Business Software Alliance

Ngày 6 tháng 11 năm 2026

Ý KIẾN ĐÓNG GÓP CỦA BSA ĐỐI VỚI BẢN CẬP NHẬT DỰ THẢO LUẬT AN NINH DỮ LIỆU

Kính gửi: Bộ Công an
Đồng kính gửi: Ủy ban Quốc phòng, An ninh và Đối ngoại của Quốc hội

Liên minh Phần mềm (**BSA**)[1] trân trọng gửi các ý kiến đóng góp dưới đây đối với bản cập nhật Dự thảo Luật An ninh dữ liệu (**Luật ANDL**) ngày 28 tháng 9 năm 2026 đã được trình Quốc hội. BSA là hiệp hội thương mại toàn cầu của ngành công nghiệp phần mềm doanh nghiệp. Các thành viên của chúng tôi là những công ty dẫn đầu trong lĩnh vực trí tuệ nhân tạo (**AI**), an ninh mạng, điện toán đám mây và các công nghệ tiên tiến khác.

BSA đã tích cực tham gia cùng Bộ Công an (**BCA**) trong suốt quá trình xây dựng Luật ANDL, thông qua các ý kiến đóng góp của chúng tôi đối với Hồ sơ chính sách và Dự thảo Luật ANDL vào tháng 7 và tháng 8 năm 2026.[2] Chúng tôi cũng trân trọng các cơ hội được trao đổi quan điểm với Bộ trưởng Lương Tam Quang tại Hà Nội vào tháng 8 năm 2026 và tại cuộc họp của đoàn Phòng Thương mại Hoa Kỳ được tổ chức nhân dịp Tuần lễ An ninh mạng quốc tế Singapore ngày 14 tháng 10 năm 2026, cũng như với Trung tướng Lê Xuân Minh tại buổi Đối thoại Chính sách Số ngày 15 tháng 10 năm 2026.

BSA hoan nghênh những cải thiện trong bản cập nhật Dự thảo, đặc biệt là nỗ lực giảm thiểu sự trùng lặp và áp dụng các yêu cầu tương xứng với cấp độ rủi ro. Trong quá trình Quốc hội xem xét Dự thảo, chúng tôi rất mong những cải thiện này được tích cực phát huy để xây dựng một khuôn khổ thống nhất giữa các quy định pháp luật của Việt Nam về dữ liệu, quyền riêng tư, an ninh mạng và AI, đồng thời bảo đảm trách nhiệm của các bên được phân định rõ ràng và giảm thiểu các yêu cầu tuân thủ chồng chéo.

Những Điểm Tích Cực Trong Bản Cập Nhật Dự Thảo

Các sửa đổi đã giải quyết một số quan ngại được nêu trong quá trình lấy ý kiến công khai, và chúng tôi hoan nghênh việc BCA đã dành thời gian xem xét các vấn đề này.

Bản cập nhật Dự thảo làm rõ mối quan hệ giữa Luật ANDL và các văn bản pháp luật hiện hành. Theo đó, việc bảo vệ dữ liệu cá nhân được tiếp tục thực hiện theo Luật Bảo vệ dữ liệu cá nhân (**Luật BVDLCN**),

---

[1] Các thành viên của BSA gồm: Adobe, Alteryx, Amadeus, Amazon Web Services, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cloudflare, Cohere, Cohesity, Dassault Systemes, Databricks, Datadog, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., TrendAI, TriNet, Veeam, Workday, Zendesk, và Zoom Communications Inc.

[2] Ý kiến đóng góp của BSA về việc xây dựng Luật An ninh dữ liệu ngày 13 tháng 7 năm 2026 tại https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-the-development-of-a-law-on-data-security, và Ý kiến đóng góp của BSA đối với Dự thảo Luật An ninh dữ liệu ngày 05 tháng 8 năm 2026 tại https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-the-draft-law-on-data-security.

hoạt động quản trị và phân loại dữ liệu được thực hiện theo Luật Dữ liệu, và việc bảo vệ an ninh mạng đối với hệ thống thông tin được thực hiện theo Luật An ninh mạng, trong khi Luật ANDL tập trung bảo vệ an ninh đối với bản thân dữ liệu (Khoản 2 Điều 3). Trường hợp các nghĩa vụ có nội dung chồng lấn, dự thảo quy định việc lập một bộ hồ sơ và thực hiện một thủ tục (Khoản 3 Điều 3).

