



GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

Ý KIẾN PHẢN HỒI GỬI BỘ CÔNG AN LẤY Ý KIẾN VỀ LUẬT AN NINH DỮ LIỆU

Ngày 05 tháng 8 năm 2026

Liên minh Dữ liệu Toàn cầu (**GDA**)¹ trân trọng cảm ơn Bộ Công an đã tạo cơ hội để chúng tôi đóng góp ý kiến đối với Hồ Sơ Chính Sách của dự án Luật An ninh dữ liệu.

GDA là một liên minh đa ngành gồm các công ty có trụ sở tại nhiều khu vực khác nhau trên thế giới, cam kết tuân thủ các tiêu chuẩn cao về quyền riêng tư và an ninh dữ liệu. GDA ủng hộ các chính sách giúp tăng cường niềm tin vào nền kinh tế số mà không áp đặt các hạn chế không hợp lý đối với hoạt động chuyển dữ liệu xuyên biên giới hoặc yêu cầu địa phương hoá dữ liệu, những yếu tố có thể làm suy yếu an ninh dữ liệu, đổi mới sáng tạo, phát triển kinh tế và thương mại quốc tế. Với trọng tâm hoạt động của GDA là các vấn đề liên quan đến dữ liệu xuyên biên giới, chúng tôi xin tập trung góp ý đối với các nội dung của Hồ Sơ Chính Sách liên quan đến chuyển dữ liệu xuyên biên giới.

Trong những năm vừa qua, GDA đã nhiều lần tham gia đóng góp ý kiến về các đề xuất của Việt Nam liên quan đến yêu cầu địa phương hoá dữ liệu hoặc hạn chế chuyển dữ liệu, bao gồm các ý kiến liên quan đến Hồ sơ về Luật An ninh dữ liệu, Luật Dữ liệu, Luật An ninh mạng và Luật Bảo vệ dữ liệu cá nhân. Các ý kiến này có thể được tham khảo tại đây.²

Các công ty thành viên GDA là những nhà đầu tư quan trọng tại Việt Nam, đã đầu tư hàng triệu đô la và hỗ trợ hàng nghìn việc làm. Chuyển dữ liệu cho phép cung cấp các công cụ số và thông tin chuyên sâu quan trọng để hỗ trợ các doanh nhân và công ty thuộc mọi quy mô, ở mọi quốc gia, tạo ra các loại việc làm mới, nâng cao hiệu quả, cải thiện chất lượng và gia tăng sản lượng.

Thời Hạn và Quy Trình Lấy Ý Kiến

Luật An ninh dữ liệu có mối liên hệ chặt chẽ với nhiều văn bản pháp luật hiện hành, ví dụ như Luật Dữ liệu, Luật Bảo vệ dữ liệu cá nhân (**LBVDLCN**), Luật An ninh mạng, Luật Trí tuệ nhân tạo (**AI**) và những văn bản hướng dẫn thi hành. Một trong những mục đích của Luật An ninh dữ liệu là để lấp đầy khoảng trống pháp lý và hoàn thiện khuôn khổ pháp luật về quản trị dữ liệu tại Việt Nam. Để đánh giá liệu Dự thảo Luật An ninh dữ liệu có đạt được mục tiêu này hay không đòi hỏi phải rà soát, đối chiếu một cách toàn diện với các quy định pháp luật hiện hành; tuy nhiên, thời gian lấy ý kiến hiện nay không đủ để thực hiện đầy đủ việc rà soát này. Do đó, các ý kiến trong văn bản này chỉ tập trung vào những vấn đề cấp thiết và dễ nhận thấy nhất. Các ý kiến này không mang tính chất đầy đủ, toàn diện và có thể sẽ còn phát sinh thêm những vấn đề khác trong thời gian tới.

Do đó, chúng tôi trân trọng đề nghị Bộ Công an chưa tiếp tục trình thông qua Dự thảo Luật An ninh dữ liệu theo lộ trình hiện nay và với nội dung như hiện tại. Một văn bản pháp luật được xây dựng với mục tiêu khắc phục tình trạng chồng chéo, phân mảnh và lấp đầy khoảng trống trong khuôn khổ pháp luật về dữ liệu chỉ có thể đạt được mục tiêu đó khi các nội dung trùng lặp, chồng chéo và khoảng trống của hệ thống pháp luật hiện hành được rà soát, xác định một cách toàn diện và có hệ thống; tuy nhiên, công việc này hiện vẫn chưa được thực hiện. Việc áp dụng Luật An ninh mạng 2025 hiện vẫn còn nhiều điểm chưa rõ ràng, một phần là do thiếu đi các văn bản hướng dẫn chi tiết, và điều này đã gây ra các khoảng trống trong quá trình thi hành và làm gián đoạn hoạt động

¹ Để biết thêm thông tin về Liên minh Dữ liệu Toàn cầu, vui lòng truy cập www.globaldataalliance.org

