US-ABC's RECOMMENDATIONS –

VIETNAM'S PROPOSAL TO AMEND DECREE 72/2013/ND-CP

The US-ASEAN Business Council ("US-ABC"), the American Chamber of Commerce in Vietnam ("AmCham Vietnam"), and our member companies would like to thank the Ministry of Information and Communications ("MIC") for the opportunity to comment on the draft proposal to amend Decree 72/2013/ND-CP on the management, supply and use of Internet services and online information ("Decree 72"). As the COVID-19 pandemic has accelerated the pace of digitalization, we applaud the Vietnam Government's efforts to develop a more inclusive digital economy that can help businesses grow while protecting consumers' interest.

We believe that Vietnam is well-placed to grow and benefit from the digital economy. A sound legal framework that adapts to the realities of an increasingly digital and data driven economy will allow for Vietnam to reap its benefits. It is widely agreed that countries need globally aligned regulations to safely promote growth and innovation. The Council and our members are invested in continuing to ensure safety on the internet by preventing and taking down illegal content. We have also scaled up efforts during the COVID-19 pandemic to combat misinformation that contradicts guidance from health authorities in Vietnam. We understand the challenges that the Government of Vietnam is attempting to address in revising the decree and are therefore committed to work together to derive purpose-fit approaches in step with global best practices.

We would like to express concerns that the proposal to amend Decree 72 in its current version would stifle the rapid pace of Vietnam's digital progression, thereby contradicting the country's vision to achieve digital transformation by 2030 (e.g., under Decision 749/QD-TTg). The draft proposal includes new concepts and requirements which are concerning in terms of feasibility, enforcement, and consistency with other laws and regulations. It introduces significant disruption to existing business processes and limits the ability of Vietnamese businesses and multinationals operating in Vietnam to service domestic and international customers. We would therefore recommend for the Draft Decree to be revised to address these requirements.

In addition, the current version of the draft proposal introduces many overlaps or conflicts with other existing laws and regulations, such as the Law on Cybersecurity ("LOCS") and its draft guiding decree, which contain provisions on content restrictions and takedown requests from relevant authorities (mainly MPS and MIC); the Law on Intellectual Property 2005 (amended 2009) and its guiding Decree 128/2018/ND-CP regarding content in the press that violate the Intellectual Property law; the draft decree on Personal Data Protection which contains provisions on data privacy protection; and Circular No. 38/2016/TT-BTTTT regulating the provision of cross-border public information. We recommend that any proposed amendments to Decree 72 should aim towards a consistent and effective approach which aligns with the existing laws and regulations in Vietnam.

On this note, we would like to emphasize the following key issues and concerns in the publicly circulated draft:

1. **Data localization and local representative office**
   The draft proposes to effectively ban data centers from transferring any customer data across borders (Article 22.3(d) and Article 44.h.5), including where the customer has requested the transfer. The proposed restrictions on the ability for customers to transfer data overseas does not take into account the technical and practical realities of the digital economy which relies on cross border data flows (including customer data). Consequently, it introduces significant disruption to existing business processes, thereby limiting the ability of Vietnamese businesses and multinationals operating in Vietnam to service domestic and international customers, while also undermining privacy and security. To better facilitate the needs of businesses using online and cloud services, we recommend that MIC removes the ban on data centers from transferring customer data across borders and the requirement for businesses to seek approvals before the transfer of customer data outside of Vietnam.

   Requiring a local presence could produce the unintended negative consequences of placing Vietnam at a competitive disadvantage as compared to other countries since establishing a local presence would significantly increase the cost of doing business in Vietnam. This competitive disadvantage could deter foreign investors and/or cause existing multinational companies in Vietnam to look for alternatives.

2. **Inclusion of data centers operation and cloud services in the scope**
   It is not clear what the main objectives of MIC are under this draft amendment and what regulatory requirements MIC intends to place on data centers, cloud services and other stakeholders, such as (B2B) cloud service providers, by expanding the scope of Decree 72. This ambiguity will create significant commercial uncertainty, and result in data centers and cloud service providers re-thinking their commercial investments in Vietnam.

   Establishment of such a regulatory regime for data center services would hinder the growth and undermine the development of cloud services in Vietnam by (1) creating barriers to entry, (2) introducing a new compliance burden that differs from, and is possibly counter to, regional and global practices, (3) reducing market competition, and (4) deterring both foreign investments and cross-border engagements. Furthermore, B2B cloud service providers may not always be in a position to be able to comply with requirements that are in the control of the 3rd party hosting provider or the end-customer and that the service provider has no legal, practical, or technical control over. Taken together, this would substantially impact the services and innovation that could otherwise be available to the citizens, businesses, and government of Vietnam. We therefore recommend that Decree 72 amendments should continue to exclude data center operations and cloud services from its scope as Decree 72 is intended to address consumer protection and content regulation issues related to business-to-customer (B2C) business models, rather than B2B.

3. **Turnaround Time**

The new timeframe for removing illegal content is not feasible to comply with due to high volumes and/or complexity of requests, and does not reflect the practical challenges of content moderation. Companies have put in place robust guidelines/community standards, removal policies and procedures that apply globally. We recommend considering more workable solutions that align with international best practices.

Furthermore, companies that provide B2B (cloud) services may not always be legally and/or technically permitted and able to remove content managed by their end customers. We recommend clarifying that B2B cloud providers are not subject to this requirement, but instead, the end customer that controls the data is required to remove illegal content.

4. **Extraterritorial jurisdiction**

It would not be practicable for Vietnam to extend its powers extra-territorially as enforceability against offshore organizations are often challenging. In addition to enforceability challenges, extraterritorial laws could create conflicting and overlapping regulatory obligations that could make compliance both overly complicated and costly for these offshore organizations and ultimately detract from the objective of these regulations. They could also be in contravention of existing trade agreements. In line with global laws on privacy or electronic transactions, we propose that the provisions under Articles 22.7, 44d and 44g should apply only to entities formed or established under the laws of Vietnam. Foreign organizations providing digital information on their international platforms targeting an international audience (not specifically targeting visitors from Vietnam) should be exempt from Decree 72.

5. **Livestreaming and revenue generating services requirement**

The new responsibilities in Article 22.3(g) and Article 23.7(g) impose an undue and impractical burden on foreign service providers to be liable for users' regulatory compliance. We believe that it is the responsibility of the content creator such as account/page/channel owners to comply with local regulations while the offshore providers are incorporated and operating overseas pursuant to foreign jurisdiction. If these accounts violate local laws, we rely on local competent authorities to alert us of these violations pursuant to the local regulations. In fact, many providers have established notice-and-takedown mechanisms that rights holders can use to report accounts that violate their rights. The requirements are also operationally impossible to implement; online service providers cannot police whether each account owner, user, channel or fanpage has exceeded 10,000 followers, whether each generates revenue on the platform, or whether each has fulfilled the MIC notification requirement. Therefore, we recommended that the drafting authority remove restrictions on live-streaming and revenue generating services under Articles 22.3(g) and 23.7(g) of the Draft.

In addition, the Draft Decree should recognize in its definitions that there are many different types of social media services and a blanket regulation is neither necessary nor pragmatic. Social media services differ significantly in terms of target audience, type of content, and features. For example, many social media services that focus on particular interests (for example graphic design, gaming, books) do not have journalistic intent or features and should not be regulated in the same way. Some of these specialized social

media services may not even need to be regulated as they have operated for years without posing any regulatory risk or issues. Instead of the current proposal which uses the same broad strokes to regulate virtually all domestic and cross-border social media services, we recommend that MIC adopt a differentiated approach and exclude the aforementioned specialized social media services.

6. **Content cooperation**

Article 22.3(c) introduces a requirement on implementation of content cooperation agreements with Vietnamese press agencies. Regulators should not prescribe entry into – nor dictate the terms of – commercial agreements between private parties at arm's length. This would contravene the principle of freedom of contract under Article 3.2 of the Civil Code. In any event, the scope of this article is so unclear that it is impossible to determine how to comply; no explanation exists as to legislative purpose nor the intended requirements that this agreement would have to meet. If passed, the article should exclude intermediaries from its scope which do not play a direct role in the creation of content but only provide a platform through which information is disseminated. Therefore, it is recommended that the drafting authority remove Article 22.3(c) from the Draft.

7. **Licensing Requirements**

In addition, while Article 23.7(a) on licensing and management of social networks clearly provides that "the management of foreign social networks will be carried out in accordance with Article 22 of this Decree" and Article 22 does not include and licensing requirements, Article 23.2 does not specifically include foreign social networks as websites which are not subject to a license, creating confusion over whether in fact foreign social networks are subject to the licensing requirements.

We understand that the Government's intention is for foreign organizations to not be subject to the licensing requirements in Article 23.1. This is unclear in the current draft and should be clarified in the legislation for the avoidance of doubt.

8. **Online games: video games**

The new provisions are unduly onerous and impractical for companies to comply with and will have the impact of restricting the growth and development of the video games industry and competitively disadvantage local gaming businesses. It could also deter foreign investment, by requiring online gaming providers to be a Vietnamese enterprise which has had a business line in service in the provision of video games online as published on the National Business Registration Portal.

