



September 9, 2022

His Excellency Phạm Minh Chính
Prime Minister
Socialist Republic of Vietnam
No. 1 Hoang Hoa Tham Street, Ba Dinh District, Hanoi

RE: Decree No. 53/2022/ND-CP detailing the implementation of a number of articles of the Law on Cybersecurity (LOCS)

Your Excellency:

On behalf of the membership of our business associations, we offer our warmest greetings and thank you for your commitment to improve business conditions and promote economic and social development in Vietnam.

Our members share your goal of developing a vibrant and competitive digital economy, and we appreciate working with you in that effort. For several years, many foreign investors and business groups in Vietnam have engaged relevant authorities on the Law on Cybersecurity (LOCS). During this time, we have raised concerns that certain aspects of the LOCS will negatively affect company operations in Vietnam and dampen Vietnam's overall investment environment. In this regard, we ask for your consideration of the following concerns on the requirements imposed by Decree No. 53/2022/ND-CP detailing the implementation of a number of articles in the LOCS – particularly on data localization.

The Decree requires “foreign” and “domestic” enterprises – presumably those that are online service providers providing the services listed in Article 26.3 of the LOCS – to store user data within Vietnam's territory and establish a branch or representative office in Vietnam, upon a direction pursuant to Article 26.3.a of the LOCS. These obligations are a significant burden on affected enterprises and may have considerable impact on the investment and business climate in Vietnam. This is especially so given that the wording of certain Articles/Clauses within Decree 53 is ambiguous and creates uncertainty as to what compliance actions are necessary. At the present time, affected enterprises are unable to accurately assess the cost and effort of doing business in Vietnam. We respectfully request that the Government provide

more detailed guidance on the interpretation of the LOCS and Decree 53, particularly in respect of the following areas.

Scope of Application of the Data Localization Requirements

- i. Article 26.3 of LOCS states that only “*domestic and foreign companies, which provide services on telecom networks and on the Internet and other value-added services in cyberspace in Vietnam having the activities of collecting, exploiting, analyzing and processing personal data, data about the relations between the users of the services, and data created by the users in Vietnam*” shall store these data in Vietnam within the time provided by the government. However, Article 26.2 of Decree 53 could be interpreted that all domestic companies must store the data in Vietnam, creating an inconsistency with the above provision of the LOCS. We respectfully request clarification on who is subject of this requirement to ensure the consistency between the law and its implementing decree.

We recommend that the scope of Article 26.2 of Decree 53 be clarified in accordance with Article 26.3 of LOCS and Article 26.3 of Decree 53 to avoid inconsistency between regulations and discrimination between domestic and foreign companies, respectively. Specifically, only the domestic companies, which are stipulated in Article 26.3 of LOCS and fail to cooperate with the public security authorities in relation to breaches pursuant to LOCS be subject to data localization requirements. Such an approach would be consistent with the way in which “foreign enterprise” requirements were identified and applied under Article 26.3 of Decree 53.

- ii. The Enterprise Law does not provide a definition of “domestic enterprises”, but rather defines “Vietnamese enterprises” (Article 2.12). Decree 53 defines “domestic enterprises” similarly as “Vietnamese enterprises”, raising a question on whether a foreign invested companies or branches of foreign companies registered in Vietnam could be interpreted as a “domestic enterprise”. Our organizations would appreciate a confirmation that foreign invested enterprises registered in Vietnam are not covered under Article 26.2 of Decree 53.
- iii. Article 26.2 of Decree 53 stipulates, “domestic enterprises shall store the data specified in clause 1 of this Article in Vietnam.” It is, however, currently unclear whether domestic enterprises are expected to store: (a) a copy of the data locally; or (b) the required data can only be stored in Vietnam. We recommend that the data localization requirement be clarified as “an electronic copy of the required data should be stored in Vietnam.” This would enable “domestic enterprises” to be able to house copies of data both locally and outside of Vietnam, with minimal disruptions to their day-to-day business.