² Xem Liên minh Dữ liệu Toàn cầu, Góp ý của GDA cho Chính phủ Việt Nam (2020 – 2025) tại: https://globaldataalliance.org/resources-results/?pub_type=resource-filings&location=loc-vietnam§or=&language=&posts_filtered=1

kinh doanh. Việc tiếp tục thúc đẩy dự luật trước khi hoàn thành quá trình rà soát nêu trên có nguy cơ làm gia tăng chính tình trạng phân mảnh mà Luật An ninh dữ liệu được kỳ vọng sẽ có thể khắc phục. Theo nội dung của bản dự thảo hiện nay, Luật An ninh dữ liệu chưa thực sự đạt được mục tiêu được nêu trong Hồ sơ chính sách là bảo đảm tính thống nhất, đồng bộ của hệ thống quy định pháp luật về dữ liệu. Thay vào đó, dự thảo chủ yếu quy định nguyên tắc ưu tiên áp dụng Luật này trong trường hợp có mâu thuẫn với các quy định pháp luật hiện hành (Khoản 2 Điều 58). Điều này đồng nghĩa với việc doanh nghiệp vẫn phải tuân thủ đồng thời nhiều văn bản pháp luật cùng điều chỉnh hoạt động dữ liệu và tiếp tục thực hiện các nghĩa vụ tuân thủ như hiện tại, bao gồm cả những nghĩa vụ có nội dung trùng lặp hoặc chồng chéo, trừ trường hợp có sự mâu thuẫn trực tiếp với Luật An ninh dữ liệu.

Trong phạm vi của Luật An ninh dữ liệu, Luật Dữ liệu, LBVDLCN, Luật An ninh mạng và Luật Trí tuệ nhân tạo, các tổ chức phải tuân thủ những nghĩa vụ có phạm vi chồng lấn, nhưng lại được soạn thảo với các ngưỡng áp dụng, thời hạn thực hiện và đối tượng chịu trách nhiệm khác nhau tùy theo từng loại dữ liệu. Các ngưỡng phân loại dựa trên quy mô dữ liệu tại các Khoản 2 và 3 Điều 6 của Luật An ninh dữ liệu không tương thích với các ngưỡng đánh giá dựa trên rủi ro theo Nghị định 356 của Luật Bảo vệ dữ liệu cá nhân. Đồng thời, yêu cầu báo cáo hằng năm đối với hoạt động chuyển dữ liệu xuyên biên giới theo Khoản 4 Điều 32 của Luật An ninh dữ liệu lại không thống nhất với cơ chế báo cáo chỉ thực hiện một lần trong suốt thời gian hoạt động theo Nghị định 165 và Nghị định 356. Ngoài ra, các nghĩa vụ liên quan đến dữ liệu đào tạo tại Điểm a Khoản 1 Điều 26 của Luật An ninh dữ liệu được áp dụng cho một nhóm chủ thể khác với các nghĩa vụ tương đương theo Luật Trí tuệ nhân tạo; và thẩm quyền đình chỉ sau khi đã chấp thuận theo Khoản 2 Điều 32 của Luật An ninh dữ liệu được thực hiện độc lập, không dẫn chiếu hoặc liên hệ với các thủ tục khắc phục hành vi vi phạm hành chính theo Luật An ninh mạng. Mặc dù Khoản 2 Điều 58 quy định rằng Luật An ninh dữ liệu được ưu tiên áp dụng trong trường hợp có sự mâu thuẫn, điều này không đồng thời giải quyết việc chồng lấn, không nhất quán giữa các định nghĩa cũng như các ngưỡng áp dụng không đồng bộ giữa các văn bản quy phạm pháp luật.

Khuyến nghị: Đề nghị chưa tiếp tục trình Dự thảo Luật An ninh dữ liệu sang giai đoạn tiếp theo cho đến khi hoàn thành việc rà soát, đánh giá một cách có hệ thống các nội dung trùng lặp, chồng chéo và khoảng trống trong khuôn khổ pháp luật hiện hành về dữ liệu trên cơ sở đã tham vấn cộng đồng doanh nghiệp. Đồng thời, đề nghị kéo dài thời gian lấy ý kiến đối với dự thảo lên tối thiểu 60 ngày và tổ chức thêm các đợt lấy ý kiến trước khi dự thảo được trình sang giai đoạn tiếp theo, bao gồm các hội thảo chuyên đề mang tính kỹ thuật với sự tham gia của cộng đồng doanh nghiệp. Để bảo đảm việc lấy ý kiến được hiệu quả, chúng tôi đề nghị Bộ Công an công bố tài liệu đối chiếu, làm rõ mối quan hệ giữa từng quy định của Dự thảo Luật An ninh dữ liệu với Luật Dữ liệu, Luật Bảo vệ dữ liệu cá nhân, Luật An ninh mạng, Luật Trí tuệ nhân tạo và các văn bản quy định chi tiết nội dung thi hành tương ứng. Việc rà soát, đối chiếu cần chỉ rõ những quy định có ngưỡng tuân thủ không đồng nhất giữa các văn bản pháp luật, đồng thời xác định các trường hợp mà sự khác biệt trong cách định nghĩa vai trò và trách nhiệm của các chủ thể dẫn đến các nghĩa vụ chồng chéo và/hoặc xung đột. Chúng tôi cũng đề nghị Bộ Công an tiếp tục tạo điều kiện để các cơ quan, tổ chức, doanh nghiệp và các bên liên quan tham gia góp ý đối với các dự thảo văn bản quy định chi tiết và hướng dẫn thi hành Luật, là các văn bản sẽ cụ thể hóa và triển khai các quy định của Luật An ninh dữ liệu trên thực tế.

