April 6, 2021

Comments by the Centre for Information Policy Leadership on Vietnam's Draft Decree on Personal Data Protection

The Centre for Information Policy Leadership (CIPL)[1] welcomes this opportunity to provide comments to the Ministry of Public Security (MPS) of Vietnam on the Draft Decree on Personal Data Protection (Draft Decree). CIPL regularly contributes to public consultations and discussions around privacy both globally and in the Asia-Pacific region. For example, in Asia CIPL has provided input to government bodies regarding India's Personal Data Protection Bill,[2] Amendments to Singapore's Personal Data Protection Act (PDPA)[3] and China's Draft Personal Information Protection Law (PIPL).[4] CIPL also regularly participates in the annual Asia Pacific Privacy Authorities (APPA) Forum and the meetings of the APEC Data Privacy Subgroup (DPS) and the APEC Digital Economy Steering Group (DESG). Moreover, CIPL has held various joint workshops and events with data protection authorities in the region, including the Japan Personal Information Protection Commission, Hong Kong Office of the Privacy Commissioner for Personal Data and Singapore Personal Data Protection Commission.

CIPL welcomes the MPS's efforts to create a comprehensive and effective data protection law for Vietnam. The current proposal contains many important data protection elements that are common to other major global data protection regimes. It also includes provisions that we believe could be improved to increase the final law's effectiveness both in providing relevant privacy protections for Vietnamese citizens, and enabling a flourishing digital economy in Vietnam. Thus, our specific recommendations and suggested modifications of the Draft Decree are focused mainly on Vietnam's ability to innovate and participate effectively in the global digital economy while at the same time providing essential data protection for its people. Due to time constraints, we were not able to include comments on every provision in the Draft Decree, but the fact that we did not comment on a particular provision or article of the Draft Decree does not mean that we fully support it, or would not have comments on it in the future if the opportunity arose. Please note that our comments are not based on the original Vietnamese text, but on an English translation. Thus, to the extent our comments reflect any misunderstanding of any of the issues, they should be understood in that light.

---

[1] CIPL is a global data privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and over 85 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

[2] See CIPL Response to the Indian Joint Parliamentary Committee on the 2019 Personal Data Protection Bill, 21 February 2020, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_indian_joint_parliamentary_committee_on_the_personal_data_protection_bill_2019__21_february_2020_.pdf.

[3] See CIPL Response to Singapore Public Consultation for Approaches to Managing Personal Data in the Digital Economy, 20 September 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_singapore_public_consultation_for_approaches_to_managing_personal_data_in_the_digital_economy.pdf.

[4] See CPIL Comments on China's Draft Personal Information Protection Law, 18 November 2020, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_chinas_draft_personal_information_protection_law__18_november_2020_-_english_.pdf.

Summary of CIPL Recommendations

- Add an accountability principle to Art. 3 as the principle through which organisations are responsible for and required to be able to demonstrate compliance with the Draft Decree.

- Introduce a distinction between data controllers and data processors that is consistent with global norms.

- Revise the Draft Decree to enable a risk-based approach for defining and processing "sensitive personal data" rather than providing set categories of pre-defined sensitive data. To the extent such pre-defined categories are retained in the Draft Decree, remove personal financial data and personal location data from the definition.

- Remove the registration requirement for sensitive personal data and replace it with requirements for organizations to document and conduct an impact assessment on their sensitive data processing activities that can be made available to the PDPC upon request.

- Introduce the necessary safeguards for the proper exercise of data subject rights to ensure that other legitimate interests, including public interest and rights of third parties, are not unduly affected.

- The Draft Decree should avoid its current over reliance on consent and the associated limitations and problems (including consent fatigue), and should embrace a basis for processing model that includes all standard bases for processing found in other major data protection laws, including a legitimate interest basis for processing.

- Remove language requiring that consent must be in a format that can be printed or copied in writing, as it is not clear how this requirement would be applied to a digital environment.

- Expand the scope of Art. 13 to enable automated decision-making for purposes beyond the performance or execution of a contract (e.g., fraud prevention, network and information security, national security such as in the context of airport travel, to grant loans, etc.). CIPL recommends that the MPS does not define a static list of permissible scenarios but rather allows organizations to make such decisions based on appropriate risk assessments and mitigations.

- Reserve the requirement to consent to automate decision-making for the most impactful and high-risk automated decisions. Guidance as to what constitutes such decisions could be provided by the PDPC and rebuttable by the organization based on relevant assessments of risk.

- Introduce an age of consent for processing of personal data in Vietnam and clarify that parental consent applies only where the processing is based on consent, and the child has not yet reached the age of consent, which we recommend should be 13.

- Enable personal data processors to make a contextual determination based on a number of factors to determine whether they are processing the personal data of children in order to meet the requirements of Art. 14 for mixed audience websites and services.

- Clarify the exceptions to the data transfer conditions to ensure that they do not overlap with the conditions themselves.

- Revise Art. 21 to remove the requirement to obtain consent on top of the other requirements to transfer personal data overseas.

- Enable Vietnam's participation in the APEC Cross-Border Privacy Rules (CBPR) and APEC Privacy Recognition for Processors (PRP) systems.

- Remove the requirement to store original data in Vietnam.

- Remove the ex ante registration requirement for cross-border data transfers from the Draft Decree and replace it with documentation and risk assessment requirements that can be requested in the case of an investigation or audit.

- Include a comprehensive set of available cross-border transfer mechanisms to enable accountable global data flows.

- Provide an exemption for intra-company transfers, including the transfer of employee related data, outside of Vietnam by global companies.

- Notifying the PDPC of data breaches should only be required when the breach is likely to result in significant harm to a data subject.

- Ensure that the term "promptly" as it relates to data breach notification is interpreted to mean as soon as is reasonable under the circumstances.

- Extend the date of effectiveness in Art. 29 in the Draft Decree to at least two years from when it is passed into law to ensure that organizations will have sufficient time to become fully compliant.