Further, by requiring online gaming providers to e.g.; submit lengthy documents for each and every G1 game license application with a reduced validity period of 5 years, monitor and censor content (Article 23.d), continuously manage the playing time of the players to restrict playing time for different ages, include a warning which reads "*Playing for over 180 minutes per day shall have an adverse effect on health"* on the game's forum and on the player's screen during the playing period, manage the player's account information and personal information, fulfill lengthy reporting obligations and administer the contents of the game's forum - to name but a few, it could make it legally, technically and financially

too burdensome for companies to continue investing in Vietnam's gaming industry - an industry, which is projected to reach a revenue of US$257m in 2021 by Statista.[1]

The game play time restrictions, personal account management, content moderation and reporting measures would fundamentally change and degrade the consumer's gaming experience altogether. Further, such provisions impose the same level of obligations on online gaming providers as they do on social networks and online information websites, even though they are fundamentally different businesses. Online gaming companies do not have the same risk profile or carry the same type of content as compared to other platforms which primarily serve to host, generate, post and facilitate the interaction and sharing by users, user generated content and/or news. More importantly, some of these provisions could be contradictory to, or in violation of existing laws which serve to safeguard the protection of consumers, such as data protection and consumer protection laws.

Given that the proposed amendments introduce a considerable number of new changes that would have significant operational impacts to existing Vietnamese and foreign organizations, compliance would require adjustments at a technical or organizational level. Small and medium enterprises (SMEs) in particular would not necessarily have the resources to pursue immediate changes. To the extent the amendments are passed with these considerable changes, we recommend a transition period of at least 24 months from the effective date built into the decree.

Lastly, we would also want to express appreciation that our comments have been taken into consideration on Articles 32d.3(b) and 33.1(dd). The current draft demonstrates an improvement from the current regulation and previous draft amendment where Articles 32d.3(b) and 33.1(dd) mentioned physical localization of payment system. The latest draft just mandates that companies work with legitimate payment service providers in Vietnam, aligned with what we earlier provided with regard to the benefit of removing the localization requirement.

A more detailed set of recommendations can be found in the annex section. We welcome the opportunity for further discussion on this round of drafting and subsequent iterations. Should you have any questions or require any clarification on the points raised, please do not hesitate to reach out to USABC Director for Digital Policy, Mario Masaya (mmasaya@usasean.org) or USABC Chief Country Representative and Deputy Regional Managing Director, Vu Tu Thanh (tvu@usasean.org), or AmCham Vietnam Executive Director Mary Tarnowka (mary.tarnowka@amchamvietnam.com).

[1] https://www.statista.com/outlook/dmo/digital-media/video-games/vietnam

US-ASEAN BUSINESS COUNCIL, INC.

Annex on
Vietnam's Proposed Amendments to Decree 72

No	Article	Comments/Concerns	Recommendation (on policy implementation/related regulation)
1	Article 3.29	Under the current version of Decree No. 72, only the cross-border provision of public information is regulated. Public information is defined as online information of an organization or individual that is publicly provided without identifications or addresses of recipients. However, the new Draft Decree widens this definition to capture any kind of information, including private information that is sent in private messages.	We recommend the Draft Decree narrow this provision to only cover public information. This would also prevent any confusion or overlaps with the draft Personal Data Protection Decree on areas relating to personal information.
2	Article 3.41	The development, ownership, maintenance and operation of data centers cannot be sufficiently governed by regulations concerning information technology and telecommunications laws (which currently form much of the backbone of Decree 72). It also requires holistic consideration of laws on matters such as cybersecurity (including data protection), network information security, electricity, and construction. The proposed Chapter VI is "incomplete", creates uncertainty, and is unimplementable.	We recommend that the regulations on data center services (including the proposed Chapter VI) should be deleted.
3	Article 3.42	"Cloud computing services" should not be captured within the scope of a "data center service". All cloud services are deployed through a data center. The cloud service provider – particularly within the definition proposed in the draft – may not be (and in	We recommend that "Cloud computing services" should be deleted from the definition of "data center service" at Article 3.42. As there is also no further

		most cases will not be) the organization that owns, maintains or operates the data center. It is neither feasible nor appropriate to impose the same set of standards among these service providers: • Whereas the draft prohibits data center service providers from transferring customer data outside of Vietnam, these types of transfers are an inherent part of a cloud computing service which is presently offered by both Vietnamese and foreign service providers alike. The Draft Decree fails to address how these service providers may continue operating in light of this prohibition. • The inclusion of "cloud computing services" within the definition of "data center services" is also inconsistent with how other laws have enabled engagement of cloud service providers. • For example, Circular 09/2020/TT-NHNN (which regulates information system security in banking operations) expressly envisages a possibility for cloud computing service providers to have data centers outside of Vietnam. The proposed restriction against cross-border customer data transfer (i.e., that customer data must remain in Vietnam) is contradictory to this arrangement. The wide definition of "cloud computing services" would include the delivery of services that fall under the category of CPC 841 - 845 and CPC 849 – i.e., computer and related services. These services have long been open to foreign investment, including cross-border supply from overseas to Vietnam. The inclusion of these services within the scope of the "data center service", together	regulation required for such services, the definition and reference to "cloud computing services" should also be deleted. Alternatively, we recommend that a list of examples for IaaS, PaaS, and SaaS should be provided.

		with the imposition of the obligations in the draft Article 44h, presents a danger of Vietnam violating its international commitments. For example: • The current prohibitions against transferring data outside of Vietnam will contravene Article 14.11 of the CPTPP. • It further leaves no option but for an investor to store that data in Vietnam – i.e., to use computing facilities in Vietnam as a condition for its business. This will contravene Article 14.13 of the CPTPP. • Article 7.6(b) of the ASEAN Agreement on Electronic Commerce provides a similar commitment. The Government's justification for including "cloud computing services" within the definition of a "data center services" is not apparent in the draft. To the extent network information security is a concern, the proposed measures are heavy-handed. Even for services provided in the banking sector, Circular 09/2020/TT-NHNN takes a light touch approach. In lieu of creating onerous, common obligations between those who own, maintain or operate data centers versus those provide "computer and related services", similar requirements in Article 34 of Circular 09/2020/TT-NHNN may be taken, in which it is sufficient for the service providers to (i) be an enterprise or organization; (ii) comply with Vietnamese law; and (iii) have an international certificate on information security (e.g., ISO/IEC 27001). The onus of ensuring that the services are sufficient for network security and safety purposes in its operations should fall on the party engaging the cloud service provider (e.g., similar to Circular 09/2020/TT-NHNN).	

		Foreign companies who have developed or are developing innovative products are disincentivized from making these available to the Vietnamese businesses. These businesses would be restricted from accessing technological advancements.	
4	Article 5	This new Draft Decree has increased prohibited acts in Article 5.1 by supplementing and specifying a number of prohibited acts which make the list of prohibited acts non-exhaustive: • Impersonate other organizations and individuals; spread and circulate fake news and/or false information that cause confusion among the people, damage to socio-economic activities, difficulties to the operation of State agencies or official duty performers, and/or violate the lawful rights and interests of other agencies, organizations and individuals; • Information affecting normal physical and mental development of children; • Information infringing upon the intellectual property rights of other organizations and/or individuals; • Stealing or obtaining personal information of citizens by illegal means; unauthorized sale or provision of citizens' personal information to others; and • Other prohibited acts as prescribed by law. The non-exhaustive prohibited acts list poses significant enforcement difficulties given that each legislative regulation has its own classification of what is determined as banned or violating. For example, there are lists of prohibited acts/violations under IP Law (Article 28 & 35), Law on Children (Article 6) and LOCS (Article 8). It is also noted that there are both similarities and discrepancies of prohibited acts between Decree 72 and LOCS,	We recommend that the Government review and make it an exhaustive list of prohibited acts included in a single legal document, for an accurate reference and more effective enforcement.

		which would be confusing to relevant stakeholders as both legislative documents regulate online contents and activities on cyberspace.	
5	Article 5.1(dd)	The introduction of a definition or category for "fake news" would not be necessary. Article 5.1(d) of Decree 72 already prohibits the dissemination of "false information" that offends the reputation of an organization or honor and dignity of an individual. While we recognize the need to address deliberately false or misleading information, the proposed "fake news" definition can be subjective and challenging to operationalize The adoption of such policies should be approached with caution, as there is always a danger that they will be perceived as being a censorship tool. This is, in large part, because the determination of whether information is true (or "fake") is highly subjective, and difficult to discern. The proposed definition of "fake news" is of particular concern because it covers all types of information – not only those that are ordinarily regarded as "news" (i.e., journalistic products under the Law on Press). It is prescriptive and presents challenges among affected parties on how the "truth" of the information could be ascertained. Its scope might potentially be viewed as a hindrance to one's freedom of expression – a right upheld under Article 19.2 of the International Covenant on Civil and Political Rights (ICCPR). It curtails the freedom of users to exchange information and knowledge, as any such exchange would inherently run the risk of being perceived as "fake news" within the current definition.	We recommend this provision on “fake news” be removed. Alternatively, we recommend against using the term “fake news” and instead referring to “misinformation” and “disinformation” as defined below: • Misinformation: Verifiably false or misleading content that may be shared unintentionally. • Disinformation: The attempt at or effort to distort or manipulate the information ecosystem through inauthentic actors and/or behaviors, with the intention of harming a person, group, organization or country. It is important to differentiate the approach to tackle disinformation, which focuses on inauthentic behaviors and actors engaged in campaigns to deceive and manipulate public discourse, from misinformation, which focuses on the accuracy and truthfulness of information. Otherwise, although determining the truth of "news" is inherently subjective,