Các sửa đổi đã củng cố cách tiếp cận dựa trên rủi ro. Chủ quản dữ liệu tự xác định cấp độ rủi ro và theo đó thực hiện các nghĩa vụ tương ứng theo từng cấp độ (Khoản 5 Điều 4 và Điều 8). Dữ liệu Cấp độ 1 không phải lập hồ sơ. Đối với dữ liệu Cấp độ 2, chủ quản dữ liệu phải xây dựng phương án bảo vệ an ninh dữ liệu theo mẫu rút gọn, tuy nhiên, hộ kinh doanh, doanh nghiệp siêu nhỏ, doanh nghiệp nhỏ và doanh nghiệp khởi nghiệp sáng tạo được miễn nghĩa vụ này (Khoản 1 đến 3 Điều 10). Dữ liệu được xác định là Dữ liệu Cốt lõi chỉ do đạt ngưỡng về số lượng chủ thể dữ liệu hoặc khối lượng dữ liệu thì được xác định là Cấp độ 3, trừ một số trường hợp luật định (Khoản 3 Điều 8). Chủ quản dữ liệu thực hiện theo văn bản hướng dẫn của cơ quan chuyên trách bảo vệ an ninh dữ liệu không bị xử lý vi phạm do xác định sai cấp độ đối với nội dung đã được hướng dẫn (Khoản 8 Điều 8).

Dự thảo áp dụng cách tiếp cận dựa trên rủi ro đối với việc lưu trữ và chuyển dữ liệu ra nước ngoài (Điều 19):

- dữ liệu Cấp độ 1 và Cấp độ 2 không phải thực hiện thủ tục theo quy định của Luật ANDL;
- đối với dữ liệu Cấp độ 3, chủ quản dữ liệu chỉ phải tự đánh giá an ninh dữ liệu trước khi thực hiện; và
- đối với dữ liệu Cấp độ 4 và Cấp độ 5, văn bản chấp thuận có thể tiếp tục áp dụng cho các hoạt động chuyển dữ liệu lặp lại trong cùng một luồng dữ liệu mà không phải xin chấp thuận mới cho từng lần chuyển, với điều kiện không có thay đổi về mục đích, loại dữ liệu, bên nhận hoặc biện pháp bảo vệ.

Chúng tôi đồng thời ủng hộ các biện pháp bảo vệ mã nguồn và trọng số mô hình trong quá trình thẩm định, kiểm tra (Khoản 7 Điều 11), cơ chế tự nguyện sử dụng mật mã an ninh đối với dữ liệu không thuộc phạm vi bí mật nhà nước (Khoản 3 Điều 16), cũng như việc tiếp tục công nhận hiệu lực của các văn bản chấp thuận và kết quả đánh giá chuyển dữ liệu ra nước ngoài đã có (Khoản 2 Điều 29).

Chúng tôi đánh giá tích cực việc bãi bỏ các mức phạt được tính theo tỷ lệ phần trăm doanh thu và nguyên tắc một hành vi vi phạm đồng thời thuộc phạm vi điều chỉnh của nhiều luật chỉ bị xử phạt một lần (Khoản 12 Điều 26). Các biện pháp hạn chế dịch vụ xuyên biên giới phải tuân thủ các biện pháp bảo đảm về thủ tục và có thời hạn áp dụng không quá 90 ngày (Điều 20).