- iv. Article 26.3 requires that foreign companies having operations in certain industries shall locate data in Vietnam and establish representative offices or branches in Vietnam. Please clarify whether the foreign companies - which have already had other forms of presence or establishment in Vietnam such as a foreign invested companies or business partnerships with a Vietnamese company - are still required to establish the representative offices or branches in Vietnam under this Article.
- v. Many foreign companies providing services to their customers in Vietnam store customer related data overseas or use cloud services to store the data. The decision to locate data or establish presence in Vietnam would depend on their size of operation in the country. In this regard, we recommend that the Government consider the size of the company and the scale of its operations within Vietnam when it demands compliance on data storage and establishment of a branch or representative office.
- vi. Article 27 of Decree 53 requires that the covered data shall be stored for at least 24 months from the date of receiving the request for the storage. This requirement may put citizens' privacy, security, and welfare at risk. There is a heightened risk of the occurrence of personal data breaches and the unauthorized processing of personal data. Therefore, a process of consultation with the relevant stakeholder and the data subjects shall be in place to make sure the compliance with this decree will not violate the right to privacy and avoid any personal data breaches and unauthorized processing of personal data.

We recommend reducing the 24-month suggested minimum period to avoid raising the risk of the occurrence of personal data breaches and unauthorized processing of personal data.
- vii. There are various forms of data storage, such as: cloud storage with no sync; cloud storage with timely sync; cloud storage + backup (DR) in Vietnam; and data center (physical server in Vietnam). We seek clarification on (i) which **form of data** needs to be stored in Vietnam; (ii) whether it is possible to **replicate data** in Vietnam to comply with this storage requirement; and (iii) the applicable retention period for local enterprises.

Duration of Data Storage Requirement

- i. Article 27 provides that the duration of the local storage of the data shall start from the date of receiving the request for data localization. We request clarification on whether the data localization is automatically applicable to the covered domestic and foreign enterprises on the effective date of Decree 53, or whether it is only applicable when the enterprises receive the request to store data from the competent authorities. In either

scenario, we also request clarification on whether the provision is applicable to both domestic and foreign companies.

- ii. There are other potential conflicts in regulations that create significant compliance uncertainty for companies and therefore require further clarification. For example, the minimum retention period for user data set out by Decree 53, is 24 months. However, according to regulations of the Law on Network Information Security (LNIS), the owner of personal information has the right to request the deletion of their personal data by the data processor. We seek guidance as to (i) how conflicts between the LNIS and the LOCS/Decree 53 should be resolved; and (ii) whether it will be necessary to obtain any additional approval from the authorized state agencies before complying with a user's lawful request to delete his/her data.

Process of Invoking Requirements for Data Localization and Local Representation

Article 26.3 provides the conditions under which a foreign enterprise can be instructed to localize data and establish a branch or representative office in Vietnam. We request further clarification on the conditions to determine when a foreign enterprise can be deemed to have “failed to comply, incompletely complied, or prevented, obstructed, disabled, or invalidated the effect of cybersecurity protection measures”, and a process for adjudicating the same.

A gradual phase-in for compliance and clarity on implementation details is required for businesses to successfully plan and implement the requirements

We recommend a compliance timeline of 24 months in line with similar regulations in the region. Businesses need adequate time to plan and execute compliance processes associated with the Decree's requirements such as: (i) Technical requirements: Re-build and/or adjust internal technical systems to filter and store requested data; (ii) Operational requirements: Build standards, determine security measures, ensure data accuracy and integrity, and ensure data protection; and (iii) Financial requirements: Investment in local infrastructure, operational costs, other financial planning.

Conclusion

Our organizations are leading voices on digital economy policy, and we place great importance on engagement with the government. We respectfully request written responses or an official dialogue between the government competent authority and the private sector to discuss the issues raised in this letter. We believe that a robust dialogue helps lead to optimal public policy outcomes and are committed to working with Vietnam to support sound policy frameworks that promote data protection, support economic growth, and foster innovation.

We appreciate the opportunity to work with you on the government's goal of developing a vibrant and competitive digital economy in Vietnam. Thank you in advance for your consideration of our requests and recommendations.