Comments

I. Accountability

For many years, CIPL has promoted the concept of organizational accountability as an essential building block of effective privacy and data protection. The concept of accountability holds that organizations should adopt measures that implement applicable privacy requirements and that they should be able to demonstrate the existence and effectiveness of such measures both internally and externally upon request.[5] Effectively, this means that organizations should implement technical and organizational measures and tools that enable legal compliance, which typically means implementing comprehensive privacy and data governance programs that cover all aspects of data processing, including collection, use, transfer to third parties, and disposal. Examples of such accountability

[5] See CIPL white papers on "The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society", 23 July 2018, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf; CIPL Accountability Q&A, 3 July 2019, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_q_a__3_july_2019_.pdf; and "What Good and Effective Data Privacy Accountability Looks Like: Mapping Organizations' Practices to the CIPL Accountability Framework," 3 June 2020, available at https://www.informationpolicycentre.com/organizational-accountability.html.

requirements can be found in the EU General Data Protection Regulation (GDPR), the Brazil General Personal Data Protection Law (LGPD), and Singapore's PDPA.[6]

Organizational accountability provides significant benefits to all stakeholders—the organizations themselves, individuals and regulators. It enables compliance with legal requirements and confers consumer trust and competitive advantages on businesses, provides for consistent and effective protection for individuals and their data, and makes regulators' jobs easier by simplifying investigations and increasing organizational transparency.

The concept of organizational accountability is not currently explicitly addressed in the Draft Decree, and the MPS should reconsider this omission. It puts the onus of demonstrating compliance on the organizations themselves, supporting regulatory activity and enforcement, and has shown to be a fundamental aspect of any modern data protection law. As such, the MPS should add an accountability principle to the list of "personal data protection principles" in Art. 3.

Recommendation: Add an accountability principle to Art. 3 as the principle through which organisations are responsible for and required to be able to demonstrate compliance with the Draft Decree.

II. Controller/Processor Distinction

The Draft Decree should further differentiate the distinction between controllers and processors of personal data, as it currently uses the term "data processors" interchangeably for those actors, whereas other international frameworks provide a key distinction between them. In the Draft Decree, it appears that the concepts of controller and processor have been conflated under the definition of "personal data processor," while service parties would potentially be captured by the notion of "third party."

It is worth clarifying that data controllers are the set of actors who decide on the means and purpose of the processing activity, and often controllers rely on service providers to actually perform the processing activities they control. These service providers, often known as "data processors" in other global privacy laws, must follow the instructions and directions of the controller, but are also responsible for ensuring their own compliance with relevant parts of the data protection law, such as data security requirements. However, there is significant overlap between the concepts of controller and processor and the definitions provided by the Draft Decree, which creates confusion about the responsibilities of each set of actors. Also, we note that service providers are not third parties in the data processing operation, but rather key players in the processing and a crucial part of the relationship between controllers and individuals. Consistent, well-established definitions of controllers and processor will bring the Draft Decree in line with modern laws on data protection and avoid legal uncertainty and unnecessary compliance costs for organizations active in Vietnam.

Recommendation: Introduce a distinction between data controllers and data processors that is consistent with global norms.

III. Processing Sensitive Personal Data

A. Definition of "Sensitive Personal Data" (Article 2, Clause 3)

[6] See, e.g., GDPR, Art. 24; Brazil Law No. 13.709 of 14 August 2018, General Personal Data Protection Law (as amended by Law No. 13.853 of 8 July 2019) (LGPD', Article 51; and Singapore Personal Data Protection Act 2012, Sec. 12.

Under the Draft Decree, the definition of "sensitive personal data" includes 11 different categories of data such as biometric data, financial data, "personal data about social relationships," etc. The definition is not aligned to global norms, and as a result will be challenging for global companies to implement.

CIPL does not recommend establishing pre-identified categories of "sensitive personal data" as sensitivity of processing is very much context driven. Processing a particular category of personal data may not carry the same risks in all processing contexts and imposing unnecessary limitations on the processing may have unintended consequences on organizations' ability to effectively develop, apply, and provide digital products and services. Instead, we recommend a risk-based approach to privacy protection that requires organizations to subject all their processing activities to a risk analysis and requires them to establish mitigations and controls appropriate to the actual risks involved. This does not mean that the law (or subsequent regulations) cannot include examples of what kinds of personal data might be particularly sensitive, but such examples should be treated as guidelines to be taken into account when conducting a context-specific risk assessment rather than as automatic and invariable triggers of heightened requirements or limitations on the use of such personal data. In other words, any categories of "sensitive personal data" set forth in the law (or in subsequent regulatory guidance) should be rebuttable presumptions, whereby organizations can demonstrate through risk assessments and appropriate mitigations that in the specific context the processing at issue is not high risk or particularly sensitive. However, to the extent that the MPS decides to include such a category in its law, CIPL has some concerns around the Draft Decree's definition of sensitive personal data.

The definition currently includes personal financial data and personal location data as types of sensitive data. Such types of personal data are regularly processed by personal data processors, and including them in the definition would hinder many common processing operations. For example, workplaces often process financial data for payroll and salary purposes and personal location data is regularly processed to deliver various forms of location-based services, including rideshare and taxi services, GPS and map applications, and weather forecast information. This also means that all organizations in the financial ecosystem, both domestic and abroad, that process personal financial data will need to register with the Personal Data Protection Commission (PDPC) in order to process financial data. This will include local and foreign banks, payment schemes, wallet providers, payment gateways and even potentially merchants that collect financial data from data subjects for purposes of payment.

Considering the registration requirements for processing sensitive personal data (discussed in detail below), including such information in the definition of sensitive personal data would likely prove particularly burdensome for organizations. CIPL recommends removing personal financial data and personal location data from the definition of sensitive personal data (to the extent this concept is retained in the law). Keeping commonly used datasets under the definition of sensitive personal data would likely create interoperability issues for organizations in Vietnam and additional obstacles for Vietnamese companies when doing business globally.

Recommendation: Revise the Draft Decree to enable a risk-based and contextual approach for defining and processing "sensitive personal data" rather than providing set categories of pre-defined sensitive data. To the extent such pre-defined categories are retained in the Draft Decree, remove personal financial data and personal location data from the definition.

B. Registration of processing of sensitive personal data (Art. 20)

The Draft Decree requires sensitive personal data to be registered with the PDPC prior to processing unless one of several narrow exceptions applies. The registration process includes: 1) an application for processing sensitive personal data, 2) an impact assessment report, and 3) any documentation related to the contents of the application and impact assessment.