		Furthermore, the criterion that information be presented by subjects "with the purpose of serving their own intentions" is vague. It may capture even genuine intentions of a subject, whose presentation of information is not necessarily harmful or intended to cause harm. It is further challenging to ascertain or substantiate one's "intention". In addition, to the extent the Government intends to regulate "fake news" in the interest of protecting national security or public order, the broad provisions of the Law on Cybersecurity had already been enacted for this purpose.	to the extent this is to be regulated, we would suggest amendments that reflect the appropriate scope of (i) covering news, (ii) covering information that can be verifiably false or misleading and (iii) covering such information that is created with intention to deceive:
6	Article 5.1(e)	The criteria at Article 5.1(e) is undefined, and no reference to such information is made in the Law on Children or its guiding Decree 56. It is also unclear as to what type of information could affect "the normal physical and mental development of children"; and how it is distinguished from "information harmful to children in the network environment". To the extent MIC wishes to regulate child protection, Decree 72 (including this Article 5.1(e)) should not expand upon the provisions of the Law on Children.	Where child protection is a priority, we recommend amending the scope of Article 5.1(e) such that it covers child abuse (being a clearer term) in the network environment: "e) acts of child abuse". This as opposed to a general information ban which is arguably more onerous than that under the Law on Children. Alternatively, this provision should use the defined term 'Information harmful to children in the network environment' for consistency. We would recommend for MIC to consider revising this provision to: "Đăng tải thông tin ảnh hưởng đến sự phát triển bình thường về thể chất và tinh thần của trẻ em"

			We would also recommend that there should be specific criteria and elements of offense used so as to determine that a subject is in violation of this prohibition.
7	Article 5.1(g)	It would be duplicative to regulate the infringement of intellectual property rights under Decree 72, given that regulations already exist under the Law on Intellectual Property and their guiding instruments, including the Joint Circular 07/2012/TTLT-BTTTT-BVHTTDL that was specifically enacted to address the duty of enterprises providing intermediary services to protect intellectual property rights on the internet and telecommunication networks environment. Given that Article 5.1(g) read with Article 22.3(b) empowers the MIC to issue Take-down Requests (TDRs) for information infringing intellectual property rights for the first time, greater clarity is needed on what the MIC would consider an infringement of intellectual property rights, for example, whether such an infringement is to be assessed against standards present in other legislation, such as the Law on Intellectual Property and related guiding instruments. Moreover, we would need more clarification for when MIC, instead of the right holders, reports content to platforms.	We recommend that Article 5.1(g) be deleted. Alternatively, we recommend it reference the Law on Intellectual Property and their guiding instruments should be inserted to ensure consistency between legislative instruments.
8	Article 5.7	To allow subjects to feasibly comply with the Decree, the prohibitions at Article 5 should be exhaustive. The catch-all provision in Article 5.7 leaves great uncertainty over the conduct that individuals and organizations should refrain in the network environment. For service providers, Article 5.7 makes it impossible	We recommend removing Article 5.7 to avoid uncertainty in the list of prohibited acts.

		for them to put in place compliance strategies that are catered to the Decree 72 prohibitions.	
9	Article 11.2 and 11.3	We encourage MIC to ensure that the VNIX is neutral and open enabling a competitive IX industry and respectfully recommend MIC/GVN to draw from the best practice framework released by UNESCAP and the Internet Society (ISOC) in setting up the right policies and enabling regulatory environment for the IX.[2] We also recommend that MIC/GVN refer to the International Telecommunication Union's (ITU) recommendations and Singapore's model in developing an enabling policy environment by providing as much policy and regulatory transparency as possible to encourage regional and international entities to participate in the local interconnection and peering. This will help develop a diversity of independent international gateways which is required to maintain a healthy internet ecosystem, reliable and high-quality internet access, lower network costs, and continued investments. According to UNESCAP, healthy competition in the local and international telecommunications market, especially through multiple independent internet gateways, will have the following impact on the growth of Vietnam's digital economy:	We would encourage MIC to open up VNIX services for competition, liberalizing IX industry and allow private industry participants to operate and manage VNIXs and welcome MIC/GVN to draw from International Telecommunication Union's (ITU) recommendations and Singapore's model for liberalizing international gateways.

[2] https://www.unescap.org/sites/default/files/2%20ISOC%20ESCAP_CLMV_IXP_BestPractice_Jul20.pdf

		• A lower cost of international bandwidth in the country, due to the entrance of new players to the market, as well as subsequent pursuit of operational efficiencies from the incumbent operator. • A lower cost of retail broadband services, whether fixed or mobile, following the cost reduction of international bandwidth. • A better quality of service for end users, because the competition would push the operators of international gateway to improve the quality of their services, compared to a monopoly situation. • More content hosted locally, which would improve both the quality of service for end users and help build a healthy hosting and peering economy in-country. • A more dynamic telecommunications sector, with more diverse players and offers for end users, more investment from players, more demand of broadband services and more innovative services.	
10	Article 22.1	**Extremely broad enforcement targets in the revised Decree 72 draft**. • Article 22, which now deals with cross-border provision of information, has vastly enlarged the scope of enforcement targets relative to what was intended by the previous iteration of Decree 72 draft amendments. Practically all foreign organizations, enterprises and individuals would be covered by this article.	We recommend that deliberation and consultations with the industry is necessary to better understand MIC's intended policy objectives. Furthermore, we recommend that the Draft Decree exempts foreign organizations providing digital information on their international platforms targeting an international

		• Under the Draft Decree, foreign organizations, enterprises, and/or individuals that **provide information across borders** and: o Rent digital data storage in Vietnam; or o Have at least 100,000 of unique visitors (UV)[3] in Vietnam per month • Will have the rights and obligations set out under Article 22.3.	audience (not specifically targeting visitors from Vietnam) from these requirements. We would also appreciate clarity and examples as to what constitute "specialized application services", for instance, whether international foreign news websites which do not target Vietnamese users but are accessible from Vietnam constitute "specialized application services".
11	Article 22.2(a)	Requirement for cross-border information providers to enter into a content cooperation agreement with Vietnamese press agencies when citing information from the Vietnamese press in accordance with copyright regulations. However, it is not clear: • What type of content cooperation agreement should be in place • To what extent/specific circumstances the offshore providers and Vietnamese press agency must enter into this contract • What level of "information cited" triggers this requirement, whether indicating the URL to link to the original websites can be consider "information cited", or • Whether there are other qualifications for this contract.	We recommend removing these requirements as all copyright related regulations should be centrally covered under the Intellectual Property Law and its implementation regulations.

[3] Article 22.3, the Draft Decree.

		• There is no definition of what is called "Vietnamese press agency", and whether this refers to the State or private sector. At the same time, according to Article 19 of Decree 22/2018/ND-CP providing guidance on Intellectual Property Law 2005 and Law on amendments to the Intellectual Property Law 2009, daily news briefs which are merely of informatory nature and contain no creative elements are not covered by copyright protection.	
12	Article 22.3	The term "*unique visitor*" should be defined under the Draft Decree to avoid confusion. The term should be broad enough to be applied/calculated in different sectors.	We recommend that the Article could include an upward review of the threshold of monthly Unique Visitors (UV) in Vietnam to 1 million people, as was suggested in earlier iterations of Decree 72 draft amendments. In addition, we recommend the MIC to clarify the definition of "*unique visitor*" under the Draft Decree.
13	Article 22.3(c)	It is unclear what this provision aims to achieve and it is therefore challenging to determine how businesses should comply. There is no explanation of the purpose of this provision or what the requirements are for any "content cooperation agreement." Introducing this new concept without any explanation invites uncertainty into the legislation. In general, Governments should not be dictating the terms of commercial agreements between parties. To the extent the intention of Article 22.3(c) is to ensure copyright protection, then it is unnecessary because the existing and proposed	We recommend Article 22.3(c) be deleted.

		provisions of the decree already address IP infringement (e.g., existing Article 5.1(dd), proposed Article 5.1(g)). We would recommend that matters concerning copyright in press activities should be left to regulations that are specific to intellectual property (Law on Intellectual Property) and/or press activities (Law on Press) - instead of a decree that targets online services and online information. Otherwise, it presents a risk of conflicts among legislation. • The Law on Intellectual Property already regulates the copyright protection of press works, and Decree 22/2018/ND-CP was enacted to detail further matters concerning copyright. • Article 37 of the Law on Press already regulates cooperation or associations that may be formed between press agencies and other legal entities or individuals. To the extent it is required for every citation of Vietnamese press information, this would conflict with Article 25 of the Law on Intellectual Property. Article 25.1(b) of the Law on Intellectual Property allows parties to make reasonable citations of works without needing to seek permission or pay remuneration. To avoid doubt, the requirement in Article 22.3(c) should exclude intermediaries that only provide a platform through which information is disseminated. In such case, publishers choose whether their content appears on the platform, which should not raise any copyright concerns.	

