asia cloud computing association

The Asia Cloud Computing Association (ACCA) is the apex industry association for Asia Pacific stakeholders in the cloud computing ecosystem. We represent a vendor-neutral voice of the private sector to government and other stakeholders, with the mission to accelerate the adoption of cloud computing through Asia Pacific by helping to create a trusted and compelling market environment, and a safe and consistent regulatory environment for cloud computing products and services.

ACCA member companies include:

aws

DIGITAL REALTY

EQUINIX

Google Cloud

HSBC

Microsoft

ORACLE

salesforce

Mr Nguyen Manh Hyung
Minister of Information and Communications
Ministry of Information and Communication (MIC)
18 Nguyen Du Street
Hanoi, Vietnam

Submitted via the MIC's online portal for comments on draft legal documents

1 Sep 2021

Dear Minister,

Re: ACCA Industry Letter to the Vietnam Ministry of Information and Communication (MIC) on the draft amendments to Decree 72 on the Management, Provision and Use of Internet Services and Online Information

The Asia Cloud Computing Association (ACCA) thanks the Ministry of Information and Communication (MIC) for the opportunity to comment on the Draft Amendments to Decree 72. As the apex industry association for Asia Pacific stakeholders in the cloud computing ecosystem, we are very pleased to note that the Government of Vietnam has adopted a consultative approach in its rulemaking. We are also pleased to note that the Vietnamese government has developed and approved an e-government development strategy where Cloud plays an integral role. We are also strongly supportive of Vietnam's goal to grow its digital economy to USD 25B by 2025.

Understanding the importance of the Draft Amendments to Decree 72 and in consultations with our members, we are submitting comments and recommendations in the attached document following this cover letter, highlighting the unintended consequences that would result from these amendments that will negatively affect Cloud adoption and digital transformation in Vietnam.

The ACCA represents a vendor-neutral voice of the private sector to government and other stakeholders. Our mission is to accelerate the adoption of cloud computing through Asia Pacific by helping to create a trusted and compelling market environment, and a safe and consistent regulatory environment for cloud computing products and services. We are committed to strengthening cybersecurity resilience and developing a robust technology ecosystem which supports a vibrant digital economy.

Thank you again for the opportunity to raise these issues, and please do reach out if you would like clarifications on the items we are submitting, or if you would like to arrange a closed-door discussion on these matters.

Best regards,
Lim May-Ann
Executive Director
Asia Cloud Computing Association
mayann@asiacloudcomputing.org

ACCA Industry Letter to the Vietnam Ministry of Information and Communications (MIC) on the Draft Amendments to Decree 72 on the Management, Provision and Use of Internet Services and Online Information

1. We recommend that Article 44h.5 be removed to facilitate the cross-border flow of data needed to grow Vietnam's digital economy.

Article 44h.5 effectively bans data centers from transferring any customer data across borders, and completely conflicts with the broader economic goals of the Vietnamese Government. The free flow of data across borders is crucial for ensuring that Vietnam meets its goal of becoming a USD 52B digital economy by 2025. Vietnam already has existing laws and regulations on cybersecurity and data protection, and this proposed restriction will lead to the following unintended negative consequences:

a) Disruption to business processes and placement of limitations on local and multinational companies operating in Vietnam to service domestic and international customers

Many Vietnamese businesses and startups rely on offshore ICT services to (1) improve cybersecurity, (2) ensure quality control, and (3) access the most innovative services in data analytics, machine learning and Internet of Things. Banning the cross-border flow of customer data will cut off these companies' access to such services, disrupting and destroying their entire business models. The survival of many SMEs and start-ups that are only starting to recover from the impact of COVID-19 on their business will also be threatened.