CIPL is concerned that an ex ante approval for processing sensitive data could greatly disrupt the day-to-day operations of thousands of businesses operating in Vietnam, especially considering the broad definition of sensitive personal data currently included in the Draft Decree. As mentioned above, under the current definition of sensitive personal data, common processing activities like processing payroll data and processing personal location data for maps and rideshare services would require registration with the PDPC prior to processing. Additionally, it will cost organizations significant time, money and human resources to complete the registration process. Overall, this requirement increases the burden of organizations doing business in Vietnam compared to other jurisdictions and places an obligation to register sensitive data on processors who may have no primary responsibility for such data.

Further, given the sheer volume of sensitive personal data that organizations will need to process on a daily basis, the PDPC is likely to be inundated with registration applications from thousands of organizations, and it is unlikely it will be able to process the registrations within 20 working days, as envisioned by Art. 20.3. Likely it will take the PDPC significantly longer to process these registrations to the point that it will have a serious impact on the operations of many organizations operating in Vietnam. This problem is further exacerbated by the fact that it is unclear when or how often organizations must register with the PDPC prior to processing sensitive personal data. It appears, at the very least, that any new purpose, type of personal data, type of data subject, or source of personal data would require the approval of a new registration application, and the Article could be interpreted to mean that every separate processing activity that an organization engages in would require its own separate registration application.

Moreover, the European Union departed from a similar requirement when it passed the General Data Protection Regulation (GDPR) in 2016, indicating a global trend away from registration requirements. The GDPR's predecessor, the Data Protection Directive, contained a similar requirement for data controllers to notify Data Protection Authorities prior to carrying out processing operations in a country.[7] The GDPR did away with this requirement and now simply requires controllers to maintain records of processing internally, which can be requested by DPAs in investigations, audits, etc.

That said, the goals of the registration process demonstrate an appropriate recognition of the importance of organizations adopting strong data protection practices and conducting impact—or risk assessments of their processing activities. Thus, rather than having to register their processing of sensitive data, an organization should document the types of sensitive data it is processing and the purposes for which it is processing that data, and should also conduct an impact assessment for all sensitive data it is processing. As such, coupled with the recommendation above for adopting a risk-based approach to defining sensitive data, CIPL recommends that the Draft Decree remove the requirement for ex ante approvals for processing sensitive personal data, and replace it with the following requirements: 1) organizations must document the information currently required in the application in Clause 2 of Art. 20, which can be made available to the PDPC upon request, and 2) organizations must conduct an impact assessment and create an impact assessment report, as required in Clause 2 of Art. 20, which can be made available to the PDPC upon request. This section

[7] European Union Directive 95/46/EC, Art. 16.

should also be clarified to require that additional documentation and impact assessments should only be required when there have been material changes to an organization's processing activities or circumstances that could change the assessments and conclusions reached in earlier impact assessments.

Such a provision would serve the same purpose as the Draft Decree's registration requirement, but would not run the same risk of slowing down the day-to-day processing activities of organizations operating in Vietnam.

Recommendation: Remove the registration requirement for sensitive personal data and replace it with requirements for organizations to document and conduct an impact assessment on their sensitive data processing activities that can be made available to the PDPC upon request.

IV. Rights of the Data Subject (Article 5)

CIPL welcomes the introduction of dedicated data subject rights in Vietnam intended to ensure a high level of data protection for all individuals. When well implemented, data subject rights empower individuals to have better control over their personal data while requiring entities collecting data to be transparent about and accountable for how they use personal data. We note that the Draft Decree introduces, in broad terms, the possibility for individuals to exercise their rights to "allow or disallow" the processing of their personal data, as well as to correct, access, delete and restrict such data. While these rights find inspiration in other data protection laws, it appears that the Draft Decree did not include the necessary requirements, limitations, and possible defenses to ensure that other important values are upheld despite the request of the individual. For instance, the right to object to the processing of personal data (right to "disallow") or to deletion may not be available where the processing is needed for compliance with the law. Similarly, the right of access may be unavailable where the requestor cannot verify his/her identity, where the individual already has access to the personal data that he/she seeks, or even where disclosing such data would adversely affect the rights and freedoms of others, or the proprietary rights of the organization.

As it stands, Art. 5 on data subject rights would be largely impractical and very difficult to implement, and is likely to give rise to disputes between individuals, organizations, and the PDPC. To that end, we refer to the Singapore PDPA and the EU GDPR as good reference points on how data subject rights can be introduced with the necessary requirements for and limitations to their exercise. This will ensure that organizations can duly implement data subject rights and individuals have sufficient clarity on when these rights are available.

Recommendation: Introduce the necessary safeguards for the proper exercise of data subject rights to ensure that other legitimate interests, including public interest and rights of third parties, are not unduly affected.

V. Consent and Other Bases for Processing

The Draft Decree requires consent for the processing (Art. 3) and disclosure (Art. 6) of personal data unless an exception (outlined in Art. 10) applies. These exceptions are: 1) as required by law; 2) in support of national security, social order and safety; 3) as required by law in emergency events that threaten life or seriously affect the health of the data subject or the public health; 4) in support of investigations and handling of regulatory violations; 5) in compliance with specific provisions that explicitly allow the processing of personal data without the data subject's consent under international

agreements or treaties to which Vietnam is a signatory; and 6) for research or statistics purposes in accordance with Art. 12 of the Draft Decree.

This consent-based approach is based on an individual control paradigm for privacy and data protection, which is widely viewed by data protection experts as an outdated model for legitimizing the processing of personal data, as it privileges consent over other available and effective bases for processing. A consent-based model places an unduly heavy and unrealistic burden on individuals to protect themselves and make a series of choices each time their data is collected or used. It also has the potential to preclude or undermine a wide range of legitimate, necessary, or beneficial processing activities if they are not covered by one of the existing exceptions. Indeed, the exceptions set forth in Art. 10 of the Draft Decree all relate to very specific data processing situations that constitute just a fraction of the vast number of processing operations that occur daily.

Given the complexities of the digital and data-driven economy, individuals cannot be expected to continuously engage with all entities that might be handling their data or to fully understand how their data will be used, by whom it will be used, and how these uses will benefit (or possibly harm) them and society, and what choices to make. Indeed, given the impossibility for individuals to fully understand the scope, purpose and implications of certain processing activities, individuals might withhold consent without good reason in situations where processing their personal data would present no risks at all, thereby impeding legitimate processing activities that could benefit them or society. Conversely, individuals might quickly consent to processing without due consideration of any potential harm to them. In such cases, consent will only serve to protect organizations from legal liability rather than reflect an informed decision by an individual.