Phân định Vai trò và Trách nhiệm của các bên

Mặc dù tại Khoản 10 Điều 3 đang dẫn chiếu đến các định nghĩa của bên kiểm soát dữ liệu cá nhân và bên xử lý dữ liệu cá nhân theo LBVDLCN và Luật Dữ liệu, các nghĩa vụ xuyên suốt trong Luật An ninh dữ liệu được áp dụng đối với “chủ quản hệ thống thông tin” hoặc “cơ quan, tổ chức vận hành hệ thống thông tin lưu trữ, xử lý dữ liệu” (ví dụ Khoản 3 Điều 6, Khoản 1 Điều 10, Khoản 2 Điều 20, Khoản 3 Điều 21, Khoản 2 Điều 35 và Điều 55). Theo đó, các nghĩa vụ như phân loại dữ liệu, đánh giá rủi ro, lưu giữ nhật ký hệ thống và giám sát kết nối được giao cho chủ thể vận hành hạ tầng công nghệ, trong khi đó trong mô hình điện toán của doanh nghiệp, chủ thể này thường là bên xử lý dữ liệu. Các bên xử lý dữ liệu này thường là nhà cung cấp dịch vụ điện toán đám mây hoặc phần mềm, không có khả năng tiếp cận, nhận biết hoặc kiểm soát dữ liệu khách hàng được xử lý trên hệ thống của mình. Bên kiểm soát dữ liệu, là chủ thể quyết định mục đích và phương thức xử lý dữ liệu, đồng thời là bên có đầy đủ thông tin và điều kiện thuận lợi nhất để thực hiện nghĩa vụ phân loại dữ liệu và đánh giá rủi ro, phải

thực hiện các quy định này theo LBVDLCN. Tuy nhiên, chủ thể này lại có thể không phải chịu các nghĩa vụ tương ứng theo Luật An ninh dữ liệu. Kết quả là, với cùng một loại dữ liệu nhưng lại tồn tại đồng thời nhiều nghĩa vụ theo hai văn bản pháp luật mà áp dụng điều chỉnh đối với hai đối tượng thực hiện khác nhau, dẫn đến việc một số nghĩa vụ được áp dụng với bên vận hành hệ thống mặc dù trên thực tế đối tượng này không có khả năng thực hiện một cách hiệu quả và có thể làm trùng lặp, chồng chéo hoặc mâu thuẫn với việc phân định trách nhiệm mà đã được quy định tại LBVDLCN.

Khuyến nghị: Thống nhất việc phân định vai trò và trách nhiệm trong Luật An ninh dữ liệu phù hợp với khuôn khổ của bên kiểm soát dữ liệu và bên xử lý dữ liệu theo LBVDLCN và Luật Dữ liệu. Các nghĩa vụ phụ thuộc vào mức độ hiểu biết đối với dữ liệu và mục đích của việc xử lý, bao gồm việc phân loại dữ liệu, đánh giá rủi ro và quyết định chuyển dữ liệu, nên được giao cho bên kiểm soát dữ liệu, trong khi đó, bên xử lý dữ liệu nên có trách nhiệm đối với việc thiết lập các biện pháp kỹ thuật nằm trong phạm vi kiểm soát thực của mình, phù hợp với mô hình phân chia trách nhiệm đang được áp dụng trong các dịch vụ điện toán đám mây dành cho doanh nghiệp. Mỗi nghĩa vụ tại Luật An ninh dữ liệu nên được rà soát để làm rõ chủ thể phù hợp nhất nào có khả năng thực hiện nghĩa vụ đó, nhằm bảo đảm rằng đối với cùng một loại dữ liệu không tồn tại các nghĩa vụ trùng lặp, chồng chéo hoặc mâu thuẫn cho nhiều đối tượng thực hiện theo các văn bản quy phạm pháp luật khác nhau.