14	Article 22.3(d)	Licensing, local entity establishment, and data localization requirements are costly requirements which would stifle innovation in cloud services and prevent many providers from offering services in Vietnam. Such requirements are not only highly restrictive for foreign businesses, but also may prove detrimental for Vietnamese businesses who heavily use online social networks to sell to customers outside Vietnam. In addition, data localization would put people and businesses' sensitive or proprietary data at greater risk of a security breach. This is because companies of all sizes use distributed networks, where data storage is spread over servers in different locations--often in different parts of the world. Distributed networks prove critical to increasing resilience and enabling back-up service in the event of a network failure. Data that is only stored locally would be destroyed or made inaccessible in the event of an outage in that location, significantly hindering the ability of businesses to prosper. By requiring data to be stored in a centralized, and therefore more accessible, location, data localization also leaves the networks and data more vulnerable to intrusion and exfiltration by malicious or unauthorized third parties. It is also important to note that the 100,000 UV threshold is unduly low, capturing mostly SMEs. These requirements will significantly raise business costs for offshore Internet organizations in their efforts to comply, possibly leading to higher costs for Vietnamese businesses using these platforms. Businesses use data to create value, and this value can only be maximized when data is allowed to flow freely across borders. COVID-19 has demonstrated that data flows are critical, enabling both economic responses (such as data sharing for medical	We suggest removing the licensing, local entity establishment, and data localization requirements. There are a variety of ways in which providers are accessible to relevant competent authorities in Vietnam as well as Vietnamese users. For example, providing contact information, including that of a specialized unit as envisioned in Article 22.3 (dd) to process and respond to requests and complaints from competent authorities and users respectively, enables access and necessary dialogue to take place. Further, foreign organizations providing digital information on their international platforms targeting an international audience (not specifically targeting visitors from Vietnam) should be exempt from these requirements. If the intent is to ensure personal data security, there are other measures that can be used, such as the framework of a Personal Data Protection Decree which is currently in progress in Vietnam. We also recommend for MIC to completely remove the reference to the Cybersecurity Law from the Draft

		research, adoption of digital services for business continuity), as well as societal responses (such as online video calls with friends and family to stay in touch during lockdowns). Data localization requirements will make it harder for Vietnam to harness the value of the data, stifling innovation and economic growth. Further, data localization is not technically feasible for companies providing global services to a set of global users. It goes against how the internet works, where data is exchanged between people in different countries. For global companies, infrastructure (both physical and software) work as a whole system to allow them to serve users. User data is processed and stored across servers globally--irrespective of the geographic origin of any data. It is not technically feasible to wall off Vietnamese user data from other countries and not transfer Vietnamese user data outside the country, as would be required by the draft provisions in Decree 72. One piece of data often relates to or is shared between multiple users, who may be in different locations. It would be impossible to maintain global services without the ability to transfer data across borders. Additionally, Article 22.3 references Article 26.3 of the Cybersecurity Law and other relevant implementing legislation. However, making such a reference under the Draft Decree may potentially cause conflict with the Cybersecurity Law. To elaborate: • **For MIC to consider omitting**: The Cybersecurity Law generally applies to both local and offshore entities engaging in the protection of national security and public order in the cyberspace. Generally, Regulated Cross-	Decree because it not only is unnecessary but also causes potential conflict with the existing law.

		Border Information Providers are also under the purview of this law and subjected to all relevant requirements thereof, including the data localization and local office requirements, if applicable. It is not necessary to reiterate the provision in the Draft Decree and we would therefore recommend omitting this section • **Potential conflict**: Article 26 of the Cybersecurity Law requires that local and foreign enterprises, which: i. Provide services on the telecom network, the internet and value-added services on cyberspace in Vietnam; and ii. Are involved in the collection, exploitation, analysis [and/or] processing of personal information, data about users' relationship [and/or] all other data generated by users in Vietnam to store those data within the territory of Vietnam must store those data within the territory of Vietnam. Foreign businesses that fall within the scope of this clause are required to establish either a branch or a representative office (RO) in Vietnam. Thus, only foreign enterprises that fulfil both points (i) and (ii) above must store data and set up either a branch or a RO in Vietnam. In addition, in the Draft Decree guiding the Cybersecurity Law, the MPS intended to limit the scope of enterprises that could be subject to the local office requirement by providing additional conditions/prong-test. Please refer to the version of the Draft Decree of 31 October 2018 for reference. By imposing the data localization and local branch/RO requirement on all Regulated Cross-Border Information Providers, the Draft Decree is broadening the scope of enterprises that could	

		be subject to this requirement and thus, would be in conflict with the Cybersecurity Law. Furthermore, the requirement of this Article would stand in contravention of Vietnam's international commitments. Specifically, it contravenes Article 10.6 of the CPTPP on maintaining local representative office, and Article 14.13 of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and Article 7.6(b) of the ASEAN Agreement on Electronic Commerce on using or locating local computing facilities. Similarly, it disrupts Vietnam's commitments to open its market to foreign investors for the cross-border supply of services under other various investment instruments (e.g., WTO). Lastly, data localization requirements have not been proposed for Vietnamese companies that reach the 100,000 UV threshold. There are no regulations in Vietnam that impose a blanket requirement on Vietnamese companies, who operate websites or applications with 100,000+ UVs, to retain their data within the Vietnamese territory. Therefore, this requirement risks being perceived as discriminatory particularly against foreign organizations and individuals who have invested in Vietnam (whether by cross-border supply or via a commercial presence) pursuant to the country's international commitments, and who have online applications made available to Vietnamese users. Consequently, it risks violating the principles of non-discrimination between	

		foreign and Vietnamese investors which have been specified in various investment protection treaties. In addition, national treatment obligations for cross-border trade in services exist under Article 10.3 of the CPTPP.	
15	Article 22.3(dd)	There are no clear requirements on the qualifications of a "specialized unit." In particular, it remains unclear as to whether such a "specialized unit" must meet any specific requirements on (i) the number of personnel/employees, (ii) minimum qualifications of employees working at the department, and (iii) whether the information of the department need to be communicated with the MIC. Additionally, the Draft Decree 72 does not specify what type of customer complaints (for example, relating to illegal contents, or services) are scoped under this regulation. Cross-border companies already have channels/webforms to receive users' complaints for specific products and services for respective purposes. The private sector should determine how internal departments are set up for customer support.	Instead of requesting Regulated Cross-Border Information Providers to have a specialized unit, we recommend that MIC allow each Regulated Cross-border Information Provider to decide their own internal business structure based on their commercial needs and conditions. As such, we recommend removing these requirements from this Draft Decree.
16	Article 22.3(g)	From the service providers' perspective, Articles 22.3(g) and 23.7(g) are operationally very challenging to implement, because the scope of notification subjects is too wide. The 10,000 follower/subscriber threshold captures millions of channels and fan pages that exist worldwide. • Organizations cannot reasonably be expected to identify whether each of these channels and fan pages have	We highly recommend removing this regulation, together with all references to the notification requirements, since it is so onerous and will negatively affect offshore providers' interests and motivations in continuing its service provision to customers in Vietnam.

		undertaken the notification procedures with MIC. Such screening exercise is not feasible, as it would require review by moderators on an individualized basis. No companies - regardless of their size - have the organizational capacity to undertake such reviews. • These articles fail to take into account the reality that follower/subscriber numbers are in constant flux. Therefore, the provision also requires organizations to perform an impossible exercise of having to constantly monitor new and existing channels/fan pages to identify when the 10,000 thresholds would be reached. • The organization cannot be expected to monitor whether a user generates revenue through its account, channel, or fan page. Aside from payment channels that may be directly integrated into the platform, the user's monetization efforts cannot be expected to fall within the social network's visibility. • As such, these Articles in the Draft Decree would unfairly shift the burden of ensuring the users' legal compliance onto the social network service provider - particularly when the latter is an intermediary that only provides a platform through which users interact. Generally, one party should never in any way be responsible and liable for regulatory compliance obligations of another external party, especially as it becomes obviously infeasible when the offshore providers are incorporated and operating overseas, pursuant to foreign jurisdiction. Articles 22.3(g) and 23.7(g) are very challenging to implement, as they fail to take into account the borderless nature of social networks.	Alternatively, we recommend the Draft Decree clarifies that the notification obligation rests only on Vietnamese account users, and Vietnamese operators of fan pages and channels and not on service providers. The regulator should be the only body having sufficient competence, function and authority to examine and certify if a user has complied with local laws, not service providers. In addition, if the provision is to remain, we recommend the MIC carve out live-streaming activities that are not news-based (for example, exercise and fitness classes, education and business training, medical/healthcare services) that would: (i) Not require the individuals to provide their contact details to MIC, and/or (ii) Not require the foreign organizations providing a platform for such activities to be licensed by MIC OR we recommend that the application of a MIC license be waived for foreign

		• Social network allows for global connectivity - providing users across the world with a common platform through which they are able to engage and develop relationships. Article 22.3(g) will effectively require foreign organizations to go against this construct, by developing a Vietnam-centric solution that (i) requires screening of channels and pages against a Vietnam-specific notification requirement and (ii) denies Vietnamese users with access to most channels and fan pages that reach the 100,000 thresholds. This presents significant and unresolvable engineering challenges. • No similar solution has been created by other countries. It would place Vietnam as an anomaly and goes against the country's economic plans. To the extent the Government seeks to address channels or fan pages that engage in prohibited conduct, then Articles 22.3(g) and 23.7(g) are unjustified and disproportionate measures. It fails to take into account that a significant majority of channels and fan pages exist for legitimate reasons - for example, sharing legitimate information and fostering relationships. With the majority of Vietnam's citizens already using social media, Article 22.3(g) would have wide socioeconomic consequences. By removing access to all channels or fan pages that have not notified MIC, it denies Vietnamese users the ability to access contemporaneous information (both inside and outside of Vietnam) on matters that affect them. Globally, it would cut access by Vietnamese users to overseas communities. Some examples where this consequence may be profound:	live-streaming platforms whose total unique monthly visitors in Vietnam is less than 100,000.