While consent remains useful for processing personal data in some situations, there are countless circumstances in which obtaining consent is impractical, impossible, ineffective, or simply not meaningful. These include, for example, (1) where there is no direct interaction by the organization with individuals and obtaining consent would be unfeasible, (2) where the data use is common, trivial and imposes no real privacy risk, (3) where large and repeated volumes of data are processed (and seeking consent at every instance may not be feasible or may become meaningless as a result of consent fatigue, which is, perhaps, the most significant threat to the effectiveness of consent), or (4) where obtaining consent would be counterproductive or undermine compelling interests from businesses and society, such as where data is processed for network and information security or child online protection. It does not appear that any of these processing activities would be covered by the current exceptions to consent outlined in Art. 10.

Instead of relying on a consent-plus-exceptions model, CIPL recommends that the Draft Decree adopt the approach followed by other modern privacy laws, such as the EU's GDPR, Brazil's LGPD, and China's draft PIPL, and provide for a number of alternative or co-equal bases for processing from which organizations can choose the most appropriate option in a given context.[8] This list of alternative bases for processing should at least include consent, contractual necessity, compliance with a legal obligation, vital interest of an individual, public interest, and legitimate interest.

We would like to particularly highlight the importance of including in Vietnam's law a basis for processing that is similar to the "legitimate interest" legal basis found in the above and other privacy

[8] See Article 6(1)(a-f) of the GDPR, Article 7(I-X) LGPD, and Article 13 of China's draft PIPL.

laws.[9] The legitimate interest ground for processing is essential in the context of the modern digital economy. It enables organizations to collect and process personal data for purposes that are not covered by other grounds for processing while ensuring they remain accountable for the processing and fully respect the data protection rights and privacy interests of individuals. Typically, the legitimate interest ground for processing requires the organization to conduct a balancing test or risk/benefit assessment to demonstrate that it or a third party has a legitimate interest to process the personal data, and that these interests are not overridden by the rights of, or harms to, the individuals whose data is the subject of the processing. Moreover, this balancing test must be fully documented and demonstrable to privacy enforcement authorities on request.

When developing a data protection law, it is important to keep in mind the dual goal of protecting the privacy of individuals and enabling businesses and other organizations to responsibly process personal data where necessary and beneficial for a wide range of legitimate purposes. CIPL, therefore, recommends the inclusion of a legitimate interest processing ground that would promote both of these goals.

The legitimate interest ground will allow for important processing activities that are not currently covered by Art. 10's exceptions to consent such as processing for information, network, system and cybersecurity; fraud prevention and detection; processing personal data in employment contexts; corporate operations and due diligence; product development and enhancement; communications, marketing and business intelligence.[10]

Indeed, in the growing data economy, the legitimate interest ground for processing will become increasingly important to enable a broad range of data processing activities not covered by other grounds, or that are currently unanticipated, but essential for a well-functioning digital economy and for organizations' ability to innovate and thrive. For example, at a fundamental level, fraud prevention in the context of payments can only work if financial data is processed. A personal data processor needs the account number and past transaction history to determine whether a transaction is fraudulent or not. Given the fundamental need for some organizations to perform fraud prevention and detection processes that are critical to the proper functioning of financial and payment systems, it would not be appropriate to require that personal data processors seek consent from data subjects for the processing of financial data that is necessary to, and forms the basis of, fraud prevention and network, and information security.

Processing of data for fraud prevention purposes would be beneficial not only to Vietnamese consumers, but also to the Vietnamese government. Lower fraud incidence means that fewer resources are expended by merchants, banks and governments for investigating and prosecuting fraudulent transactions. Lower fraud incidence would also allow Vietnamese consumers to trust the use of digital payments, which will support Vietnam's digital economy.

Moreover, it is important to note that due to the required risk/benefit assessments inherent in the "legitimate interest" basis for processing, which must be demonstrable to enforcement authorities,

---

[9] See Article 6(1)(f) GDPR and Article 7(IX) of the Brazil LGPD; Note that Singapore has recently updated its Personal Data Protection Act to include a legitimate interest ground for processing, see https://www.jonesday.com/en/insights/2021/02/singapores-personal-data-protection-regime-enhanced.

[10] See CIPL White Paper on Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR, 19 May 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf.

and the associated requirement to implement risk-appropriate mitigations and controls, the legitimate interest basis for processing provides a high standard of personal data protection for individuals. It thereby places the burden of protecting individuals' data on the organizations that use the data rather than on individuals themselves via consent.

Additionally, Art. 8 of the Draft Decree requires that "data subjects' consent must be in a format that can be printed or copied in writing." To apply the "printed or copied in writing" requirement across all sectors and industry broadly will only create an administrative burden without adding to the validity of the consent itself. It would be advisable for the Draft Decree to hold data processors accountable for obtaining valid consent and presenting information to the user to make an informed decision, rather than rely on printing and copies as proof of such. Designing digital systems and processes to manage user consent will eliminate the need for unnecessary paper and copies that can be lost, stolen or inadvertent disclosures of user consents. This is part of the digital economy capabilities and responsible community practices that Vietnam should encourage by way of its laws and regulations.

Recommendation: The Draft Decree should avoid its current over reliance on consent and the associated limitations and problems (including consent fatigue) and should embrace a basis for processing model that includes all standard bases for processing found in other major data protection laws, including a legitimate interest basis for processing.

Recommendation: Remove language requiring that consent must be in a format that can be printed or copied in writing, as it is not clear how this requirement would be applied to a digital environment.

VI. Automated processing of personal data (Article 13)

Under the Draft Decree, "automated processing of personal data may only be done during the process of contract executing or performance," as long as the data subjects are notified and provide consent to the processing. CIPL believes that the definition of "automated processing of personal data" should be revised, as the current definition could be read as applying to a broad swath of automated decisions. This is a significantly broader definition than is articulated by international frameworks of data protection, including the GDPR.