Hoàn Thiện Quy Định Nhằm Giảm Thiểu Các Nghĩa Vụ Chồng Chéo

Hồ sơ chính sách của Luật ANDL đã xác định tình trạng phân mảnh và chồng chéo pháp luật là một trong những hạn chế lớn nhất trong khuôn khổ quản trị dữ liệu tại Việt Nam. Dự thảo quy định các thủ tục về chuyển, xử lý Dữ liệu Cốt lõi và Dữ liệu Quan trọng xuyên biên giới cũng như việc đánh giá rủi ro theo Luật Dữ liệu được thực hiện theo Luật ANDL (Khoản 2 Điều 27). Dự thảo cũng công nhận kết quả đánh giá, thẩm định, kiểm tra, kiểm toán, chứng nhận đã được thực hiện hợp pháp theo luật khác và còn hiệu lực (Điểm b Khoản 3 Điều 3), đồng thời cho phép một báo cáo sự cố duy nhất đáp ứng nghĩa vụ báo cáo, thông báo cho BCA đối với cùng một sự cố theo Luật An ninh mạng và Luật BVDLCN (Điểm c Khoản 3 Điều 3). Hiệu quả của những sửa đổi này sẽ phụ thuộc vào việc Nghị định 165, Nghị định 356 và các nghị

định quy định chi tiết thi hành Luật An ninh mạng được sửa đổi một cách thống nhất trước khi Luật ANDL có hiệu lực, đồng thời các nội dung còn chồng chéo liên quan đến đánh giá chuỗi cung ứng, ngưỡng quy mô và đánh giá tác động được giải quyết.

Ví dụ, Điểm c Khoản 3 Điều 18 yêu cầu sản phẩm, dịch vụ kết nối, tiếp cận dữ liệu từ Cấp độ 3 trở lên phải được đánh giá, kiểm tra an ninh mạng trước khi kết nối. Đối với phần mềm doanh nghiệp được triển khai cho nhiều khách hàng, quy định này có thể dẫn đến việc cùng một sản phẩm hoặc nền tảng dùng chung phải được đánh giá, kiểm tra nhiều lần, trừ trường hợp các kết quả đánh giá và chứng nhận hiện có được công nhận. Dự thảo cũng áp dụng một số ngưỡng riêng biệt dựa trên quy mô, bao gồm:

- ngưỡng quy mô lớn đối với dữ liệu cá nhân nhạy cảm (Điểm c Khoản 1 Điều 8);
- ngưỡng xác định hoạt động xử lý dữ liệu quy mô lớn (Khoản 1 Điều 14);
- ngưỡng về số lượng chủ thể dữ liệu hoặc khối lượng dữ liệu làm căn cứ xác định dữ liệu là Dữ liệu Cốt lõi theo Quyết định số 20/2025/QĐ-TTg (Khoản 3 Điều 8).

Khuyến nghị: Sửa đổi Nghị định 165 và các văn bản quy định chi tiết thi hành có liên quan để bảo đảm thống nhất với Điều 27 trước khi Luật ANDL có hiệu lực. Công bố tài liệu đối chiếu chính sách để làm rõ những nghĩa vụ hiện hành nào được thay thế, tiếp tục áp dụng hoặc bổ sung; đồng thời thống nhất thời hạn và nội dung báo cáo sự cố trong hệ thống báo cáo thống nhất.

Khuyến nghị: Công nhận các kết quả đánh giá và chứng nhận có liên quan hiện có cho mục đích áp dụng Điểm c Khoản 3 Điều 18, để sản phẩm hoặc nền tảng dùng chung đã được đánh giá một lần không phải đánh giá lại cho từng khách hàng và chỉ phải thực hiện đánh giá bổ sung đối với các rủi ro riêng biệt. Công bố các tiêu chí khả thi để công nhận chứng nhận theo Điểm b Khoản 7 Điều 10. Thống nhất các ngưỡng quy mô và phương pháp tính theo Điểm c Khoản 1 Điều 8, Khoản 3 Điều 8 và Khoản 1 Điều 14 với nhau và với Quyết định số 20/2025/QĐ-TTg, trên cơ sở tham vấn cộng đồng doanh nghiệp. Đối với dữ liệu cá nhân, xác nhận theo Điểm b Khoản 3 Điều 3 và Điểm a Khoản 7 Điều 10 rằng nội dung về an ninh trong hồ sơ bảo vệ dữ liệu cá nhân được công nhận cho mục đích đánh giá tác động an ninh dữ liệu theo Khoản 4 Điều 10, và chỉ yêu cầu bổ sung thông tin đối với các vấn đề về an ninh mà hồ sơ này chưa bao quát.