Phân Loại Dữ Liệu

Điều 6 phân loại dữ liệu theo 04 cấp độ: Dữ liệu Thông thường (Cấp độ 1), Dữ liệu Nội bộ (Cấp độ 2), Dữ liệu Quan trọng (Cấp độ 3) và Dữ liệu Cốt lõi (Cấp độ 4). Khoản 4 Điều 6 xác định nhóm Dữ liệu Cốt lõi và Dữ liệu Quan trọng có tác động trực tiếp, tức thời đến quốc phòng, an ninh, an toàn xã hội, tài chính - ngân hàng, năng lượng, viễn thông, điều hành khẩn cấp là đối tượng phải thực hiện nghĩa vụ lưu trữ nội địa nghiêm ngặt, cấm không được chuyển giao ra ngoài Việt Nam. Tuy nhiên, việc quy định theo hướng bao quát tất cả dữ liệu có khả năng tác động đến các lĩnh vực tài chính, ngân hàng, năng lượng và viễn thông là chưa phù hợp, bởi cách tiếp cận này có nguy cơ xếp cả những dữ liệu kinh doanh hoặc dữ liệu vận hành thông thường của các lĩnh vực này vào nhóm Dữ liệu Cốt lõi hoặc Dữ liệu Quan trọng, bất kể dữ liệu đó có thực sự ảnh hưởng đến quốc phòng hoặc an ninh quốc gia hay không. Khoản 2 và Khoản 3 Điều 6 còn quy định dữ liệu thuộc cấp độ thấp hơn khi tích tụ đạt ngưỡng quy mô lớn, làm thay đổi bản chất rủi ro tác động thì được áp dụng cấp độ bảo vệ cao hơn tương ứng. Đồng thời, tổ chức vận hành hệ thống thông tin lưu trữ, xử lý dữ liệu phải thiết lập hệ thống công nghệ tự động giám sát, phát hiện và cảnh báo khi tổng quy mô tích tụ dữ liệu đạt hoặc vượt ngưỡng quy định. Thêm vào đó, các nghĩa vụ liên quan đến phân loại dữ liệu, kiểm kê dữ liệu, lập bản đồ dữ liệu và đánh giá rủi ro quy định từ Điều 10 đến Điều 21 được áp dụng đối với cả bốn cấp độ dữ liệu. Điều này đặt ra các yêu cầu tuân thủ cơ bản đối với mọi tổ chức, kể cả đối với dữ liệu có mức độ rủi ro thấp, trong khi các nghĩa vụ này có thể không tương ứng với mức độ rủi ro thực tế của dữ liệu được xử lý.

Khoản 1 và 2 của Điều 24 yêu cầu dữ liệu vận hành các hạ tầng kỹ thuật thuộc các lĩnh vực quốc gia trọng yếu – Tài chính – Ngân hàng, Năng lượng, Y tế, Giáo dục, Viễn thông, Giao thông vận tải bắt buộc phải được phân loại và áp dụng các biện pháp bảo vệ ở mức độ tối thiểu là dữ liệu Quan trọng (Cấp độ 3) hoặc dữ liệu Cốt lõi (Cấp độ 4) cho mọi hệ thống thông tin của các lĩnh vực này, khi kết nối hoặc liên thông đều phải tích hợp giải pháp kỹ thuật giám sát kết nối theo thời gian thực với hệ thống giám sát an ninh dữ liệu tập trung của Bộ Công an. Khoản 2 Điều 35 yêu cầu chủ quản của Dữ liệu Quan trọng phải thực hiện kết nối kỹ thuật, chia sẻ thông tin cảnh báo an ninh về hệ thống này. Điều này dẫn đến việc sẽ có rất nhiều loại dữ liệu thương mại và vận hành thông thường sẽ phải chịu nghĩa vụ giám sát chặt chẽ nhất, đồng thời phải duy trì kết nối giám sát kỹ thuật chỉ vì lĩnh vực hoạt động của khách hàng thay vì dựa trên mức độ nhạy cảm của dữ liệu.

Như đã nêu trong các văn bản góp ý trước đây của chúng tôi, các quy định này sẽ tác động đến một khối lượng lớn dữ liệu do khu vực tư nhân nắm giữ, đồng thời tạo ra các điểm nghẽn trong quá trình chuyển giao và khai thác dữ liệu. Điều này có thể làm chậm hoạt động thương mại, làm suy giảm hiệu quả bảo đảm an ninh dữ liệu và cản trở quá trình đổi mới sáng tạo một cách đáng kể. Việt Nam đã ban hành Luật Dữ liệu, theo đó dữ liệu được phân thành ba nhóm gồm Dữ liệu Cốt lõi, Dữ liệu Quan trọng và dữ liệu khác. Do đó, Dự thảo Luật An ninh dữ liệu cần

làm rõ mối quan hệ giữa các nhóm dữ liệu theo Luật Dữ liệu và hệ thống phân loại dữ liệu theo bốn cấp độ được quy định tại Dự thảo Luật An ninh dữ liệu.