CIPL believes that Art. 13 places limits on the use of automated processing that are far too strict and would hinder beneficial uses of the technology. Automated processing is used to make decisions to ensure fraud prevention and network security, to facilitate facial recognition for security in airports, and for verifying eligibility for loans and insurance. None of those uses would be permitted under the Draft Decree's standard of ensuring that automated decision-making takes places for purposes of executing a contract. For example, it is unlikely that there will be any contractual arrangement in place between individuals and airports to use facial recognition for border control purposes. It also is sometimes not feasible or realistic to inform data subjects about the use of automated processing, such as in the case of fraud monitoring.

CIPL proposes that organizations should be able to engage in automated processing generally, including outside the process of executing or performing a contract, but should provide avenues for redress when an individual does not agree with an automated decision that impacts them. Organizations should also conduct risk assessments on automated processing activities that may result in legal or other similarly significant impacts. Similarly, any consent requirement for automated decision-making should be reserved for the most impactful and high-risk automated decisions, and where the automated decision is not necessary for the performance of a contract or otherwise authorized by law. Otherwise, common and vital automated decision-making may not be able to take place in Vietnam.

Without these changes, Art. 13 has the potential to significantly reduce the ability for Vietnamese companies to us AI effectively and in a way that their global counterparts are using it.

Recommendation: Expand the scope of Art. 13 to enable automated decision-making for purposes beyond the performance or execution of a contract (e.g., fraud prevention, network and information security, national security such as in the context of airport travel, to grant loans, etc.). CIPL recommends that the MPS does not define a static list of permissible scenarios but rather allows organizations to make such decisions based on appropriate risk assessments and mitigations.

Recommendation: Reserve the requirement to consent to automate decision-making for the most impactful and high-risk automated decisions. Guidance as to what constitutes such decisions could be provided by the PDPC and rebuttable by the organization based on relevant assessments of risk.

VII. Processing of children's data (Article 14)

Under the Draft Decree, in order to process children's personal data, a personal data processor must verify a child's age and obtain consent from a parent or guardian.

We welcome the Draft Decree's additional privacy safeguards for children, who merit specific protection when it comes to the processing of their personal data, as they may be less aware of the risks. However, we note that in most countries, persons under 18 are allowed to provide their consent to the processing of their personal data after they reach a minimum age, consistent with their increasing autonomy and development. Thus, we recommend the Draft Decree introduces an age of consent, after which adolescents can exercise their choices in respect to the processing of their personal data. We suggest the age of consent be set at 13, consistent with various international laws on the matter.

Consistent with the recommendations in Section III, Consent and Other Bases for Processing, we encourage the MPS to clarify that parental consent applies only where the processing is based on consent and where the child has not yet reached the age of consent. This is particularly relevant in the presence of other legal bases for processing, as suggested earlier. Otherwise, there could be a misconception that parental consent is the only basis for processing children's data, even where other legal authorities may be equally or more appropriate to ensure privacy protections.

Further, this requirement for parental consent appears to be triggered regardless of whether the personal data processor knows or should know that the personal data it is seeking to process is that of a child. While it is relatively straightforward to determine whether a personal data processor is processing a child's personal data when it comes to online products and services that are directed to children, the situation becomes more complicated for mixed audience websites (i.e., when a website is not directed to children, but children nonetheless use the service). Verifying the ages of all users who visit mixed audience websites to determine who is or is not a child under the age of consent in order to determine whether it is necessary to obtain parental consent would create a massive burden on organizations and their customers. In addition, it would require the collection of additional personal data, such as identity documents, which would be contrary to the Draft Decree's purpose limitation and data minimization principles. Moreover, age-gating mechanisms that require users to self-report ages are of dubious value, as children can lie to bypass these restrictions.

CIPL recommends that the MPS revise Art. 14 to enable personal data processors to conduct a contextual determination as to whether they are likely processing the personal data of children through an appropriate risk-based test. This test could include the consideration of the following factors to determine whether it is likely that users are children: the nature of the online service or

product offered, the accessibility of the service, the potential attractiveness of the service to children, and whether children have been attracted to similar or competing services. The requirements of Art. 14 would thus only apply if the assessment determines that a processor is likely to process the personal data of children.[11]

Such an approach is consistent with the requirement of obtaining consent where a personal data processor should know that it is handling the personal data of a child. Moreover, this approach will ensure that personal data processors obtain consent from the parents or guardians of children under the age of consent without necessitating the verification of all users' ages and the collection of further information to facilitate such verification.

Recommendation: Introduce an age of consent for processing of personal data in Vietnam and clarify that parental consent applies only where the processing is based on consent and the child has not yet reached the age of consent, which we recommend should be 13.

Recommendation: Enable personal data processors to make a contextual determination based on a number of factors to determine whether they are processing the personal data of children in order to meet the requirements of Art. 14 for mixed audience websites and services.

VIII. Cross-border transfer of personal data (Article 21)

A. Conditions for transfer of personal data out of Vietnam

CIPL appreciates the Draft Decree's recognition that personal data may need to be transferred outside of Vietnam. Art. 21 of the Draft Decree permits the transfer of personal data of Vietnamese citizens out of Vietnam when all of the following conditions are met: 1) data subject's consent is granted for the transfer; 2) original data is stored in Vietnam; 3) a document is granted proving that the recipient country or territory has issued regulations on personal data protection at a level equal to or higher than that specified in the Draft Decree; and 4) a written approval is obtained from the PDPC.

While the data protection goals behind these requirements are legitimate, requiring all four conditions to be met for all transfers of personal data is impractical, poses an overly onerous burden on organizations, will significantly hinder and possibly halt the transfer of personal data out of Vietnam, and, as a result, will impede Vietnam's ability to participate and flourish in the global digital economy. Further, several of the specific conditions present a variety of concerns and thus should not be used as the sole means of transfer without offering alternatives. Instead, the Draft Decree should provide a more feasible approach to data transfers that would still ensure that personal data can flow outside Vietnam with all of the protections afforded by the Draft Decree.

Additionally, the exceptions to the data transfer conditions, which are outlined in Clause 3 of this Article and which seemingly are intended to be in the alternative rather than cumulative, appear to overlap with the conditions in Clause 1 of this Article. This is confusing and should be clarified. For

[11] This approach has been embraced in Sec. 312.2 in the United States' Children Online Privacy Protection Act, which states that "In determining whether a Web site or online service, or a portion thereof, is directed to children, the United States' Federal Trade Commission will consider its subject matter, visual content, use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics of the Web site or online service, as well as whether advertising promoting or appearing on the Web site or online service is directed to children. The Commission will also consider competent and reliable empirical evidence regarding audience composition, and evidence regarding the intended audience."

example, if consent or a written approval from the PDPC alone are sufficient to transfer personal data out of Vietnam, as it would appear to be per the language of Clause 3 of Art. 21, then it is not clear when, if ever, an organization would have to meet all four of the conditions in Clause 1 (which include consent).