Các Nghĩa Vụ Cần Tương Xứng Với Rủi Ro Và Phạm Vi Kiểm Soát

Tác động thực tế của phương pháp tiếp cận dựa trên mức độ rủi ro sẽ phụ thuộc vào cách dữ liệu được xác định theo từng cấp độ. Một số loại dữ liệu có thể được xác định là Cấp độ 3 do đạt các ngưỡng về quy mô, chẳng hạn như dữ liệu cá nhân nhạy cảm được xử lý đạt ngưỡng quy mô lớn và dữ liệu được xác định là Dữ liệu Cốt lõi theo Luật Dữ liệu chỉ do đạt ngưỡng về số lượng chủ thể dữ liệu hoặc khối lượng dữ liệu. Dữ liệu Cấp độ 3 phải đáp ứng các yêu cầu về lập danh mục dữ liệu, đánh giá tác động và kiểm toán định kỳ, cũng như kiểm soát quyền truy cập và ghi nhật ký sự kiện an ninh. Điều này đặc biệt có ý nghĩa đối với các nhà cung cấp phần mềm doanh nghiệp phục vụ khách hàng trong lĩnh vực tài chính, y tế và nhân sự, do các dịch vụ thông thường giữa các doanh nghiệp này có thể liên quan đến việc xử lý khối lượng lớn các loại dữ liệu nêu trên. Nếu các tiêu chí được quy định quá rộng, một phần đáng kể hoạt động xử lý dữ liệu thương mại thông thường có thể bị xác định là Cấp độ 3, mặc dù bản thân dữ liệu đó không làm phát sinh rủi ro an ninh ở mức độ cao hơn.

Tương tự, yêu cầu phải dừng kết nối và thu hồi ngay quyền truy cập dữ liệu của bên cung cấp khi phát hiện nguy cơ hoặc sự cố an ninh dữ liệu, kể cả đối với dữ liệu Cấp độ 1 và Cấp độ 2 (Điểm c Khoản 4 và Khoản

5 Điều 18), có thể vô tình cản trở hoạt động ứng phó sự cố và khiến các nhóm an ninh đã được cấp quyền không thể triển khai bản vá, ngăn chặn các cuộc tấn công và khôi phục dịch vụ. Vấn đề này đặc biệt đáng lưu ý đối với các nhà cung cấp dịch vụ điện toán đám mây và phần mềm doanh nghiệp, là các chủ thể vận hành và bảo vệ hạ tầng hoặc ứng dụng mà khách hàng không thể tự quản trị. Luật nên cho phép duy trì quyền truy cập ở mức hạn chế cần thiết để thực hiện các biện pháp ngăn chặn, khắc phục tương xứng đối với kết nối hoặc hoạt động xử lý bị ảnh hưởng.

Chúng tôi ủng hộ cách tiếp cận của Dự thảo khi giao chủ quản dữ liệu trách nhiệm xác định cấp độ rủi ro. Khoản 2 Điều 18 phân định trách nhiệm theo vai trò của từng bên. Theo đó, bên xử lý dữ liệu chịu trách nhiệm đối với các nghĩa vụ, hành vi thuộc phạm vi được giao hoặc do mình trực tiếp thực hiện, trong khi chủ quản dữ liệu vẫn chịu trách nhiệm đối với các nghĩa vụ thuộc phạm vi quản lý và quyết định của mình. Các nhà cung cấp dịch vụ điện toán đám mây và phần mềm doanh nghiệp thường xử lý dữ liệu thay mặt khách hàng, tuy nhiên, họ có thể không có đầy đủ thông tin để xác định nội dung dữ liệu của khách hàng, đồng thời cũng chỉ có quyền kiểm soát hạn chế đối với cách thức khách hàng sử dụng dữ liệu đó. Do Luật ANDL không định nghĩa "chủ quản dữ liệu", các nhà cung cấp này có thể bị coi là chủ quản dữ liệu và phải chịu trách nhiệm phân loại, đánh giá và bảo vệ dữ liệu của khách hàng mà họ không kiểm soát.