Respectfully Yours,



John Goyer
Executive Director, SE Asia
U.S. Chamber of Commerce



Adam R. Sitkoff
Executive Director
AmCham Hanoi



Jeff Paine
Managing Director
Asia Internet Coalition

cc: H.E. General Tô Lâm, Minister of Public Security
H.E. Nguyễn Mạnh Hùng, Minister of Information and Communications
H.E. Nguyen Quoc Dung, Ambassador of Vietnam to the United States
HON Marc E. Knapper, Ambassador of the United States to Vietnam



U.S. Chamber of Commerce



Ngày 9 tháng 9 năm 2022

Kính gửi: Ngài Phạm Minh Chính
Thủ tướng Nước Cộng hòa Xã hội Chủ nghĩa Việt Nam
Số 1 Hoàng Hoa Thám, Quận Ba Đình, Hà Nội

Về việc: Nghị định số 53/2022/NĐ-CP quy định chi tiết về việc thi hành một số điều luật của Luật An ninh mạng

Kính thưa Ngài,

Thay mặt các thành viên của hiệp hội doanh nghiệp, chúng tôi xin gửi tới Ngài lời chào trân trọng cùng lời cảm ơn sâu sắc vì các cam kết trong nỗ lực cải thiện điều kiện kinh doanh nhằm củng cố khu vực kinh tế tư nhân và thúc đẩy phát triển nền kinh tế, xã hội tại Việt Nam.

Chúng tôi bày tỏ sự trân trọng đối với cơ hội được cùng Ngài hiện thực hóa mục tiêu tạo ra một nền kinh tế kỹ thuật số phát triển và cạnh tranh. Đây cũng là mục tiêu chung được chia sẻ bởi các thành viên của chúng tôi. Những năm vừa qua, nhiều nhà đầu tư và doanh nghiệp nước ngoài tại Việt Nam đã làm việc cùng các nhà chức trách có thẩm quyền về vấn đề Luật An ninh mạng. Trong khoảng thời gian đó, chúng tôi đã bày tỏ quan ngại về việc một số khía cạnh của Luật An ninh mạng có khả năng ảnh hưởng tiêu cực đến hoạt động kinh doanh các doanh nghiệp tại Việt Nam cũng như môi trường đầu tư chung của quốc gia. Do đó, chúng tôi kiến nghị Ngài cân nhắc những yêu cầu do Nghị định số 53/2022/NĐ-CP quy định chi tiết thi hành một số điều trong Luật An ninh mạng - đặc biệt là về vấn đề bản địa hóa dữ liệu.

Theo Nghị định, các doanh nghiệp "nước ngoài" và "trong nước" phải lưu trữ dữ liệu người dùng tại lãnh thổ Việt Nam, đồng thời thành lập chi nhánh hoặc văn phòng đại diện tại đây theo yêu cầu quy định tại Điều 26.3.a của Luật An ninh mạng. Các doanh nghiệp đề cập đến ở đây có thể là những doanh nghiệp đang cung cấp các dịch vụ trực tuyến được liệt kê trong Điều 26.3 Luật An ninh mạng. Những yêu cầu này gây ra gánh nặng đáng kể đối với các doanh nghiệp trực tiếp liên quan và có thể ảnh hưởng tiêu cực đến môi trường đầu tư và kinh doanh tại Việt Nam. Đặc biệt, cách diễn đạt của một số Điều/Khoản tại Nghị định 53 còn chưa rõ ràng khiến doanh nghiệp gặp khó khăn trong việc xác định những hành động tuân thủ nào là cần thiết. Tại thời điểm hiện tại, các doanh nghiệp liên quan chưa thể đánh giá chính xác chi phí và nỗ lực cần thiết để hoạt động kinh doanh tại Việt Nam. Do đó, chúng tôi kính đề nghị Chính phủ cung cấp hướng dẫn chi tiết, giải thích Luật An ninh mạng và Nghị định 53, đặc biệt đối với các lĩnh vực sau.