Recommendation: Clarify the exceptions to the data transfer conditions to ensure that they do not overlap with the conditions themselves.

B. Consent Requirement for Data Transfers

CIPL would like to highlight that the requirement to obtain a data subject's consent for data transfers alongside the other requirements outlined in Art. 21 is an outlier among data protection laws globally and will seriously affect the ability of organizations to transfer data abroad for legitimate and beneficial purposes.

The key concerns with requiring consent in addition to the other requirements are:

- Consent does not provide additional protection to individuals; it merely provides cover from liability for organizations that have obtained an individual's consent.

- Requiring consent for every transfer sends a confusing and inappropriate message about transfers to individuals. Asking for consent for all cross-border transfers could mislead people to think there is something inherently wrong or risky with such transfers. In the modern digital economy, cross-border transfers are essential to the provision of a wide range of products and services for consumers.

- Requiring consent imposes an unnecessary burden on individuals. Asking individuals to consent to every transfer of data would dramatically increase the number of consent requests they receive, thereby overburdening them and having the effect of diluting and undermining the effectiveness of consent in situations where it might be meaningful.

- Requiring consent imposes an unnecessary burden on organizations. In preparing for compliance with the Draft Decree, organizations would have to implement the mechanisms and procedures associated with obtaining consent for transfers of personal data. This could cause substantial costs to new and existing businesses, and disruption to organizations that already have established mechanisms in place for the transfer of personal data across borders in line with common approaches found in many global data protection laws.

- Obtaining consent for every transfer of personal data is not always feasible. In some cases, it may be impossible to obtain consent for a transfer of personal data due to an organization's lack of relationship with, and/or contact information of, an individual whose personal data is being transferred.

- Consent can be withdrawn by the data subject at any time, effectively placing data transfers under permanent legal uncertainty.

In addition to the concerns raised above, it is important to highlight that, internationally, countries have steered away from requiring consent for the cross-border transfer of personal data. For example, the GDPR allows the use of explicit consent as a basis for transfer only in limited cases such as when a transfer cannot be made pursuant to a range of other appropriate safeguards like binding corporate rules, transfer codes of conduct or certifications, or standard contractual clauses, and the individual has been informed of the possible risks of the transfer. The GDPR also allows the use of consent as the

basis for transfer where a transfer cannot be made pursuant to an official determination that the other country provides essentially equivalent protections (i.e., where there is no finding of "adequacy"). Thus, under the GDPR, the use of consent is a derogation from the general rules on overseas transfers. Moreover, in Canada, the Office of the Privacy Commissioner of Canada (OPC) conducted a public consultation in 2019 on changing its policy position for transfers to require consent for transborder data flows. At the conclusion of the consultation, in which stakeholders made all of the above points, the OPC decided that consent for transfers is not required, and that the existing approach, based on accountability safeguards that ensure all domestic protections flow with the data, remains appropriate.[12]

Moreover, Vietnam is part of APEC. One of the core objectives of APEC's Privacy Framework and Cross Border Privacy Rules (CBPR) system, which Vietnam endorsed in 2011, is to ensure the free flow of data in the Asia-Pacific region and to promote "effective privacy protections that avoid barriers to information flows."[13] The role of the CBPR is to further both privacy and maintaining information flows among APEC economies and with their trading partners, as well as to encourage organizational accountability with respect to personal data.[14] Indeed, one of the foundational premises of the Framework was to create "conditions, in which information can flow safely and accountably, for instance through the use of the CBPR system." According to the Framework, the CBPR system was created so that "individuals may trust that the privacy of their personal information is protected" no matter where it flows.[15] An APEC Privacy Framework[16] section specifically on cross-border transfers provides as follows:

- *70. Any restrictions to cross border flows of personal information should be proportionate to the risks presented by the transfer, taking into account the sensitivity of the information, and the purpose and context of the cross border transfer.*

Further, it is noteworthy (but not surprising) that the program requirements of the APEC CBPR do not provide for choice or individual consent with respect to cross-border data transfers. Such an option would be inconsistent with APEC's and the CBPR's premise of providing accountability-based protections to the information regardless of geographic location.[17]

---

[12] See CIPL Comments on the Office of the Privacy Commissioner of Canada's Consultation on Transborder Dataflows, 17 May 2019, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_the_office_of_the_privacy_commissioner_of_canadas_consultation_on_transborder_data_flows.pdf; and CIPL Comments on the Office on the Privacy Commissioner of Canada's Reframed Consultation on Transfers for Processing, 5 August 2019, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_response_to_the_opcs_reframed_consultation_on_transfers_for_processing.pdf.

[13] See, for example, APEC Privacy Framework at Foreword and Preamble, paragraph 4, available at https://www.apec.org/-/media/APEC/Publications/2017/8/APEC-Privacy-Framework-(2015)/217_ECSG_2015-APEC-Privacy-Framework.pdf.

[14] *Id.* at Preamble, section 8.

[15] *Id.* at Part IV, B, III, paragraphs 65 and 67.

[16] *Id.* at Part IV, B, IV, paragraphs 69 and 70.

[17] There is one limited exception to this. The Framework's accountability principle (Part III, principle IX, para. 32 plus Commentary) provides that where personal information in a domestic or international transfer cannot be protected through exercise of due diligence or other reasonable steps, an organization should obtain consent "to assure that the information is being protected consistent with these principles." However, this would not be the context under the CBPR or any mechanism whereby the transfer of personal data occurs subject to appropriate accountability measures that ensure continued protection at the appropriate level.

Vietnam's proposal to introduce a consent requirement, therefore, is inconsistent with the goals of the APEC Privacy Framework and the specific purpose and requirements of the CBPR: to make geographic location of personal data irrelevant because protections should flow with the information regardless of where it goes. The CBPR system is a mechanism specifically designed to ensure that privacy protections flow with the data, including across borders.