Khuyến nghị: Luật An ninh dữ liệu cần áp dụng cách tiếp cận phân loại dữ liệu theo hướng chặt chẽ và dựa trên mức độ rủi ro, nhằm tránh tình trạng phân loại quá rộng và gây ra những hạn chế không mong muốn đối với hoạt động kinh tế. Dữ liệu Quan trọng (Cấp độ 3) và Dữ liệu Cốt lõi (Cấp độ 4) cần được xác định rõ ràng, có sự dẫn chiếu đến Luật Dữ liệu và chủ yếu giới hạn đối với nhóm dữ liệu thuộc sở hữu hoặc chịu sự kiểm soát của Nhà nước, có tác động trực tiếp đến quốc phòng, an ninh, an toàn xã hội hoặc trong hoạt động của các hạ tầng trọng yếu thực sự mang tính quốc gia. Các cấp độ này không nên mặc nhiên bao gồm các loại dữ liệu được khu vực tư nhân nắm giữ rộng rãi, chẳng hạn như dữ liệu tài chính, giao thông vận tải hoặc dữ liệu y tế, cũng như không nên được xác định là Dữ liệu Quan trọng hoặc Dữ liệu Cốt lõi chỉ dựa trên lĩnh vực hoạt động hoặc quy mô của nhóm dữ liệu này. Việc phân loại trên diện rộng bao gồm toàn bộ các ngành, lĩnh vực hoặc các loại dữ liệu thông thường thuộc nhóm thương mại, vận hành hoặc dữ liệu khách hàng là Dữ liệu Quan trọng (Cấp độ 3) hoặc Dữ liệu Cốt lõi (Cấp độ 4) sẽ làm hạn chế sự phát triển của nền kinh tế số một cách không cần thiết, tạo ra chính những điểm nghẽn về dữ liệu mà Hồ sơ chính sách của Dự thảo Luật An ninh dữ liệu đang hướng tới khắc phục, cũng như gây ra sự gián đoạn đáng kể đối với hoạt động kinh doanh đang diễn ra. Những lĩnh vực được liệt kê xuyên suốt Khoản 4 Điều 6, Khoản 2 Điều 16, Khoản 1 Điều 24 và Khoản 1 Điều 28 nên được loại bỏ hoàn toàn. Trường hợp vẫn được giữ lại, các danh mục này chỉ nên giới hạn ở những ngành nghề, lĩnh vực có mối liên hệ trực tiếp với mục tiêu thiết yếu đối với an ninh quốc gia.

Khuyến nghị: Bãi bỏ cơ chế cộng gộp dữ liệu theo quy mô quy định tại Khoản 2 và Khoản 3 Điều 6. Trường hợp vẫn duy trì cơ chế này, cần xây dựng các ngưỡng định lượng trên cơ sở tham vấn, được công bố trước và được xác định ở mức không bao gồm các hoạt động xử lý dữ liệu trong bối cảnh thương mại thông thường. Cụ thể, các ngưỡng áp dụng đối với các nhóm dữ liệu ở cấp độ thấp hơn, chẳng hạn như Dữ liệu Thông thường và Dữ liệu Nội bộ, cần được điều chỉnh phù hợp nhằm tránh việc các doanh nghiệp bị áp đặt nghĩa vụ quá mức chỉ vì xử lý khối lượng lớn dữ liệu này trong quá trình hoạt động kinh doanh thông thường; yếu tố dựa trên quy mô dữ liệu làm tiêu chí xác định nghĩa vụ tuân thủ là không phù hợp để đánh giá rủi ro về an ninh trong trường hợp bản thân dữ liệu đó đã được xếp vào nhóm có mức độ tác động thấp. Tương tự, sửa đổi Khoản 4 Điều 6 để loại bỏ các tham chiếu rộng đến các ngành nghề cụ thể, ví dụ như tài chính ngân hàng, năng lượng và viễn thông. Thêm vào đó, yêu cầu triển khai hệ thống giám sát tự động để theo dõi việc vượt ngưỡng quy mô dữ liệu không nên áp dụng đối với các hệ thống thuộc khu vực tư nhân chỉ xử lý Dữ liệu Thông thường (Cấp độ 1) hoặc Dữ liệu Nội bộ (Cấp độ 2). Ngoài ra, do Nghị định 165 hướng dẫn thi hành Luật Dữ liệu đã quy định hoạt động chuyển dữ liệu xuyên biên giới theo cơ chế dựa trên quy mô dữ liệu nên cần được rà soát thay vì tiếp tục áp dụng một cách chồng chéo.