Phạm vi Áp dụng của các Yêu cầu về Lưu trữ Dữ liệu

- i. Điều 26.3 của Luật An ninh mạng quy định rằng chỉ “các doanh nghiệp trong nước và ngoài nước cung cấp dịch vụ trên mạng viễn thông, mạng Internet và các dịch vụ gia tăng trên không gian mạng tại Việt Nam có hoạt động thu thập, khai thác, phân tích, xử lý dữ liệu về thông tin cá nhân, dữ liệu về mối quan hệ của người sử dụng dịch vụ, dữ liệu do người sử dụng dịch vụ tại Việt Nam tạo ra” sẽ phải lưu trữ những dữ liệu này tại Việt Nam trong thời gian theo quy định của Chính phủ. Tuy nhiên, Điều 26.2 của Nghị định 53 có thể được hiểu là tất cả các doanh nghiệp trong nước phải lưu trữ dữ liệu tại Việt Nam, gây ra sự mâu thuẫn với quy định nêu trên của Luật An ninh mạng. Do đó, chúng tôi cho rằng cần làm rõ đối tượng của yêu cầu này để đảm bảo tính thống nhất giữa luật và nghị định.

Chúng tôi kiến nghị làm rõ phạm vi của Điều 26.2 của Nghị định 53 theo Điều 26.3 của Luật An ninh mạng và Điều 26.3 của Nghị định 53 để tránh gây mâu thuẫn giữa các quy định và sự phân biệt đối xử giữa các doanh nghiệp trong nước và nước ngoài. Cụ thể là chỉ các doanh nghiệp trong nước, được quy định tại Điều 26.3 của Luật An ninh mạng và không hợp tác với cơ quan công an liên quan đến các vi phạm Luật An ninh mạng mới phải tuân theo các yêu cầu về lưu trữ dữ liệu. Cách tiếp cận như vậy sẽ thống nhất với các yêu cầu “doanh nghiệp nước ngoài” được xác định và áp dụng theo Điều 26.3 của Nghị định 53.

- ii. Luật Doanh nghiệp không có khái niệm về “doanh nghiệp trong nước” mà chỉ có định nghĩa về “doanh nghiệp Việt Nam” (Điều 2.12). Theo Nghị định 53 “doanh nghiệp trong nước” được định nghĩa tương tự như “doanh nghiệp Việt Nam”. Điều này đặt ra câu hỏi về việc liệu doanh nghiệp có vốn đầu tư nước ngoài hoặc chi nhánh của doanh nghiệp nước ngoài đăng ký tại Việt Nam có thể được hiểu là “doanh nghiệp trong nước” hay không. Chúng tôi kính đề nghị làm rõ các doanh nghiệp có vốn đầu tư nước ngoài hay chi nhánh các công ty nước ngoài đăng ký tại Việt Nam sẽ không thuộc phạm trù khái niệm “doanh nghiệp trong nước” và vì vậy không thuộc phạm vi điều chỉnh của Điều 26.2 Nghị định 53.
- iii. Điều 26.2 Nghị định 53 quy định “các doanh nghiệp trong nước phải lưu trữ dữ liệu quy định tại khoản 1 Điều này tại Việt Nam”. Tuy nhiên, điều này chưa rõ liệu các doanh nghiệp trong nước sẽ cần lưu trữ: (a) bản sao dữ liệu trong nước; hay (b) dữ liệu chỉ được lưu trữ tại Việt Nam. Chúng tôi khuyến nghị rằng yêu cầu lưu trữ dữ liệu cần được làm rõ là “một bản sao điện tử của dữ liệu được yêu cầu cần được lưu trữ tại Việt Nam”. Điều này sẽ cho phép “các doanh nghiệp trong nước” tiếp tục lưu trữ dữ liệu của họ cả trong nước lẫn bên ngoài Việt Nam, để hạn chế tối thiểu sự gián đoạn trong hoạt động kinh doanh hàng ngày của doanh nghiệp.
- iv. Điều 26.3 yêu cầu các doanh nghiệp nước ngoài hoạt động trong một số ngành nhất định phải đặt dữ liệu tại Việt Nam và thành lập văn phòng đại diện hoặc chi nhánh tại Việt Nam. Chúng tôi cho rằng cần làm rõ liệu các doanh nghiệp nước ngoài đã có các hình thức hiện diện khác tại Việt Nam như doanh nghiệp có vốn đầu tư nước ngoài hoặc doanh nghiệp hợp doanh với doanh nghiệp Việt Nam, có cần phải thành lập văn phòng đại diện hoặc chi nhánh tại Việt Nam theo quy định tại Điều này hay không.