Multinational companies from all sectors operating in Vietnam will also be affected. Many of these companies rely on ICT service providers for data storage, data processing, and advanced data analytics services to support their customers. Many of these services occur offshore for reasons of cost efficiency. Some of this analytics is also only possible with the benefit of globally aggregated data to provide insights. A ban on cross-border data flow will make all this impossible, ultimately reversing the current upward trend of Foreign Direct Investment (FDI) into Vietnam across all sectors as Vietnam becomes significantly less attractive to investors.

b) Undermine data privacy and security in Vietnam, and slow down digital transformation

The most critical factor in determining data security is not its physical location, but the efficacy of the technical and operational measures and solutions that are implemented to secure the data. By mandating data localization, providers offering cybersecurity-related services are prevented from offering their services in Vietnam because of the higher infrastructure and operating costs required to do so. As a result, data localization will negatively affect the cybersecurity industry in Vietnam, undermining data privacy and security.

Likewise, companies operating in Vietnam will also have reduced access to cybersecurity innovations from other countries, resulting in higher costs, slower innovation, and lower cybersecurity readiness. Local start-ups and traditional brick-and-mortar companies undergoing digital transformation that depend on low-cost Cloud storage and computing

services will be the most affected. Ultimately, this will slow down the rate of digital transformation in Vietnam.

Apart from its negative consequences on Vietnam's economic growth, Article 44h.5 is also impractical to implement. Data center and cloud service providers have a shared responsibility model with their clients, where the client decides where to store or transfer their data/content, and data is not transferred outside the country without the client's decision and consent. In addition, Article 44h.5 also seems to be in conflict with Article 44g which acknowledges the need for cross-border data services.

Given the points above, we recommend that Article 44h.5 be removed from the draft as it would burden and limit local and international businesses operating in Vietnam, and is also impractical to implement. Instead, MIC may consider establishing guidelines to facilitate data transfer in a safe and secure manner, such as by recognizing international data security, privacy and information management standards and certification (e.g., ISO standards).

2. **It is unclear what the inclusion of data center operations and Cloud services (Article 44) into Decree 72 is meant to achieve. We recommend retaining Decree 72's original focus on regulating online content, media and games and excluding Article 44. We also suggest that industry consultation be conducted to discuss measures to address regulatory concerns.**

The existing Decree 72 focuses on regulating online content, media and gaming, and the objective of the amendments in expanding it to cover data centers and Cloud services is unclear. Establishing such a regime would hinder the growth and development of Cloud services in Vietnam by:

a) Creating unnecessary barriers to entry
b) Introducing new regulatory and compliance burden that is possibly counter to regional and international practice
c) Reduce market competition
d) Deter foreign investment and cross-border engagements and transactions

Overall, the draft amendments create significant commercial uncertainty about Vietnam's approach to Cloud adoption and will result in data centers and Cloud Service Providers (CSPs) reconsidering their commercial investments in Vietnam. To avoid this unintended outcome, we propose that industry consultation be conducted to define the key areas of concern that require regulatory intervention or self-regulation and discuss measures to address Vietnam's regulatory concerns. In this way, Vietnam can ensure that concerns are addressed while still promoting the growth and development of data center operations and Cloud services in Vietnam by ensuring alignment with international best practice, promoting a Cloud first policy and Cloud adoption in the public and private sector, and enabling access to domestic and international connectivity under competitive terms.

3. If Article 44 is to be retained, we recommend that it be revised to exclude data center and Cloud service providers to reflect the Shared Responsibility model of Cloud computing and ensure that regulations are placed on the appropriate party.

Fundamentally, Decree 72 was designed and drafted to manage consumer protection and content regulation issues that pertain to B2C business models. It is not suitable to regulate Cloud services which are B2B, where CSPs and their business clients operate on a Shared Responsibility model. With some variation depending on the details of the commercial agreement, CSPs are responsible for providing and maintaining the underlying infrastructure, whereas client businesses are responsible for the use of the infrastructure and the deployment of applications on top of the infrastructure. Hence, if Decree 72 is to be expanded to cover data centers and Cloud services, it should also be amended to ensure that regulations are placed on the appropriate parties. Business clients should be responsible for choosing the services they procure, the integration of those services into their IT environment, deployment of the applications, and for compliance with applicable laws and regulations.