Khuyến nghị: Khoản 1 Điều 24 chỉ nên áp dụng đối với dữ liệu vận hành các hạ tầng kỹ thuật do các đơn vị được chỉ định quản lý, thay vì áp dụng cho toàn bộ một ngành nghề, lĩnh vực. Đồng thời, quy định này cần loại trừ một cách rõ ràng dữ liệu dịch vụ thương mại và dữ liệu khách hàng được các nhà cung cấp giải pháp công nghệ xử lý thay mặt cho các tổ chức thuộc những ngành nghề, lĩnh vực đó. Trường hợp vẫn duy trì cơ chế giám sát tự động đối với việc vượt ngưỡng phân loại dữ liệu theo các Khoản 2 Điều 24, Điều 35 và Điều 38, nghĩa vụ kết nối với hệ thống giám sát an ninh dữ liệu tập trung của Bộ Công an và nghĩa vụ chia sẻ thông tin chỉ nên giới hạn ở dữ liệu cảnh báo tổng hợp (aggregated alert metadata) hoặc dữ liệu nhật ký hệ thống (system-log telemetry), thay vì nội dung dữ liệu thô, cùng với các biện pháp bảo đảm cụ thể nhằm ngăn chặn việc cơ quan nhà nước tiếp cận dữ liệu cá nhân hoặc bí mật kinh doanh. Các quy định này cũng không nên tạo ra quyền tiếp cận hoặc khả năng tiếp cận đối với các hệ thống hạ tầng dùng chung để phục vụ khách hàng tại các quốc gia khác. Đối với các nền tảng dùng chung cho nhiều khách hàng (multi-tenant platforms), các nhà cung cấp dịch vụ nên được phép thực hiện nghĩa vụ kết nối và chia sẻ thông tin thông qua giao diện hoặc cơ chế tích hợp do khách hàng tại Việt Nam vận hành, thay vì phải kết nối trực tiếp giữa hạ tầng dùng chung của nhà cung cấp với hệ thống giám sát an ninh dữ liệu tập trung của Bộ Công an.

Lưu Trữ Dữ Liệu và Hạn Chế Đối Với Hoạt Động Chuyển Dữ Liệu Xuyên Biên Giới

Khoản 1 Điều 28 quy định Dữ liệu Cốt lõi và Dữ liệu Quan trọng trong các ngành, lĩnh vực được liệt kê phải được lưu trữ tại trung tâm dữ liệu đặt trên lãnh thổ nước Cộng hòa xã hội chủ nghĩa Việt Nam, đồng thời chỉ cho phép sử dụng dịch vụ điện toán đám mây quốc tế khi có thể duy trì liên tục bản sao lưu cập nhật theo thời gian thực tại Việt Nam dưới sự “kiểm soát tối cao” thuộc về cơ quan nhà nước có thẩm quyền của Việt Nam. Khoản 3 và Khoản 4 Điều 28 quy định doanh nghiệp nước ngoài có hành vi vi phạm pháp luật về an ninh dữ liệu hoặc bảo vệ dữ liệu cá nhân của Việt Nam phải thiết lập hạ tầng, lưu trữ dữ liệu tại Việt Nam, đồng thời đối với bất kỳ vi phạm nào có thể bị áp dụng biện pháp kỹ thuật ngăn chặn như giới hạn băng thông và đình chỉ quyền truy cập luồng dữ liệu trên lãnh thổ Việt Nam.

Khoản 2 Điều 32 quy định việc chuyển dữ liệu Quan trọng hoặc Cốt lõi ra nước ngoài được Bộ Công an thẩm định, cấp văn bản chấp thuận về an ninh trước khi thực hiện. Khoản 4 Điều 6 lại nghiêm cấm chuyển dữ liệu Cốt lõi hoặc Quan trọng mà có tác động trực tiếp đến các lĩnh vực liệt kê trừ các trường hợp ngoại lệ được Chính phủ cho phép. Khoản 3 và Khoản 4 Điều 32 miễn yêu cầu thẩm định trước trong trường hợp dữ liệu là bí mật kinh doanh của doanh nghiệp khi đáp ứng một trong các điều kiện về quốc gia tiếp nhận được công nhận tương đương, sử dụng Hợp đồng tiêu chuẩn về bảo vệ dữ liệu hoặc có Chứng nhận hợp quy, nhưng vẫn yêu cầu tự lập hồ sơ đánh giá tác động an ninh dữ liệu và báo cáo định kỳ hằng năm về Bộ Công an.

Những quy định này đặt ra các hạn chế mới đối với hoạt động chuyển dữ liệu xuyên biên giới với phạm vi tác động rộng rãi. Chẳng hạn, Luật An ninh dữ liệu sẽ yêu cầu phải có chấp thuận trước đối với việc chuyển Dữ liệu Quan trọng ra nước ngoài, bổ sung cơ chế cấm chuyển dữ liệu trong một số trường hợp và áp dụng yêu cầu lưu trữ dữ liệu tại Việt Nam đối với dữ liệu do khu vực tư nhân nắm giữ trong một số trường hợp nhất định. Thay vì chỉ thực hiện báo cáo một lần trong mỗi kỳ hoạt động theo quy định của Luật Dữ liệu (xem Nghị định 165) và Luật Bảo vệ dữ liệu cá nhân (xem Nghị định 356), Luật An ninh dữ liệu hiện yêu cầu thực hiện báo cáo hằng năm đối với hoạt động chuyển dữ liệu ra nước ngoài. Các biện pháp này không phù hợp với cách tiếp cận hậu kiểm được đặt ra trong Hồ sơ chính sách và cũng không nhất quán với các cam kết của Việt Nam về việc chuyển giao dữ liệu và lưu trữ dữ liệu nội địa theo các điều ước quốc tế như Hiệp định Đối tác Toàn diện và Tiến bộ xuyên Thái Bình Dương (CPTPP), Hiệp định Thương mại Tự do Việt Nam - Liên minh Châu Âu (EVFTA), và Hiệp định Khung về Kinh tế số (DEFA) dự kiến được ký kết trong thời gian tới.