- v. Nhiều doanh nghiệp nước ngoài cung cấp dịch vụ cho khách hàng tại Việt Nam đang lưu trữ dữ liệu của họ ở nước ngoài hoặc sử dụng dịch vụ đám mây để lưu trữ dữ liệu. Quyết định lưu trữ dữ liệu hay thành lập chi nhánh của doanh nghiệp tại Việt Nam sẽ phụ thuộc vào quy mô hoạt động của họ tại Việt Nam. Về vấn đề này, chúng tôi khuyến nghị Chính phủ xem xét quy mô và mức độ hoạt động của doanh nghiệp tại Việt Nam khi yêu cầu tuân thủ về lưu trữ dữ liệu và thành lập chi nhánh hoặc văn phòng đại diện.
- vi. Điều 27 của Nghị định 53 yêu cầu dữ liệu phải được lưu trữ ít nhất 24 tháng kể từ ngày nhận được yêu cầu lưu trữ. Yêu cầu này có thể khiến quyền riêng tư, an ninh và quyền lợi của các chủ thể liên quan gặp rủi ro. Nguy cơ xảy ra vi phạm và xử lý trái phép dữ liệu cá nhân là rất cao. Do đó, nên có một quy trình tham vấn các bên liên quan và các chủ thể dữ liệu để đảm bảo việc tuân thủ nghị định này sẽ không vi phạm quyền riêng tư và tránh mọi vi phạm và xử lý trái phép dữ liệu cá nhân.

Chúng tôi khuyến nghị nên giảm thời gian lưu trữ dữ liệu tối thiểu 24 tháng này để tránh làm tăng nguy cơ xảy ra vi phạm và sử dụng trái phép dữ liệu cá nhân.

- vii. Có nhiều hình thức lưu trữ dữ liệu, chẳng hạn như: lưu trữ đám mây không đồng bộ; lưu trữ đám mây đồng bộ theo chu kỳ; lưu trữ đám mây + sao lưu (DR) tại Việt Nam; và thành lập trung tâm dữ liệu (máy chủ vật lý tại Việt Nam). Chúng tôi mong muốn được làm rõ các vấn đề sau: (i) loại hình lưu trữ dữ liệu nào cần được áp dụng ở Việt Nam; (ii) liệu có thể nhân bản dữ liệu tại Việt Nam để tuân thủ yêu cầu lưu trữ này hay không; và (iii) thời hạn lưu trữ áp dụng cho các doanh nghiệp trong nước.

Yêu cầu về Thời lượng Lưu trữ Dữ liệu

- i. Điều 27 quy định rằng thời hạn lưu trữ dữ liệu trong nước cục bộ của dữ liệu sẽ bắt đầu từ ngày nhận được yêu cầu nội địa hóa dữ liệu. Chúng tôi kiến nghị làm rõ việc nội địa hóa dữ liệu có được tự động áp dụng cho các doanh nghiệp trong và ngoài nước kể từ ngày Nghị định 53 có hiệu lực hay chỉ áp dụng khi doanh nghiệp nhận được yêu cầu lưu trữ dữ liệu từ cơ quan có thẩm quyền. Trong cả hai trường hợp, chúng tôi cũng yêu cầu làm rõ liệu điều khoản này có được áp dụng cho cả công ty trong nước và nước ngoài hay không.
- ii. Chúng tôi cho rằng vẫn còn nhiều mâu thuẫn tiềm ẩn khác trong các quy định của pháp luật khiến các doanh nghiệp không chắc chắn về quy trình tuân thủ và do đó cần làm rõ thêm. Ví dụ, Nghị định 53 yêu cầu thời hạn lưu trữ tối thiểu đối với dữ liệu người dùng là 24 tháng. Tuy nhiên, theo quy định của Luật An toàn thông tin mạng, chủ sở hữu thông tin cá nhân có quyền yêu cầu bên xử lý dữ liệu xóa dữ liệu cá nhân của mình. Chúng tôi khuyến nghị có hướng dẫn về (i) cách giải quyết xung đột giữa Luật An toàn thông tin mạng và Luật An ninh mạng/Nghị định 53; và (ii) liệu có cần thêm sự chấp thuận từ các cơ quan nhà nước có thẩm quyền trước khi thực hiện yêu cầu hợp pháp của người dùng về việc xóa dữ liệu của họ hay không.