		• A large number of SMEs in Vietnam are reliant on social media as a means of connecting with customers or employees - some even having their business centered on social media engagement. Many of these SMEs do so through the channels and fan pages that the draft intends to capture. Article 22.3(g) would severely and adversely impact these SMEs. For those Vietnam-based businesses that rely on outreach with customers outside of Vietnam, they are left at a competitive disadvantage against businesses of other jurisdictions that do not impose similar restrictions. • During measures to combat the COVID-19 pandemic, a significant number of Vietnamese users were reliant on community-based efforts to access essential goods and services. For example, fitness instructors, doctors providing tele-health services, psychologists/therapists providing counselling and mental health services, as well as tuition teachers/schools providing education services, could all be considered "live-streaming". Had Article 22.3(g) been effective, it would have curtailed these efforts by (i) denying users access to such information and/or (ii) discouraging users from initiating such community-based efforts. • For Vietnamese users seeking information on affairs outside of Vietnam (e.g., students seeking to study overseas, expatriates or individuals planning to emigrate overseas), these channels or fan pages are often the only contemporaneous resource available. Article 22.3(g) would deny these users the ability to access such information.	

		It is uncertain as to what Article 22.3(g) seeks to achieve, when there are already wide, legal channels through which the Government can address the dissemination of prohibited content. For example, Article 5 of Decree 72 already regulates prohibited acts in the online environment, and against which the Government is empowered to order removal of content. Assuming MIC targets those deemed to be spreading fake news and disinformation, it would be impractical and a burden on MIC's resources to lump all live-streamers together, and for MIC staff to process notifications from those not providing news to their viewers – for instance, fitness instructors. The target subjects of the notification are unclear. Whereas Article 22.3(g) requires blanket notification if livestreaming or revenue generation is involved, it fails to address the reality that the channel or fan page owner may not actually be the user who engages in such activity. Social network communities exist because they allow for interaction among users - not necessarily just a unilateral flow of information from one user. • It is entirely possible that livestreaming or revenue generation could be undertaken by another participant within the channel or fan page. • Article 22.3(g) does not address such scenarios. It would not be appropriate for the channel or fan page owner (i.e., the notifying party) to bear the responsibility of the conduct of other users that participate in the channel or fan page. This would discourage the creation of any such channel or fan page. • It would also not be possible for MIC to require a notification from every single user that seeks to livestream	

		or generate revenue through the channel or fan page. This would essentially cover millions of users.	
17	Article 22.3(h)	Where the interests of individual users are concerned, the Law on Consumer Rights Protection already regulates the rights of consumers in Vietnam and the liability of organizations that provide services to consumers in Vietnam. Article 14.2 of the Law on Consumer Rights Protection expressly requires consumer contracts to be clear and easy to understand. Therefore, it is we would recommend that MIC does not impose an additional layer of obligations on the organization, which would already be subsumed into such provisions. The standards of what comprises something that is "concise, clear, intuitive and easy to understand" is highly subjective, and has not been defined or regulated. It is also an extension to the criteria under Article 14 of the Law on Consumer Rights Protection above.	We recommend that Article 22.3(h) be deleted.
18	Article 22.3(i)	Regulated Cross-Border Information Providers must prepare annual reports (before 31 December each year) or reports on an ad-hoc basis at the request of MIC. Such reports must be made in accordance with Form No. 04 in the Annex of the Draft Decree. The report Form No. 04 includes information regarding: • Total number of users in Vietnam as of the reporting date; • Number of unique visitors in Vietnam;	We recommend that Article 22.3(i) be deleted. Alternatively, we recommend for MIC to amend certain sections of Form No. 4, particularly: ○ Remove the section regarding "*A detailed list of complaints*

		• Revenue generated in Vietnam; • A detailed list of complaints on content from users in Vietnam that have been handled, including (i) content of the complaint, (ii) account of the complainant, and (ii) handling result; • Total number of illegal content that has been handled; and • Changes to contact information (if there are any changes). Users' complaints may include personal data and privileged information, and thus, a Regulated Cross-Border Information Provider will need to obtain express consent from the users. This requirement could cause the users to be more hesitant in reporting violations and/or illegal activities. Additionally, considering the large volume of complaints that a Regulated Cross-Border Information Provider may receive within a year, reporting all complaints and their details could be quite burdensome. Consequently, this requirement is onerous and impractical for foreign service providers that do not maintain a presence in Vietnam. This is compounded by the fact that a 100,000 UV threshold is low, and already captures a significant number of service providers. In addition, revenue data should not be required in the report because (i) it is irrelevant, (ii) Decree 72 is not the appropriate legal platform to do so and (iii) it is unclear as to the type of revenue that the report seeks to capture. For example: • Decree 72 would arguably require e-commerce websites that reach the 100,000 UV threshold to submit reports. It is	*on content from users in Vietnam that have been handled, including (i) content of the complaint, (ii) account of the complainant, and (ii) handling result*". We would also like the MIC to clarify the "*illegal content*" section, and how would (i) the total number of users in Vietnam, and (ii) the total revenue generated in Vietnam be calculated.

		not clear whether the reported "revenue" is intended to include sales that were generated by selling the goods to buyers in Vietnam. Such type of revenue data would not fall within the oversight of MIC. • A major source of revenue for social networks is advertising. The Law on Advertising and Decree 70/2021/ND-CP already regulates business activities concerning cross-border advertising. The reporting requirement should not be applied to those organisations that already publish transparency reports on a periodic basis. These reports are available to the public, including the Government, and contain much of the data and statistics in Form No. 4.	
19	Article 22.4	While the offshore service providers are not incorporated in VN territory, these providers are not obliged to disclose their data and their business revenue to the local authorities, but to comply with the strict regulations within their own jurisdiction. At the same time, global companies must adhere to their own strict internal policies and contractual agreements with customers, including among others, disclosure of sensitive information, privacy and business confidential information. As this is not a known worldwide practice, it will significantly reduce the interest of foreign entities to actively provide useful and efficient solutions and support to local businesses and users. If the government is looking to regulate citizens in the country, the requirements should directly address local users or companies, not	We strongly recommend removing the request for information from offshore providers. For information on content removal among others, local authorities can refer to transparency reports published by companies that contain data for Vietnam. We also recommend the MIC amend the wording of the second point under Article 22.4(a) as follows: "*Contact point: name of the representative organization or*

		offshore service providers. Having said that, some information can be found in globally published reports by companies such as transparency reports on content removal or efforts to combat child abuse safety contents on their platforms with country-by-country data. This requirement may also be interpreted to mean that Regulated Cross-Border Information Providers must appoint/authorize a representative organization or an individual in Vietnam (i.e., a contact point in Vietnam).	*individual in Vietnam **(if any)**, email address, and phone number.*" In accordance with the above-suggested amendment, Regulated Cross-border Information Providers will have the right to appoint a contact point in Vietnam **at their own discretion** and in accordance with their internal business structure and capacity.
20	Article 22.5, Article 22.3(b), and Article 22.3(e)	**24 hours or 3 hours (for live-streaming)** to deal with complaints on content from Vietnamese users and MIC is too short, as Regulated Cross-Border Information Providers need sufficient time to review the complaint and content and coordinate internally to make an official response to the authorities. This is especially the case for cloud service providers who act only as intermediaries for the content in question, and who may not be able to monitor their networks for such content due to legal restrictions in other jurisdictions and/or in their customer contracts and may need time to identify and contact the customer (of the cloud service provider) that was the source of the content. The new take-down time frame does not reflect ground realities of how the global digital economy operates. As a matter of practice, the current 48-hour turnaround time required under Circular 38 effective since 2016 already presents practical difficulties and obstacles. It does not reflect scenarios where a high volume of content (hundreds or thousands) is submitted at the same time.	We recommend that the Decree removes 24-hour (or 3 hours for live-streaming) timeline for user's complaint as platforms have their global policies and procedures to determine and implement how to handle users' complaints and what are the penalties for repeated violations. Alternatively, we recommend replacing the time frame of 24 or 3 hours with a clear, reasonable mechanism and timelines for cross-border information providers to review, comply and appeal the MIC's takedown requests. • In accordance with international standards (e.g., the European