While the APEC Privacy Framework and the CBPR explicitly do not prohibit domestic privacy protections that go above and beyond what is provided by APEC or the CBPR, implementing a new requirement that is at odds with the very premise of the APEC Privacy Framework and the CBPR warrants careful consideration. Part of the promise of the CBPR, which Vietnam someday might join (as evidenced by Vietnam's Ministry of Industry and Trade's previous efforts to prepare for Vietnam's potential CBPR participation), is to harmonize privacy and data protection practices across the APEC region (and maybe even beyond). This harmonization across the APEC region will be one of the principal benefits and incentives for organizations that certify to the CBPR. Any unnecessary national deviation, therefore, has the potential to directly undermine this harmonization benefit and, thus, the relevance and effectiveness of the CBPR in the long run as well as Vietnam's ability to participate in the CBPR.

Recommendation: Revise Art. 21 to remove the requirement to obtain consent on top of the other requirements to transfer personal data overseas.

Recommendation: Enable Vietnam's participation in the APEC CBPR and PRP[18] systems.

C. Storing Original Data in Vietnam

CIPL understands that countries may determine that certain forms of information are required to be stored locally within a country for public interest and national security purposes. In particular, we note that the definition of "original data" as "the first copy of personal data processed by the personal data processor, not yet transferred to a third party" will cause data to stop at the Vietnamese digital border due to uncertainty as to what this means. The legal concept of what constitutes "original," who determines this, and what it is intended to achieve in data protection terms is also inconsistent with international frameworks and global norms. Creating a new category of data that is vague, open to interpretation and excessively restrictive of the opportunities for transferring data outside of Vietnam may lead to the unintended disruption of legitimate data flows that prevent companies from offering products and services in-country and from expanding their service coverage regionally or globally.

Further, CIPL cautions against any form of data localization in a privacy law. Given the global nature of the digital economy, CIPL believes that countries should enable the free flow of personal data while ensuring the protection of such information through organizational accountability and sensible data transfer mechanisms. Requirements to store personal data locally can have the following consequences:

[18] The APEC Privacy Recognition for Processors (PRP) are a companion certification to the CBPR specifically designed for "data processors" that process data for "data controllers." (In many global data protection laws, "controllers" determine the purpose and means of processing and "processors" are entities that process data on behalf of and at the direction of "controllers.") The Draft Decree does not employ the same terminology for these categories of entities but establishes the category of "Personal Data Processors" (which may include both data controllers and data processors—it is not clear) and "Third-parties" that also engage in "some processing activities." CIPL recommends clarifying these terms in the final law and, if possible, consider greater alignment with global norms around these concepts.

- They significantly impede the use of technologies that rely on global and distributed networks, such as data analytics, cloud computing and AI, and machine learning applications, reducing the local offer of services and products.

- They impose the creation of redundant storage systems. International organizations operating in Vietnam would be required to create redundant storage systems in Vietnam to store data which would raise costs, disrupt business processes and create information security risks.

- They increase costs to prohibitive levels for local and foreign small and medium enterprises. New market entrants may be unable to take advantage of competitive cloud computing services that allow them to enter the market and compete with larger organizations. Foreign enterprises may not have the capital to set up redundant storage systems in Vietnam, which effectively blocks them out of the market and prevents their ability to serve Vietnamese consumers.

- They compromise data security. Requiring the concentration of personal data in Vietnam prevents organizations from partitioning data across global servers, which can provide an additional layer of protection against hackers and business continuity in the case of natural disasters.

Given the above consequences, CIPL recommends that the requirement to store original data in Vietnam be removed.

Recommendation: Remove the requirement to store original data in Vietnam.

D. Written Approval from the Personal Data Protection Commission

Similar to our concerns expressed above regarding the registration requirement for the processing of sensitive personal data, CIPL is concerned that the requirement to obtain a written approval from the PDPC prior to transferring personal data out of Vietnam would result in a considerable burden for organizations, overwhelm the PDPC with thousands of requests for such written approval, and could significantly slow or halt the transfer of data out of Vietnam.

Per the registration requirements in Clause 7 of this Article, the specificity of the information that must be included in the application for approval appears to indicate that a separate application would be required for each different transfer purpose, each location where personal data is registered, and each set of conditions relied upon to transfer the data. However, this Clause is unclear and could be read to mean that every single transfer of an individual's personal data would require its own separate application and approval. Even if that was not the intent of this provision, the registration requirement would result in the use of significant resources by organizations for each application they must submit, and, given the volume of applications that the PDPC is likely to receive, lengthy delays for approval far beyond 20 days.

As such, CIPL recommends that Draft Decree remove the requirement for ex ante approvals for data transfers completely, and replace it with the following requirements for data transfers: 1) organizations must document the information currently required in the application in Clause 7 of Art. 21, which can be made available to the PDPC upon request, and 2) organizations must conduct an impact assessment and create an impact assessment report, as required in Clause 7 of Art. 21, which can be made available to the PDPC upon request.

Recommendation: Remove the ex ante registration requirement for cross-border data transfers from the Draft Decree and replace it with documentation and risk assessment requirements that can be requested in the case of an investigation or audit.

E. Solutions for improving the current transfer framework in Art. 21

Instead of allowing transfers only when the conditions listed in Art. 21 are fulfilled, the Draft Decree should also include a comprehensive set of available and widely-accepted cross-border transfer mechanisms to enable accountable global data flows. This approach is necessary to ensure global consistency and convergence, and to build on existing and accepted business and regulatory practices to enable benefits from cross-border data flows while ensuring protection from harms and risks to individuals.[19] It is particularly important for multinational organizations that operate in many countries to be able to leverage the same transfer mechanisms globally, as well as for Vietnamese companies to effectively operate in the global market.

As such, Vietnam should consider including all of the following mechanisms in the Draft Decree:

- ***Contracts:*** The law should allow cross-border transfers on the basis of contractual arrangements, such as the Association of Southeast Asian Nations (ASEAN) Model Contract Clauses (MCCs), that stipulate appropriate data privacy and security controls to be implemented by the organizations, thus establishing sufficient levels of protection for data leaving the jurisdiction.

- ***Corporate Rules:*** The law should allow cross-border transfers based on binding corporate rules (similar to the EU GDPR's binding corporate rules or "BCR") that provide for uniform and high-level protection and privacy compliance by all local entities of a multinational group.