Khuyến nghị: Bãi bỏ yêu cầu lưu trữ dữ liệu tại Việt Nam đối với dữ liệu do khu vực tư nhân nắm giữ. Mục tiêu quản lý nên hướng tới kết quả của việc bảo đảm an ninh dữ liệu thay vì địa điểm lưu trữ dữ liệu, và các tổ chức nên được phép sử dụng các dịch vụ điện toán đám mây quốc tế đáp ứng các yêu cầu an ninh được quy định dựa trên các cơ chế và tiêu chuẩn được quốc tế công nhận như điều khoản hợp đồng mẫu (Standard Contractual Clauses - SCCs), quy tắc ràng buộc nội bộ doanh nghiệp (Binding Corporate Rules - BCRs), chứng nhận theo Hệ thống Quy tắc về Quyền riêng tư xuyên biên giới toàn cầu (Global Cross-Border Privacy Rules - Global CBPR) hoặc các tiêu chuẩn do Tổ chức Tiêu chuẩn hóa Quốc tế (ISO) ban hành. Điều kiện về “kiểm soát tối cao” cần được thay thế bằng các cơ chế được quy định rõ ràng về quyền truy cập, kiểm toán và trách nhiệm phối hợp. Trường hợp vẫn duy trì nghĩa vụ lưu trữ dữ liệu theo Điều 28, nghĩa vụ này chỉ nên được áp dụng đối với dữ liệu có mối liên hệ trực tiếp với an ninh quốc gia và không nên áp dụng đối với dữ liệu do các tổ chức thuộc khu vực tư nhân nắm giữ.

Khuyến nghị: Điều chỉnh cơ chế chuyển dữ liệu xuyên biên giới cho phù hợp với khuôn khổ pháp luật hiện hành theo Luật Dữ liệu và Nghị định 165: duy trì cơ chế chỉ yêu cầu thông báo đối với Dữ liệu Quan trọng; chỉ áp dụng cơ chế thẩm định trước đối với Dữ liệu Cốt lõi được xác định theo phạm vi hẹp và rõ ràng; đồng thời bãi bỏ quy định cấm chuyển dữ liệu ra nước ngoài tại Khoản 4 Điều 6. Trường hợp vẫn duy trì lệnh cấm đối với một nhóm dữ liệu quốc phòng, an ninh do Nhà nước nắm giữ được xác định trong phạm vi hẹp, luật cần quy định rõ tiêu chí áp dụng, trình tự, thủ tục và thời hạn xử lý đối với trường hợp ngoại lệ, và trong mọi trường hợp không nên cấm việc chuyển dữ liệu do các tổ chức thuộc khu vực tư nhân nắm giữ, bao gồm dữ liệu trong các lĩnh vực như tài chính, ngân hàng, năng lượng, giao thông vận tải và viễn thông.

Khuyến nghị: Thay thế nghĩa vụ báo cáo hằng năm quy định tại Khoản 4 Điều 32 bằng việc lập một hồ sơ tự đánh giá duy nhất trong suốt thời gian hoạt động của tổ chức và chỉ cập nhật khi có thay đổi đáng kể, phù hợp với Nghị định 165 và Nghị định 356. Đồng thời, bảo đảm duy trì nguyên tắc không trùng lặp được quy định tại Khoản 3 Điều 42 Nghị định 356, theo đó một báo cáo đánh giá duy nhất là đủ trong trường hợp một tập dữ liệu đồng thời thuộc phạm vi điều chỉnh của nhiều khuôn khổ pháp luật khác nhau. Trường hợp vẫn duy trì các nghĩa vụ theo Khoản 4 Điều 32, Luật An ninh dữ liệu cần quy định rõ các điều kiện áp dụng, yêu cầu về nghĩa vụ thực hiện thông báo trước và thời hạn tối đa đối với việc đình chỉ luồng dữ liệu sau khi đã được chấp thuận. Việc đình chỉ chỉ nên được thực hiện trên cơ sở có quyết định bằng văn bản, nêu rõ căn cứ và lý do, đồng thời chỉ có hiệu lực sau khi đã hết một thời hạn thông báo hợp lý và được xác định trước.