		To ensure a globally-consistent approach and application, content removal decisions are centralized at headquarters and require analysis and participation by multiple stakeholders. In addition, organizations remain heavily reliant on human moderators. This is necessary not least because (i) the criteria for determining what comprises unlawful content are not always clear, due to lack of information from the complaints or context from the local laws (ii) only human moderators are able to understand the contexts and nuances of content, and (iii) certain types of subjective and highly contextual content are not suitable for technology-assisted review (e.g., defamatory content or content that "infringes the honor and dignity" of an individual). Communicating with international teams, time zone differences also make a 24-hour takedown time infeasible. In certain emergency circumstances, we have and continue to make best efforts to respond to requests by government authorities as soon as we can. This is only possible for emergency cases, not for removal at scale. We have a strong commitment to comply with the law and protect our users. We have put in place and published policies and procedures to enable users and government agencies to report content for removal under applicable laws. As illegal content may vary from country to country, reasonable time is required to ensure due process and that the claims are accurate. Generally, the regulation should not attempt to compel foreign companies to take down customer content hosted on their systems where such content is hosted on equipment outside of Vietnam (and may be lawful content in the country in which it is hosted).	Union's GDPR or Singapore's PDPA Amendment), we suggest this to be changed to allow 72 hours for a company to respond to the request. Furthermore, while a service provider is well suited to determine if a user's actions violate their company's policies (e.g., an Acceptable Use Policy), they are not well suited to evaluate whether a particular customer has violated certain Vietnamese regulations and a complaint is "legitimate." Requiring a foreign organization to self-determine what is a "legitimate" complaint that someone has violated Vietnamese law and temporarily block or remove reported content could lead to a subjective or erroneous interpretation of law, materially harming customers and end users. • Alternatively, we recommend the following approach: (i) prioritize contents which may lead to **imminent harm to lives or cause immediate injury**, and **have them removed as expeditiously as possible**, and

		Requests to block of remove unlawful content, requests to cooperate with law enforcement in relation to unlawful content, and requirements to execute content cooperation agreements with press agencies should be directed to the entity responsible for publishing that content, not an intermediary hosting that content (such as a cloud service provider or data center service provider). Additionally, the proposed amendments do not include an opportunity for foreign Internet organizations to appeal or clarify with MIC, before content is taken down. Application developers should be given the opportunity to make changes that remedy the illegal activity, rather than have their apps removed. Decisions to remove a game or an app from an app store are not taken lightly. There are many considerations and factual research is required to help all sides make the right decision. At the same time, companies have put in place strict and rigorous global policies and procedures to ensure apps listed in their platform to ensure a safe and trustworthy ecosystem for users and developers as well as protect them from bad actors. Similarly, the requirement to **remove law-violating apps from application stores within 24 hours** is unreasonable. The scope of the measure is vague, as it would require 24-hour takedown upon any violation of the law by the online applications. To the extent any such removal provision is to be imposed, it can only be feasibly implemented when there is a clear scope of the violations that would give rise to removal. In addition, it is unclear what this measure aims to achieve, considering the existing legislation already has in place a broad range of measures to address legal violations.	(ii) review and take appropriate action on all other categories of contents in a timely manner. This would allow platforms to seek guidance/clarification and consult legal experts before making any decision to remove content. We recommend removing the 24-hour timeline for app removal from application stores. We recommend removing the provision in Article 22.3(e) regarding user complaints. Information providers should handle user reports in accordance with their internal policies, and only be legally required to comply with take down requests from the competent authorities (e.g., the MIC). Alternatively, we recommend the 24-hour turnaround timelines should be removed as being operationally infeasible, and the information sharing requirements should be removed.

		Likewise, the proposed **24-hour turnaround time to address user complaints** is neither reasonable nor operationally feasible. User complaints are not always reliable, and have been open to abuse. A greater time window will be required for an organization to thoroughly and accurately review the veracity of the complaints. There is no clear justification for the requirement that an organization provide the complainant's email address to the user whose content is removed. This would likely discourage users from making reports of potential violations, which would have an opposite effect to what the Government is striving to achieve under Article 22.3(e) - that content be regulated through Government action, but through the active participation of the community. In any case, this requirement raises safety and personal data privacy and protection concerns. Personal data protection laws prevent such type of disclosure without a legitimate basis - e.g., consent, which is unlikely to be given by the complainant for reasons above (e.g., safety). Lastly, Regulated Cross-Border Information Providers must block and/or remove illegal content, services, livestreams, accounts, fan pages, and channels at the request of the MIC. The Draft Decree, however, does not clearly define what will constitute "illegal content, services, livestreams, accounts, fan pages, and channels." Under the Draft Decree, the MIC will be the only authority that communicates a takedown request. However, we note that Article 26 of the Cybersecurity Law empowers the Ministry of Public Security ("MPS") to request cross-border information providers to block and/or remove illegal content. There may be cases whereby	We also recommend that the Draft Decree should include a mechanism for foreign Internet organizations to appeal or clarify with MIC, before illegal content is taken down. In addition, the following should also be revised to take into account this review/clarification process: • We recommend the MIC to clarify the concept of "*illegal online, content, services, and applications*" that are subject to a takedown request under the Draft Decree. We note that under Decree 72 and Circular 38, illegal content that is subject to takedown requests will be determined based on Article 5.1 of Decree 72 that provides a list of prohibited acts on cyberspace. • We recommend the MIC to clarify the effectiveness of content takedown requests of other non-MIC authorities, especially content takedown requests issued under the Cybersecurity Law.

		other ministries/authorities base on the Cybersecurity Law (instead of the Draft Decree) to issue a takedown request.	• We recommend the MIC to clarify what would be considered a "Vietnamese user", as it could mean users of the nationality of Vietnam or users that are located in Vietnam.
21	Article 22.6	"Enterprises leasing space for data storage in Vietnam" is not defined. In addition to the fact that cloud service providers lack visibility into customer content and that reporting violating content to the MIC within three hours of detection is untenable, foreign service providers are not properly placed to evaluate the legality of content under Vietnamese regulations. This Draft Decree contains many new obligations relating to domain name registration and maintenance services.	That term should be clarified to make clear that it does not apply to cloud computing service providers, data center service providers, or any similar service providers that have no visibility into the customer content hosted on their systems (and therefore could not comply with the obligations that Article 22 seems to impose on such enterprises). We request clarity on what is intended by "customer information records" in 22.6. We would like to confirm and to be clarified that the scope of these regulations does not extend beyond .vn domain name registrations or services.
22	Article 23.1	Article 23.1, read with article 23.7, fails to remedy the uncertainty as to whether the management and licensing obligations will apply to foreign social networks. Clarity on this subject had been sought	We recommend that foreign social networks should be specifically excluded from the scope of Article 23.1.

		since the enactment of Decree 72. We understand that the Government's intention is for foreign organizations to not be subject to the licensing requirements in Article 23.1. We recommend that this be clarified in the legislation for the avoidance of doubt. As the Draft Decree (at Article 22) now seeks to explicitly regulate foreign organizations, including social networks, it is critical now that greater clarity be given to avoid overlaps (or an over-regulation of foreign organizations). In particular: • Article 23.1, which regulates the subjects of the provisions as "organizations, enterprises operating in Vietnam", fails to clarify whether it would also include foreign organizations whose websites are used or accessed by users in Vietnam. • This is particularly in view of Article 23.7(a), which categorizes social networks into (i) a "foreign social network" which is provided cross-border by foreign individuals/entities and (ii) a "domestic social network", which is clearly defined to be provided by "organizations/entities having Vietnamese legal status". • Therefore, the determination of when an entity is "operating in Vietnam" at Article 23.1 appears to disregard the nationality of social network owner/operator - i.e., thereby including both foreign and domestic social networks. On the other hand, the list of license-exempt websites in the proposed Article 23.2 does not include websites of foreign organizations. The application for social network license under	

		Article 23.7 makes no distinction between Vietnamese and foreign organizations. The Government will derive limited (if any) value from requiring foreign social networks to obtain a license to operate and it may discourage some foreign social networks from entering or continuing to operate in Vietnam. There is no justification to extend the licensing requirements to these foreign social networks. The Government already regulates (and intends to further regulate in Article 22) foreign social networks - via provisions applicable to providers of cross-border information. Other discrete regulations already exist to govern foreign organizations, to which foreign social networks will also need to observe. For example, Article 5 of Decree 72 and Article 5 of the Law on Cybersecurity already specify a broad scope of prohibited acts and requirements which are applicable to foreign organizations. The onshore licensing requirement will act as a barrier to entry for foreign social networks. It goes against the borderless nature of such services (and Internet-based services in general), which thrive on the ease of global connectivity. It further fails to take into account that not all social networks are operated by major corporations. In fact, compounded by the low 10,000 VN threshold, most will be operated by SMEs or even individuals (as social networks include "personal pages"). Over a long-term horizon, Vietnamese users will stand to lose out the greatest. Licensing requirements for social networks would hurt both consumers and the industry by creating a new barrier to entry. Low barriers to entry, the open nature of the internet, and rich interactions and experiences that social networks enable are key to	

		the continued growth of Vietnam's digital economy. Stringent licensing requirements may deny users the ability to access much of these websites, despite their availability to the rest of the world. The licensing requirements may see these websites either move towards content that are exclusionary for the Vietnamese population or even geo-block Vietnam altogether.	
23	Article 23.7(g)	It is unclear if the responsibility of notifying contact information to MIC belongs to Accounts' owners on social networks or the social networks themselves Additionally, based on a combined reading of the amendments to Article 22 and Article 23, it is unclear what exactly the threshold is for licensing. What is the threshold for a Foreign Internet Organization providing social network services to be licensed by MIC? Is it 100,000 or 10,000 unique monthly visitors in Vietnam? It would be important for foreign Internet organizations to understand what exactly the threshold of unique monthly visitors is, for them to be in scope.	The draft should clarify that social networks will take responsibility to notify contact information of those accounts on their platforms to MIC. If Foreign Internet Organizations require a license, the threshold should be risk-based and tailored to the network's reach in Vietnam. This will ensure that MIC is not over-burdened with administrative procedures. In this respect, can the threshold for licensing set by MIC be 100,000 (and not 10,000) monthly unique visitors?
24	Article 34d	We request for clarity regarding if and how this provision applies to data center service providers and how that works with Article 44. Complying with this provision would requires (1) the CSP to know a customer is subject to the laws of Vietnam, is in the business of publishing games, and is required to obtain a license, and (2) the CSP to proactively verify the customer has such license. Cloud	Article 34 (d) should be revised to ensure that the respective regulatory compliance obligations are imposed on video game services providers only.