Another result of this shared responsibility model is that the clients are the ones who retain ownership of the data being used and transferred. In fact, CSPs and data center service providers typically do not have the capability to access the client business' data in a human readable format. Hence, requirements for the service providers to proactively detect, report, and prevent illegal activities concerning the use of the data are beyond the capability of CSPs and data center service providers, and should not be imposed on them.

4. We recommend removing or revising draft regulations with extra-territorial applications under Article 22.7, Article 44d, and Article 44.g

Extra-territorial applications of the draft regulations in the amendments is impractical, and enforcement on offshore organizations will be challenging. These requirements create conflicting and overlapping regulatory obligations that make it complicated and costly for cross-border operations, and ultimately detract from the objective of these regulations. We recommend that Vietnam's regulation apply to entities formed or established under the laws of Vietnam to be in line with global best practice and laws on data privacy and electronic transactions.

Article 22.7 should not require organizations and individuals to detect and notify foreign organizations of possible violations. Offshore organizations would often be unable to act on such notifications, especially since they may be unverified, based on a misinterpretation of the law, or be misdirected to organizations that are unable to address their concerns. Instead, such notices should only be directed Ministry of Information and Communication (MIC). Article 44d on the registration of data center businesses and Article 44g on the obligations of data center service providers should likewise only apply to entities formed or established under the laws of Vietnam.

5. **Noting the proposed establishment of the Vietnam National Internet Exchange (VNIX) under Article 11, we recommend that Vietnam open up VNIX services for competition by liberalizing the IX industry and allowing private industry players to operate and manage VNIXs.**

A diversity of independent international gateways is necessary to maintain a healthy internet ecosystem that is able to deliver reliable and high-quality internet access to the people of Vietnam at lower network costs. A study by the United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP)[1] found that opening international gateways to competition will have the following positive impact on the growth of a country's digital economy:

a) Lower cost of international bandwidth – the entrance of new players results in greater pursuit of operational efficiencies by operators
b) Lower cost of retail broadband services – both fixed and mobile services are found to follow the cost reduction of international bandwidth
c) Better quality of service for end-users – competition pushes operators to improve service quality, and the lower cost of international transit allows retail service providers to buy more capacity to increase international bandwidth
d) More content hosted locally – this improves the quality of service for end-users and helps build a healthy hosting and peering economy in-country
e) More dynamic telecommunications sector – more diverse players and offerings for end-users invites more investment and grows demand for broadband and other innovative services.

Hence, we recommend and encourage the MIC to open up VNIX services for competition by allowing private industry players to operate and manage VNIX, and to develop policies to support internet and international gateways in four main areas: (i) interconnection agreements, (ii) co-location at the landing stations, (iii) connection services and (iv) ensuring access to all cables. The recommendations of the International Telecommunication Union (ITU) and Singapore's approach to liberalizing international gateways provide good references.

6. **We recommend that Article 34d be revised to be explicit that its compliance obligations are for video game service providers only.**

The title of Article 34d covers the rights and obligations of businesses providing server rental services, server space leasing, business telecommunications services and internet services. However, the clauses within appear to be specific to service providers working with video game publishers.

CSPs are not able to comply with the provisions included under Article 34d as it requires the CSP to be able to know whether a customer/end-user of the client's business is subject to the laws of Vietnam, is in the business of game publication, or is required to obtain a license. CSPs have no visibility into the content of the data belonging to its business client, which is encrypted and also homogenized with data from other clients. As a result, CSPs are unable to determine which

[1] UNESCAP Information and Communications Technology and Disaster Risk Reduction Division, Working Paper on the Effect of Open International Gateways on the Broadband Connectivity Market, https://www.unescap.org/resources/effect-open-international-gateways-broadband-connectivity-market

regulatory requirements might apply to the client or its end-users, and hence are unable to proactively verify if the customer/end-user has the relevant license. The obligation and responsibility to comply with the laws applicable to its business lies with the client. This is the prevalent understanding within the context of Cloud computing and is typically captured in customer agreements between CSPs and their client businesses.