Khuyến nghị: Bãi bỏ Khoản 6 Điều 8. Theo Luật Dữ liệu, Dữ liệu Quan trọng và Dữ liệu Cốt lõi là dữ liệu thuộc danh mục do Thủ tướng Chính phủ ban hành. Việc yêu cầu chủ quản dữ liệu tự xác định dữ liệu chưa có tên trong danh mục nhưng đáp ứng tiêu chí Dữ liệu Quan trọng hoặc Dữ liệu Cốt lõi và áp dụng biện pháp bảo vệ tương ứng trong thời gian chờ cập nhật danh mục tạo ra sự thiếu chắc chắn và không phù hợp với cơ chế phân loại theo danh mục cũng như Khoản 2 Điều 8. Thẩm quyền rà soát, cập nhật danh mục (Khoản 7 Điều 8) và xác định lại cấp độ dữ liệu (Khoản 9 Điều 8) của cơ quan có thẩm quyền đã đủ để xử lý các tập dữ liệu nhạy cảm mới phát sinh.

Khuyến nghị: Quy định rõ tại Điều 2 các khái niệm "chủ quản dữ liệu" và "bên xử lý dữ liệu", bảo đảm phù hợp với các định nghĩa hiện hành theo Luật BVDLCN và các khuôn khổ được quốc tế công nhận. Làm rõ rằng chủ thể xử lý dữ liệu thay mặt khách hàng được xác định là bên xử lý dữ liệu, không phải chủ quản dữ liệu. Xác nhận rằng theo Khoản 2 Điều 18, trách nhiệm của bên xử lý dữ liệu chỉ giới hạn trong các nhiệm vụ xử lý dữ liệu và biện pháp kiểm soát kỹ thuật đã thỏa thuận với khách hàng, trong khi chủ quản dữ liệu tiếp tục chịu trách nhiệm về phân loại dữ liệu, đánh giá tác động và quyết định chuyển dữ liệu. Nhà cung cấp dịch vụ điện toán đám mây doanh nghiệp hoặc dịch vụ phần mềm (*Software-as-a-Service - SaaS*) thực hiện xử lý dữ liệu thay mặt và theo chỉ dẫn của khách hàng nên được xác định là bên xử lý dữ liệu, bất kể nhà cung cấp đó quản lý hạ tầng kỹ thuật nào. Trường hợp cùng một dịch vụ điện toán đám mây được cung cấp cho nhiều khách hàng, nhà cung cấp không nên phải tự thực hiện việc phân loại hoặc đánh giá dữ liệu riêng cho từng khách hàng. Các nghĩa vụ này nên thuộc trách nhiệm của khách hàng với tư cách là chủ quản dữ liệu.

Khuyến nghị: Theo Điểm c Khoản 4 và Khoản 5 Điều 18, cần cho phép nhà cung cấp duy trì quyền truy cập có kiểm soát trong phạm vi cần thiết để bảo vệ dịch vụ và thực hiện các hoạt động an ninh đã được xác định cụ thể. Chỉ nên bắt buộc dừng kết nối dịch vụ của nhà cung cấp trên phạm vi rộng hơn khi việc tiếp tục duy trì quyền truy cập gây ra rủi ro không thể chấp nhận được. Việc làm rõ các nội dung này sẽ bảo đảm nhà cung cấp có đủ quyền kiểm soát về mặt vận hành để thực hiện trách nhiệm bảo đảm an ninh của mình, đồng thời vẫn duy trì vai trò giám sát của chủ quản dữ liệu và các biện pháp bảo vệ nhằm ngăn ngừa việc sử dụng sai mục đích.