		service providers have no visibility into a customer's content, or which regulatory requirements apply to that customer. Most businesses would have an obligation in their Customer Agreement stating that the customer must comply with whatever laws are applicable to its business. It is not feasible to "proactively refuse, suspend or discontinue connection with video game providers" for carrying on certain activities (of which the cloud service providers would have no knowledge) without a license. This section also requires that CSPs proactively report detected information safety and security violations to the government. These responsibilities should lie with the customer and the relevant regulator.	
25	Article 44a.3	This Article requires telecommunications enterprises and Internet service providers to: • monitor their networks and block offending content; and • connect with MIC's systems and implement such measures as may be requested by MIC. Concerning network monitoring, telecommunications enterprises and Internet service providers are often prevented, due to secrecy obligations under the laws of various jurisdictions around the world and in their customer contracts, from monitoring the contents of communications flowing across their networks. Accordingly, it may not be legally (or, in some cases, technically) feasible for such enterprises and providers to take proactive measures to filter out or block offending content. Regarding the connection with MIC's systems, this may compromise the overall security of the network of telecommunications enterprises and Internet service providers. This may also result in such enterprises and providers being in	Omit Article 44 (a.3). In its place, have a provision requiring telecommunications enterprises and Internet service providers to provide reasonable cooperation to MIC with respect to ensuring network security.

		breach of the security laws of other jurisdictions. It is also unclear what measures MIC may request, and these may prove to be technically infeasible and overly onerous.	
26	Article 44b.3	This Article requires telecommunications and Internet enterprises to put in place a variety of measures at the request of MIC. It is also unclear what measures MIC may request, and these may prove to be technically infeasible and overly onerous.	Amend Article 44 (b.3) to require that MIC consult with the enterprises on the measures to be put in place, and to only request for such measures as may be reasonable and technically feasible.
27	Article 44c and 44h.2	A termination or suspension of data center services would likely have an immediate and material impact on our customers. Laws and regulations should be enforced by government agencies, not by data center service providers who can discontinue services based on their terms and conditions. Data center service providers should have the flexibility in their contractual provisions/terms and conditions.	We recommend the removal of this wording in Article 44c: "discontinue service for organizations and individuals that violate the regulations on information security." Alternatively, we request for the clarity that a service provider may base on our contractual terms and conditions to discontinue services following a court judgment/formal legal process confirming that the applicable customer violated the laws or regulations on information security. Vietnam should not force a service provider to discontinue services merely due to allegations or a subjective opinion that a service provider has violated the regulations.

28	Article 44d	This section proposes other responsibilities related to child protection in the Internet that would apply to both onshore and offshore social network providers having 1,000,000 or more unique visitor of as follows: • Show warning that contents are not suitable for children. • Have a feature where content harmful to children, child abuse acts can be reported; Publicize the handling process for such contents; Share the statistics about the total number of complaints and handling results with the MIC (AIS) on a quarterly basis. • Block, filter out contents harmful to children, and users accounts with child abuse acts. • Implement age registration in case of user account registration and take measures to help parents and caregivers monitor the activities of users who are children. We agree that child online safety is very important and must be enhanced. For years, we have been continuously investing in safety measures and improving our services and features to handle inappropriate content for children, as well as to provide more options for parents/guardians in managing, monitoring and deciding what and how their kids can explore useful information via the Internet. In addition, we also publishes transparency reports indicating our efforts and resources to combat with child abuse safety contents on our platforms. Article 44.d.1 This Article requires data center service businesses to register. It is unclear what such registration process entails.	We recommend that offshore providers' efforts to publish and update transparency reports be recognized and that the decree not impose a timeframe restriction (i.e. quarterly report) Omit Article 44d.1 in its entirety. Alternatively, amend Article 44d.1 to provide for a simple notification requirement. In line with global laws on privacy or electronic transactions, we propose that the regulation, and this notice requirement, should apply only to entities formed or recognized under the laws of Vietnam.

		As discussed in section 4 above, it would not be practicable or enforceable for Vietnam to exercise extra-territorial effect of Vietnamese laws on offshore companies.	
29	Article 44d.2(a)	For social networks to display warnings on content (that it may be unsuitable for children) will require them to proactively review and inspect each content to ascertain whether the warning should be applied. However, proactive review is impossible to comply with because social networks are online intermediaries that typically play no direct role in the creation or dissemination of content. This is unlike, for example, broadcasters and online publishers that are actively involved in screening, potentially curating, and disseminating the content. This means the same or similar in Circular 09/2017/TT-BTTTT cannot be applied to social network service providers. For social network service providers, billions of new content are produced and transmitted on their platform each day. There is currently no process or technology that is sophisticated enough to review and flag such volumes against the criteria required in the draft. This is made even more challenging by the lack of clarity in Article 44d.2, which gives it an unlimited reach: • It is unclear as to what "content" will be subject to the warnings. If it is intended to apply against all user-generated content, then this would include comments, posts, reviews, images, videos and other forms of social media engagement.	We recommend that Article 44d.2(a) should be deleted. The warning requirement is better placed on the content producers/generators, especially in light of the fact that organizations and enterprises are already required to provide guidance on the use of services and access to information to protect children, pursuant to Article 34.3 of Decree 56.

		• Not only would reviewing all such content be impossible, but the placement of the "warnings" presents technical challenges • It is unclear as to when content would be deemed "not suitable for children". This criterion is neither defined nor guided by existing legislation. As a child is a person anywhere up to 16 years of age, whether content is considered suitable varies considerably. In addition, the requirement to include warnings would not be necessary, as the law already mandates the removal of violating content against children. It is overly prescriptive to impose obligations on organizations to apply both proactive and reactive measures. Article 35.3 of Decree 56 envisages that to ensure child safety in the network environment, organizations would provide warnings or remove harmful content. The law also already regulates other measures with the interest of minimizing harm to children. For example: • Article 5 of Decree 72 already prohibits obscene and pornographic material; • the draft (at Article 44d) is proposing to block and filter out child abuse content; • Article 8.14 of the Law on Advertising already bans advertisements that could adversely affect children, as well as other unsuitable content (e.g., alcohol and gambling); and	

30	Article 44d.2(b)	The criteria of when content is "harmful to children" is unclear, and open to subjective interpretation. Any reporting feature that relies on such criteria would invariably be open to abuse, and presents challenges for the social network service providers in determining whether the content is "harmful". Consequently, the MIC is unlikely to derive benefit from statistics through the quarterly reports in this Article 44d.2(b). In contrast, we note that the Government has defined clearer criteria in determining age suitability of other types of audio-visual content. For example: • For online games, the Government was able to determine age suitability by reference to content involving violence or combat, depictions of sexual imagery, and age-inappropriate language (Article 31a in Draft Decree 72). • For films, the Government was able to determine age suitability by reference to content involving violence, nudity, sex, depictions of drugs, stimulants and narcotic substances, horror, and crude imagery, sound and language (Circular 12/2015/TT-BVHTTDL). Online content should not be subject to a different standard. Therefore, in lieu of legislating a scope of reportable conduct, the Government should define specific content that would be considered "harmful" to children - to the extent they have not already been specified as prohibited acts under Article 5 of Decree 72. The definition at Article 3.40 should be revised accordingly. In addition, it is uncertain as to what type of "data" MIC seeks in relation to the complaints and processing results in Article	We recommend that Article 44d.2(b) be amended by introducing greater clarity on the extent of content that is considered "harmful" to children (which also necessitates revision to Article 3.40). The requirement to share data on reports and result of processing such reports to MIC on a quarterly basis, should be deleted. In addition, we recommend the Article 44d.2(c) be revised for greater clarity, in the same manner as provided in Article 44d.2(b).