- ***Cross-Border Rules:*** The law should allow for the use of enforceable corporate cross-border privacy rules such as the APEC CBPR and the APEC PRP.[20]

- ***Codes of Conduct, Certifications, Privacy Marks, Seals and Standards***: The law should allow for the use of approved codes of conduct, certifications, privacy marks, and seals and standards as cross-border transfer mechanisms. (Note that the CBPR and PRP are privacy certifications for transfer purposes.)

- ***Bilateral Arrangements:*** The law should allow the possibility of cross-border transfers based on negotiated arrangements with other countries, such as arrangements that rely on certification or "self-certification" to a given privacy standard, coupled with enforcement. (The EU-U.S Privacy Shield is an example of this.)

---

[19] For more information on this topic, see CIPL White Paper on Essential Legislative Approaches for Enabling Cross-Border Data Transfers in a Global Economy, 25 September, 2017, available at https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper__final__-_essential_legislative_approaches_for_enabling_cross-border_data_transfers.pdf.

[20] Note that any differences between the CBPR (and PRP) privacy standards and the standard ultimately adopted by Vietnam through this proposed law should not be an impediment to enabling use of the CBPR as a valid transfer mechanism. The CBPR system explicitly envisions the possibility that domestic privacy requirements may differ or exceed the CBPR on some points and requires certified organizations to also comply with any additional domestic requirements. Thus, CBPR-certified entities in Vietnam would still have to comply with Vietnamese requirements not found in the CBPR, including when transferring data outside of Vietnam.

- ***Adequacy and Whitelists:*** The law should allow for adequacy rulings and "whitelists."

- Other grounds for transfer or derogations or exceptions to transfer restrictions, including necessity for the performance of a contract, public interest, establishment or defense of legal claims, vital interests, public register information, and compelling legitimate interest.

Moreover, CIPL recommends that the Draft Decree provide an exception for intra-company transfers, including the transfer of employee data, outside of Vietnam for global companies. Such transfers are necessary for day-to-day operations and would promote increased investment in Vietnam, as organizations would not have to create separate business entities to engage in the Vietnamese market.

Additionally, it is worth noting that Vietnam is one of ten member states of the ASEAN, which in January 2021 approved a new Data Management Framework (DMF) and MCCs for Cross Border Data Flows. The ASEAN MCCs were developed to harmonize the standards for cross-border data flows across the region.[21] Given Vietnam's participation in ASEAN, it would make sense if Vietnam's privacy law reflected both the ASEAN DMF and MCCs. Thus, the MCCs should be adopted as one of the mechanisms to allow organizations to transfer personal data out of Vietnam.

Recommendation: Include a comprehensive set of available cross-border transfer mechanisms to enable accountable global data flows.

Recommendation: Provide an exemption for intra-company transfers, including the transfer of employee related data, outside of Vietnam by global companies.

IX. Data Breach Notification (Article 28)

Art. 28 of the Draft Decree requires organizations to "promptly notify the Personal Data Protection Commission of breaches to personal data protection," though it makes no reference to the likelihood or severity of the harm. CIPL recommends a risk-based approach to determine when organizations must notify the PDPC in the event of a breach.

For example, Canada's Personal Information Protection and Electronics Document Act (PIPEDA) and Singapore's PDPA contain risk-based approaches to data breach notification, and the MPS should follow their lead and require notification only when a breach is likely to result in significant harm to a data subject. To determine whether this threshold is met, organizations should consider the sensitivity of the personal data involved, the probability that the data will be misused, as well as the confidentiality and volume of the data that has been reached. Without such a threshold, the existing requirement has the potential to be unduly burdensome to organizations and could overwhelm the PDPC with the volume of notifications.

Additionally, the term "promptly" should be clarified to mean as soon as is reasonable under the circumstances. Within the first few days after a breach, organizations may not have sufficient information to know the nature or full scope of the breach. Further, in the crucial hours and days after a breach, organizations' resources should be focused on investigating the breach and not preparing notifications to regulators, and it is likely organizations will have very little information to provide to

[21] For more information, see the press release from Singapore's Personal Data Protection Commission, available at https://www.pdpc.gov.sg/help-and-resources/2021/01/asean-data-management-framework-and-model-contractual-clauses-on-cross-border-data-flows.

a regulator so early in the investigation. As such, organizations should be given sufficient time to understand the nature and scope of the beach prior to notification.[22]

Recommendation: Notifying the PDPC of data breaches should only be required when the breach is likely to result in significant harm to a data subject.

Recommendation: Ensure that the term "promptly" as it relates to data breach notification is interpreted to mean as soon as is reasonable under the circumstances.

X. Timeframe for Adoption (Article 29)

The Draft Decree currently states in Art. 29 that it shall take effect on December 1, 2021. Given that this review process is still in its early stages, and that many changes may be made to the Draft Decree, this timeframe should be significantly extended to provide organizations with sufficient time after the law has been finalized to come into compliance with the new law. To comply, companies will need to become familiar with the provisions of the law, understand how it may be interpreted by regulators and practically applied, and take appropriate measures internally. This is particularly important where no previous comprehensive privacy law has existed.

A reasonable timeframe would instead be at least two years. The EU's GDPR provided for two full years for implementation from its completion, and Brazil's LGPD included an implementation timeframe of two years as well. Without an appropriate implementation timeframe, organizations simply will not be able to come into compliance with the law in time.

Recommendation: Extend the date of effectiveness in Art. 29 in the Draft Decree to at least two years from when it is passed into law to ensure that organizations will have sufficient time to become fully compliant.

XI. Conclusion

CIPL is grateful for the opportunity to provide input to the Ministry of Public Security of Vietnam on the Draft Decree on Personal Data Protection. We look forward to future opportunities to comment on and provide input into this process.

If you would like to discuss any of the comments in this paper or require additional information, please contact Markus Heyder, mheyder@HuntonAK.com, Sam Grogan, sgrogan@HuntonAK.com or Matthew Starr, mstarr@HuntonAK.com.

[22] For a full discussion of aligning global data breach notification standards, see the United States Chamber of Commerce and Hunton Andrews Kurth report on Seeking Solutions: Aligning Data Breach Notification Rules Across Borders, 3 April 2019, available at https://www.huntonak.com/en/insights/seeking-solutions-aligning-data-breach-notification-rules-across-borders.html.