Given this context, we request for clarity on if and how Article 34d is supposed to apply to data center service providers, and how it will interact with Article 44. As CSPs are unable to meet the requirements set out in Article 34d to proactively detect, react and report to such violations, we recommend that these responsibilities continue to lie with the business entities themselves rather than the CSP that is only providing Cloud services.

7. We recommend the removal of the following text from Article 44c: "discontinue service for organizations and individuals that violate the regulations on information security".

Articles 44c and 44h.2 mandate that telecommunications, internet and data center service providers' contracts must include commitments by the customers to comply with legal provisions to ensure the safety and security of information networks, and to terminate services with customers that violate regulations.

In the case of CSPs, given the diverse and critical operational functions that depend on the Cloud services being provided, the termination or suspension of data center services would likely have an immediate and significant impact on clients' business operations, and is not likely to be an appropriate or commensurate penalty for most, if not all, possible violations. We recommend that government agencies continue to be responsible for enforcing laws and issuing punishments.

Alternatively, the regulation could clarify that a service provider may discontinue services following a legal ruling against a customer for the violation of laws or regulations relating to information security, based on the contractual terms and conditions. It is our view that regulators should not force a service provider to discontinue services merely due to allegations or a subjective opinion, and data center service providers should only be obligated to discontinue service to a client after receiving a court ruling confirming that the client in question has violated the applicable law.

8. We recommend that the response time provided under Article 22.5(b) be increased from 24 hours to 72 hours.

As highlighted in earlier recommendations, under the shared responsibility model, data center service providers and CSPs typically do not have access to the client business' data in a human readable format. As a result, requiring such entities to self-determine whether a complaint concerning a violation of Vietnamese law is legitimate or not could lead to a misinterpretation of the law, thereby harming the businesses and end-users involved. Furthermore, service providers also do not have a direct relationship with the data subject. Hence, our view is that the data owner (i.e., the client) should be the one held responsible for taking the corrective action.

Even if service providers are expected to prevent or remove the content in question, the 24-hour period provided to take action is insufficient. Most CSPs are multinational companies operating in a few different time zones. More time is needed to consult with the client responsible for the

content (who is the data owner) and investigate the issue before deciding on the best course of action that causes the least harm to the data subjects affected. While service providers are familiar with the Acceptable Use Policy and commercial agreements with their clients, more time is needed to evaluate whether a client / end-user has violated Vietnam's regulations and is a complaint is legitimate. More time will also be needed if the service providers are required to provide substantive and useful information and updates.

We recommend that MIC align this requirement with international standards and best practices (e.g., the European Union's GDPR or Singapore's PDPA) to allow companies 72 hours to respond to the request.

9. **We recommend that the requirements under Article 22.6 be further clarified, and should not apply to data center service providers, CSPs, or service providers in general who have no visibility into the content of its clients' data.**

As highlighted in earlier recommendations, data center service providers and CSPs do not have access to the content of their clients' data hosted on their systems in a human readable format, and thus do not have the capability to comply with the obligations under Article 22, including Article 22.6.

Article 22.6(a), which requires entities to report violating data content to the MIC within three hours, is especially unfeasible. Apart from not being able to understand the content of client data, data center service providers and CSPs would also need a lot more time to consult the client who is the data owner, investigate the issue, and then evaluate its legality under Vietnamese regulations.

10. **We would like to confirm that the scope of regulations relating to domain name registration and maintenance services do not extend beyond .vn domain name registrations or services.**

This draft decree contains various new obligations and requirements relating to domain name registration and maintenance services. We would like to confirm that the scope of these regulations does not extend beyond .vn domain name registrations or services.