Hệ thống AI. Khoản 2 Điều 15 áp dụng các nghĩa vụ như nhau đối với mọi tổ chức nghiên cứu, phát triển, cung cấp hoặc triển khai hệ thống AI xử lý dữ liệu từ Cấp độ 3 trở lên. Các nghĩa vụ này bao gồm bảo đảm dữ liệu huấn luyện có nguồn gốc hợp pháp và áp dụng biện pháp kỹ thuật ngăn chặn việc trích xuất dữ liệu huấn luyện từ mô hình. Tuy nhiên, doanh nghiệp triển khai mô hình do bên thứ ba phát triển không thể xác minh cách thức mô hình đó được huấn luyện hoặc thay đổi cách thức mô hình phản hồi các hành vi nhằm trích xuất dữ liệu. Đây là những vấn đề hoàn toàn thuộc phạm vi kiểm soát của nhà phát triển đối với mô hình đó.

Khuyến nghị: Phân định các nghĩa vụ tại Khoản 2 Điều 15 theo vai trò của từng bên. Các nghĩa vụ liên quan đến dữ liệu huấn luyện và thiết kế mô hình nên thuộc trách nhiệm của nhà phát triển mô hình. Bên triển khai nên chịu trách nhiệm về việc cấu hình và sử dụng hệ thống, bao gồm các biện pháp kiểm soát đối với hệ thống AI tự động theo Điểm e Khoản 2 Điều 15. Làm rõ rằng yêu cầu tại Khoản 4 Điều 9 về việc sử dụng dữ liệu đã khử nhận dạng hoặc dữ liệu tổng hợp khi sử dụng dữ liệu từ Cấp độ 3 trở lên để huấn luyện AI không áp dụng đối với khách hàng doanh nghiệp và các nhà cung cấp dịch vụ được khách hàng ủy quyền trong trường hợp tinh chỉnh hoặc cấu hình các tính năng AI trong phạm vi và cho mục đích cụ thể đã được xác định trong hợp đồng.

Chuyển Dữ Liệu Xuyên Biên Giới

Phần mềm doanh nghiệp và dịch vụ điện toán đám mây phụ thuộc vào hạ tầng quốc tế an toàn, bao gồm các hệ thống được phân bổ tại nhiều khu vực địa lý nhằm bảo đảm khả năng dự phòng và khắc phục thảm họa, phát hiện mối đe dọa trên phạm vi toàn cầu và quản lý khóa mã hóa. Bản cập nhật Dự thảo tạo điều kiện cho các hoạt động này khi chỉ yêu cầu chấp thuận trước đối với các hoạt động chuyển dữ liệu có mức độ rủi ro cao nhất.

Khóa mã hóa. Điểm b Khoản 1 Điều 19 quy định việc lưu trữ dữ liệu Cấp độ 3 hoặc Cấp độ 4 ở nước ngoài không được coi là hoạt động chuyển, xử lý dữ liệu xuyên biên giới nếu dữ liệu đã được mã hóa, trong đó khóa giải mã do chủ quản dữ liệu quản lý tại Việt Nam và bên nước ngoài không nắm giữ, không kiểm soát. Việc quy định theo hướng này tạo thuận lợi cho hoạt động chuyển và lưu trữ dữ liệu an toàn trên phạm vi quốc tế và là một điểm tích cực. Tuy nhiên, quy định này không nên được diễn giải thành yêu cầu trên thực tế về việc quản lý khóa tại Việt Nam. Nhiều tổ chức bảo vệ dữ liệu bằng khóa do khách hàng quản lý và được lưu giữ thông qua các dịch vụ quản lý khóa phân tán trên phạm vi toàn cầu. Cách tiếp cận này vừa duy trì quyền kiểm soát của khách hàng đối với khóa mã hóa và qua đó bảo đảm an ninh cho dữ liệu của họ, vừa tăng cường khả năng chống chịu và an ninh của cả khóa và dữ liệu.