Quy trình Yêu cầu đối với Lưu trữ dữ liệu và Thành lập Đại diện trong nước

Điều 26.3 qui định các trường hợp doanh nghiệp nước ngoài nhận yêu cầu lưu trữ dữ liệu và/hoặc thành lập chi nhánh hoặc văn phòng đại diện tại Việt Nam. Chúng tôi yêu cầu làm rõ thêm về các tiêu chí để xác định khi nào một doanh nghiệp nước ngoài có thể bị coi là “không tuân thủ, tuân thủ không đầy đủ hoặc ngăn chặn, cản trở, vô hiệu hóa hoặc làm mất tác dụng của các biện pháp bảo vệ an ninh mạng” và quy trình xử lý tương ứng.

Cần có thời gian chuyển tiếp để các doanh nghiệp lên kế hoạch và thực thi các quy định

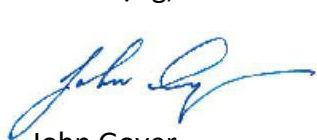
Chúng tôi đề xuất một giai đoạn chuyển tiếp là 24 tháng như các quy định tương tự trong khu vực. Doanh nghiệp cần có đủ thời gian để lên kế hoạch và thực hiện các quy trình tuân thủ liên quan đến các yêu cầu của Nghị định như: (i) Yêu cầu kỹ thuật: Xây dựng lại và/hoặc điều chỉnh hệ thống kỹ thuật nội bộ để lọc và lưu trữ dữ liệu được yêu cầu; (ii) Yêu cầu về hoạt động: Xây dựng tiêu chuẩn, xác định các biện pháp bảo mật, đảm bảo tính chính xác và toàn vẹn của dữ liệu, đồng thời đảm bảo bảo vệ dữ liệu; và (iii) Yêu cầu tài chính: Đầu tư vào cơ sở hạ tầng địa phương, chi phí vận hành, lập các kế hoạch tài chính khác.

Kết luận

Là đại diện tiếng nói hàng đầu về chính sách kinh tế kỹ thuật số, chúng tôi bày tỏ sự trân trọng tới cơ hội được hợp tác với Chính phủ. Chúng tôi rất mong sẽ nhận được phản hồi bằng văn bản hoặc qua cuộc đối thoại chính thức giữa cơ quan có thẩm quyền của Chính phủ với Khu vực tư nhân nhằm thảo luận sâu hơn về các vấn đề được nêu trong thư này. Chúng tôi tin rằng một cuộc đối thoại thẳng thắn sẽ giúp đạt được những chính sách công tối ưu, đồng thời thể hiện cam kết hỗ trợ Việt Nam tạo ra một khuôn khổ chính sách hợp lý giúp thúc đẩy an ninh dữ liệu, hỗ trợ tăng trưởng kinh tế và đẩy mạnh tính đổi mới.

Một lần nữa, chúng tôi xin bày tỏ sự trân trọng với cơ hội được cùng Ngài thực hiện mục tiêu của Chính phủ phát triển một nền kinh tế kỹ thuật số sôi động và giàu tính cạnh tranh ở Việt Nam. Cảm ơn Ngài đã xem xét các yêu cầu và đề xuất của chúng tôi.

Trân trọng,



John Goyer
Giám đốc Điều hành, Đông Nam Á
Phòng Thương mại Hoa Kỳ



Adam R. Sitkoff
Giám đốc Điều hành
Hiệp hội Thương mại Mỹ



Jeff Paine
Giám đốc điều hành
Liên minh Internet Châu Á

Đồng kính gửi:

Ngài Đại tướng Tô Lâm, Bộ trưởng Bộ Công an
Ngài Nguyễn Mạnh Hùng, Bộ trưởng Bộ Thông tin và Truyền thông
Ngài Nguyễn Quốc Dũng, Đại sứ Việt Nam tại Hoa Kỳ
Ngài Marc E. Knapper, Đại sứ Hoa Kỳ tại Việt Nam