		44d.2(b). Due to the "borderless" nature of social media, it is challenging to provide jurisdiction-specific reports. For example, content distributed by Vietnamese users may be reported by overseas users (and vice versa). In any event, the reporting is would also not be necessary. Major social network service providers publish transparency reports on a periodic basis. These reports are available to the public, and provide data and statistics regarding the service provider's actions against violating content.	
31	Article 44e	Legislation should not be used to regulate the provisions of contracts that have been mutually reached between the parties. To do so would go against the principles of freedom of contract under Article 3.2 of the Civil Code. The mandatory contents set out in Article 44e, which are couched in general terms, would not be necessary. This is because much of these items have already been covered by the provisions concerning service contracts under Articles 78 – 87 of the Commercial Law. It is also uncertain as to the rationale for imposing mandatory contractual contents. Particularly, for each of the contents: • The information regarding rights and responsibilities of relevant parties forms the cornerstone of civil contract under Article 385 of the Civil Code – i.e., a contract "in	We recommend that Article 44e be deleted.

		relation to the establishment, modification or termination of civil rights and obligations." • The information regarding prohibited and unlawful acts would be subsumed into the scope of Article 44e.1. Furthermore, the prohibitions under Vietnamese law (particularly those under Article 5 of Decree 72) would exist irrespective of their inclusion in the parties' contract. • The information regarding service standards and commitments that the service providers will deliver would be subsumed into the scope of Article 44e.1. Furthermore, Articles 79 and 80 of the Commercial Law already regulates obligations of the service providers concerning their service performance. • The identification information of the customer that uses the services would already be specified in the course of contracting. To the extent the Government seeks to identify the information of all individuals who use the services, then this would not be operationally feasible. For example, a common cloud service that is offered is ERP product to enterprise. The enterprise customer would not be able to specify each and every employee that would gain access to the ERP product. Finally, mandatory contractual content would be a deterrent for foreign online service providers entering into agreements with local data center providers, which would be detrimental to Vietnam's digital economy.	

32	Article 44g	In light of the proposed broad scope of "data center service providers", the notification requirement is impractical. It will capture a significant number of Vietnamese and foreign service providers. It is further unclear as to the purpose that an Article 44g notice will serve.	We recommend that Article 44g be deleted.
33	Article 44h	Referring to the above main argument that data center/cloud service providers should not be regulated and such regulatory obligations listed in Article 44h should not be imposed on them. As cloud service providers do not have visibility into customer content, it is not feasible to detect and prevent illegal activities. In line with our requests above, we ask for the clarity that a data center service provider only be obligated to discontinue service after receiving a court judgment confirming that the applicable customer violated applicable law. The regulation should also not obligate organizations and individuals to notify foreign organizations of information that they believe violates Vietnamese law. Foreign organizations would often be unable to act on such notifications, as they may be unfounded or based on a subjective or erroneous interpretation of law. Organizations and individuals should instead direct such notices to the Ministry of Information and Communications. Additionally, we request clarity on what is intended by 44.h.5: based on the shared responsibility model explained above, data center/cloud services users elect where to store or transfer their	We recommend deleting the provision 44.h.5 from the draft Decree.

		data/content. Data center service providers do not have control over it: their customer content is typically not transferred outside the country without the customer's decision and consent. This provision is not in line with Article 44.g which acknowledges cross border data services.	
34	Article 44h.1	This Article requires data center service providers to monitor their networks for illegal activities. Data center service providers, which include cloud service providers, are also often subject to secrecy obligations under the laws of various jurisdictions around the world and in their customer contracts, from monitoring the contents of communications flowing across their networks. Accordingly, it may not be legally (or, in some cases, technically) feasible for data center service providers to monitor their networks. It is also operationally and technologically impossible to comply with. Most of the time, service providers are not involved in and would not have visibility over the users' activities. Users are often free to configure the service parameters to suit their needs and/or would consume the services without the service provider's direct involvement. A simple example is an email client that is delivered through a SaaS model. The service provider cannot feasibly develop a solution that is capable of screening and stopping unlawful information from being exchanged through the email client. While by no means exhaustive, given the huge variations of offerings available within the scope of a "cloud computing service", the same challenges exist for services that include servers or databases delivered through a PaaS or IaaS model and services that contain collaborative elements. The reporting requirement is also vague:	We recommend the Article 44h.1 be removed in its entirety.

		• The phrase "unlawful activities" as its stands suggests that service providers are required to report on any violation of Vietnamese law. • As the service providers' scope of responsibility is generally confined to delivering the infrastructure, platform or software (a "hands off" service), it would not be operationally feasible to extend such scope to include policing the conduct of the users. • There is no clarity on which "competent authorities" would receive the reports. Article 44h.1 is also redundant because the draft (at Article 44a) already seeks to impose broad responsibilities on organizations and enterprises to ensure networking information security. These include a requirement to (i) implement network information security to meet safety requirements and (ii) implement measures to detect, filter and stop certain matters (e.g., malicious software).	
35	Article 44h.2	It is not practical or appropriate as a legal matter to impose the burden on the service provider to determine whether or not the customer's use of the service is "unlawful". Only the State authorities can be vested with the ability to make that determination. By shifting the risk onto the service provider in making the judgment, Article 44h.2 may work against the Government's intention in drafting this clause. Service providers are more likely to take a conservative approach, by avoiding any stoppage/end to the customer's use of the services in order minimize liability exposure by the customer.	

36	Article 44h.4	To avoid legislative conflicts, regulations concerning data transfers should be left to the decree on personal data protection.	
37	Article 44h.5	Article 44h.5 is, in effect, a customer data localization requirement. Such requirement has broad socioeconomic implications: It results in greater risk exposure to compromises of customer data. As part of their cybersecurity strategies, both Vietnamese and foreign cloud service providers store data in data centers overseas. One of the major reasons for this is the shortage of sufficiently secure systems in Vietnam. It will ultimately inhibit cloud service adoption by individuals and organizations in Vietnam. One of the drivers of cloud service usage is its cost efficiency for users, which is largely achieved by service providers pooling users and leveraging shared third-party infrastructure - the latter of which is often overseas-based. Mandating the use of Vietnam-based infrastructure can drive costs higher for Vietnamese users - compared to other jurisdictions. This would result in fewer options for local consumers and consequently less overall consumer benefit. For the above reason, it will also inhibit investment in "cloud computing services" in Vietnam. Vietnamese and foreign investors will be disincentivized from developing the services, which are a core component of Vietnam's digital transformation initiatives. This is simply because the localization requirements will increase costs or may not afford the security and safety standards necessitated by the business to make it viable.	We recommend removing Article 44h.5 in its entirety. Alternatively, we recommend clarifying which requirements are applicable to cross-border service providers, and remove the restriction on outbound transfer of customer data. As a principle, we recommend that to avoid legislative conflicts, regulations concerning personal data, such as those in the proposed Article 5.6, should be left to the decree on personal data protection.

		This will put Vietnamese companies at a disadvantage to other countries. Data localization regulations will restrict consumers in Vietnam from being able to use new and innovative online applications and services and impair the ability of Vietnamese businesses to use online applications to grow and reach more people. The global reach of online applications makes them useful to business, including small businesses, because it enables them to reach a larger customer base that extends beyond Vietnam's borders. This, in turn, increases their business and collectively expands the Vietnamese economy. A localization requirement could fragment applications and services provided over the Internet and therefore erode the utility and usefulness of a global outlet for Vietnamese businesses. Keeping the Internet open, decentralized, and free of barriers is critical to helping Vietnamese businesses remain competitive in today's increasingly digital economy. Lastly, this Article imposes data localization requirements on data center service providers which might contravene Vietnam's obligations in the CPTPP not to impose any data or server localization requirements.	
38	Chapter VI on Cross-border data center services	The new Draft Decree 72 introduced a new set of provisions regulating data center service, in which data center service providers doing business on a cross-border basis are particularly required to notify, either directly in writing or via the MIC portal: • Name of the representative; • Contact information (phone number, or email); and • The types of data center services [to be provided on a cross-border basis].	We recommend Chapter VI be deleted in its entirety. Alternatively, we recommend clarifying the scope of who is covered by these requirements.

		Apart from the above requirement, there are other obligations for data center services such as registration, eligible conditions, technical standards, customers' data, handling illegal data, etc. It is unclear: • Whether these requirements apply to local only or also to data centers; • How the draft Data Protection Decree will interact with this Draft Decree regarding personal data privacy. We believe the technical implementation of data centers and cloud computing services should not be subjected to regulation. Rather, areas of concern such as cybersecurity, data protection, and network information services should be addressed in legislation as appropriate in a technology neutral way. The Asia Cloud Computing Association found in its Cloud Readiness Index for 2020[4], that emerging APAC markets risk losing out on economic recovery from Covid-19 by not leveraging promising 'leapfrog' technologies. Vietnam scored the lowest overall for cloud readiness of all the countries analyzed. The Cloud Readiness Index for 2020 also noted that cloud services need secure and reliable data flows across borders, networks, and third-party providers. Government support is also critical to support cloud adoption. But this is not achieved by regulating cloud services or prescribing how cloud services must be provided, instead it requires technology neutral regulation so users know their information is secure and held privately without any unexpected breaches in the cloud.	

[4] https://www.digitalcentre.technology/wp-content/uploads/2020/06/CRI2020_ACCA_Final.pdf

		Similarly, if Vietnam wishes to grow its data center activity and encourage investment locally, it should not prescribe how data centers operate. Instead, it should focus on technology neutral regulation such as cybersecurity and data protection.	