Khuyến nghị: Xác nhận rằng Điểm b Khoản 1 Điều 19 chỉ đưa ra một phương án bổ sung chứ không phải là điều kiện để hoạt động chuyển dữ liệu được coi là hợp pháp. Quy định này cần được áp dụng trong mọi trường hợp chủ quản dữ liệu kiểm soát khóa giải mã và nhà cung cấp dịch vụ không nắm giữ khóa, bất kể khóa được lưu giữ ở đâu. Đồng thời, cần bảo đảm khách hàng tiếp tục được lựa chọn cơ chế quản lý khóa an toàn, bao gồm cả việc sử dụng dịch vụ quản lý khóa.

Khuyến nghị: Công nhận các cơ chế chuyển dữ liệu được quốc tế thừa nhận, chẳng hạn như Hệ thống Quy tắc về Quyền riêng tư Xuyên biên giới Toàn cầu (*Global Cross-Border Privacy Rules System*) và Điều khoản Hợp đồng Mẫu ASEAN (*ASEAN Model Contractual Clauses*), là đáp ứng các nội dung tương ứng của hồ sơ tự đánh giá an ninh dữ liệu đối với dữ liệu Cấp độ 3 và là bằng chứng về việc áp dụng các biện pháp bảo vệ đầy đủ trong quá trình thẩm định đối với dữ liệu Cấp độ 4 và Cấp độ 5. Các yêu cầu bổ sung

chỉ nên giới hạn ở những rủi ro an ninh còn lại mà các cơ chế này chưa xử lý, chẳng hạn như yêu cầu về mã hóa và kiểm soát quyền truy cập đối với dữ liệu được chuyển.

Thi Hành

Phần lớn tác động thực tế của Luật ANDL sẽ phụ thuộc vào các nghị định và văn bản hướng dẫn thi hành, bao gồm các tiêu chí xác định cấp độ rủi ro và quy định chi tiết về các ngưỡng quy mô. Một số nghĩa vụ phải được hoàn thành trong thời hạn 12 tháng kể từ ngày Luật có hiệu lực thi hành (Điều 29). Theo đó, các hệ thống đang vận hành xử lý dữ liệu Cấp độ 4 và Cấp độ 5 phải hoàn thành lần kiểm toán an ninh dữ liệu đầu tiên và tổ chức hoạt động giám sát; chủ quản dữ liệu Cấp độ 2 phải hoàn thành việc lập phương án bảo vệ an ninh dữ liệu. Tuy nhiên, các thời hạn này có thể đến hạn trước khi các nghị định và biểu mẫu có liên quan được ban hành.

Khuyến nghị: Tổ chức lấy ý kiến công khai trong thời gian tối thiểu 60 ngày đối với các nghị định và văn bản hướng dẫn thi hành, đồng thời ban hành các văn bản này trong khoảng thời gian hợp lý trước khi Luật ANDL có hiệu lực. Các thời hạn chuyển tiếp theo Điều 29 nên được tính từ ngày ban hành các nghị định và văn bản hướng dẫn có liên quan thay vì từ ngày Luật có hiệu lực thi hành.

Kết luận

Chúng tôi xin cảm ơn BCA và Ủy ban đã xem xét các ý kiến đóng góp của chúng tôi đối với Luật ANDL và hy vọng Quý Cơ quan sẽ cân nhắc các khuyến nghị nêu trên. Chúng tôi mong muốn tiếp tục hợp tác tích cực với BCA trong quá trình xây dựng các văn bản quy định chi tiết và hướng dẫn thi hành Luật ANDL. BSA sẵn sàng tiếp tục hỗ trợ BCA thông qua việc đóng góp ý kiến chính sách, chia sẻ quan điểm toàn cầu và các thông lệ quốc tế tốt nhất trong lĩnh vực phần mềm doanh nghiệp. Nếu Quý Cơ quan cần thêm thông tin hoặc làm rõ bất kỳ nội dung nào, xin vui lòng liên hệ với chúng tôi. Một lần nữa, chúng tôi xin trân trọng cảm ơn Quý Cơ quan đã dành thời gian và quan tâm xem xét.

Trân trọng,

Wong Wai San
Giám đốc, Chính sách – Châu Á - Thái Bình Dương