political considerations influencing the office's data protection decisions.

RECOMMENDATION: Revise Article 4 to include terms adapted from the ICDPPC's indicators for independence of data regulators.

LACK OF SUPPORT TO LOW-RESOURCED ORGANIZATIONS

ISSUE: Because CSOs are non-profit entities and do not always have access to large amounts of funding, date protection laws should make adjustments that enable CSOs to comply with the law without jeopardizing their ability to operate.

ANALYSIS: The reality is that certain businesses and associations will need assistance and time to adjust their internal processes to comply with the mandates of the Draft PDP Law. Article 24 requires all data controllers and data processors to "appoint a personal data protection officer who possesses the qualifications to practice the personal data protection."[29] Under this article, all entities, including CSOs, could be required to hire a new staff member specifically to ensure compliance with the Data Protection Law. Even if a new hire is not required, it will take time for all entities to properly train existing staff so that they have the requisite qualifications to be the data protection officer.

It will likely take businesses and organizations several weeks after the enactment of a data protection law to create internal processes to comply with the mandates of the law and will need advice on how to do so. For example, following the adoption of the GDPR, civil society organizations based in Europe stated that they faced difficulty ensuring their internal policies, procedures, and tech infrastructure enabled compliance.[30] Even with the grace period

[29] Draft PDP Law, 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.

[30] Open Society Foundations, "Civil Society Organizations and General Data Protection Regulation Compliance: Challenges, Opportunities, and Best Practices" (2020), https://reliefweb.int/sites/reliefweb.int/files/resources/civil-society-organizations-and-gdpr-compliance-20200210.pdf.

afforded in the GDPR, European nonprofits stated that they did not receive adequate compliance advice and that the advice that was available was not tailored to their needs. Many nonprofits reported paying a substantial portion of their overhead for compliance advice and upgrades to their tech and security infrastructure.[31]

RECOMMENDATION: Provide a grace period to socialize the new requirements, enable entities to get into compliance, or to provide support to help low-resourced entities like small businesses and nonprofits/CSOs. Including a grace period and compliance assistance, particularly to small businesses and nonprofits, will mitigate the risk that associations in Cambodia will be unduly disadvantaged.

Conclusion

ICNL appreciates the opportunity to analyze the Draft PDP Law. The Draft PDP Law does an admirable job of protecting individuals' personal data. The issues highlighted in this analysis, while problematic, are easily fixed through the suggested recommendations. Revising these provisions would significantly enhance data protection and the privacy of people in Cambodia. For further information or queries, please contact ICNL's Digital Rights Team (digital@icnl.org).

[31] Id.