Khuyến nghị: Xây dựng các cơ chế công nhận tương đương (whitelisting), Hợp đồng tiêu chuẩn và chứng nhận trên cơ sở tham vấn cộng đồng doanh nghiệp; đồng thời công nhận các cơ chế chuyển dữ liệu được thừa nhận rộng rãi trên phạm vi quốc tế, bao gồm Điều khoản Hợp đồng Tiêu chuẩn của Liên minh châu Âu (EU Standard Contractual Clauses), Điều khoản Hợp đồng Mẫu ASEAN (ASEAN Model Contractual Clauses) và Hệ thống Quy tắc Bảo mật Xuyên biên giới Toàn cầu (Global Cross-Border Privacy Rules System), là cơ sở hợp lệ cho việc chuyển dữ liệu mà không phải đáp ứng thêm các yêu cầu về báo cáo hoặc xin chấp thuận của Bộ Công an hoặc cơ quan nhà nước có thẩm quyền tương tự.

Chế Tài Xử Phạt Bằng Tiền

Khoản 2 Điều 57 quy định mức phạt tiền tối đa bằng 5% tổng doanh thu của tổ chức vi phạm tại Việt Nam đối với các hành vi vi phạm “đặc biệt nghiêm trọng” liên quan đến Dữ liệu Quan trọng và Dữ liệu Cốt lõi. Quy định này đồng thời cho phép Chính phủ quy định việc áp dụng mức phạt được tính trên cơ sở doanh thu toàn cầu của tập đoàn, với mức tối đa không quá 5%, đối với các tập đoàn đa quốc gia có doanh thu tại Việt Nam “không tương xứng với quy mô, mức độ nghiêm trọng của hành vi vi phạm”. Tuy nhiên, các hành vi vi phạm có thể bị áp dụng mức phạt tính theo tỷ lệ phần trăm doanh thu này hiện chưa được xác định cụ thể mà được giao Chính phủ quy định chi tiết (Khoản 4 Điều 57). Việc áp dụng mức phạt dựa trên doanh thu toàn cầu của tập đoàn, trên cơ sở các điều kiện áp dụng cụ thể sẽ được làm rõ trong các văn bản của Chính phủ sau này, khiến một rủi ro phát sinh riêng tại một quốc gia có thể trở thành rủi ro ở quy mô toàn cầu khi doanh nghiệp đánh giá các kịch bản tuân thủ và rủi ro pháp lý nghiêm trọng nhất. Cách tiếp cận này không tương đồng với các khuôn khổ quản trị dữ liệu khác trong khu vực và có khả năng làm giảm sức hấp dẫn của Việt Nam đối với các nhà đầu tư nước ngoài.

Khuyến nghị: Chỉ áp dụng cơ chế tính mức phạt theo tỷ lệ phần trăm trên cơ sở doanh thu phát sinh tại Việt Nam, đồng thời bãi bỏ cơ chế tính phạt dựa trên doanh thu toàn cầu. Trường hợp vẫn duy trì cơ chế tính phạt trên cơ sở rộng hơn đối với các trường hợp ngoại lệ, các nguyên tắc và tiêu chí áp dụng cần được quy định rõ ràng, khách quan, theo danh mục cụ thể và bảo đảm tương xứng với mức độ nghiêm trọng của hành vi vi phạm. Mức phạt chỉ nên được tính trên doanh thu phát sinh tại Việt Nam của chính chủ thể thực hiện hành vi vi phạm, phù hợp với nguyên tắc tương xứng được thừa nhận rộng rãi trong pháp luật quốc tế cũng như các cam kết của Việt Nam theo Hiệp định chung về Thương mại Dịch vụ (GATS), Hiệp định CPTPP và Hiệp định EVFTA.

Kết luận

Chúng tôi xin cảm ơn Bộ Công an đã xem xét các ý kiến đóng góp của chúng tôi đối với Luật An ninh dữ liệu và hy vọng Quý cơ quan sẽ tích cực cân nhắc các khuyến nghị của chúng tôi. Chúng tôi xin nhấn mạnh lại sự cần thiết phải có thêm thời gian để đánh giá toàn diện sự tương tác giữa Luật An ninh dữ liệu và khuôn khổ pháp luật rộng hơn, bao gồm cả các luật mới và hiện hành. Điều quan trọng là các văn bản hướng dẫn thi hành phải được hoàn thiện thông qua quá trình tham vấn minh bạch với các bên liên quan trước khi Luật có hiệu lực. Chúng tôi trân trọng đề nghị Bộ Công an tiếp tục duy trì đối thoại với các khu vực tư nhân và thúc đẩy các thảo luận cởi mở nhằm hướng tới mục tiêu chung là xây dựng một nền kinh tế số năng động và có năng lực cạnh tranh cao. Nếu Quý Bộ 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 Bộ đã dành thời gian và quan tâm xem xét các ý kiến đóng góp này.

Trân trọng,

Joseph Whitlock

Nếu Quý Bộ có bất kỳ câu hỏi hoặc ý kiến nào, xin vui lòng liên hệ với Joseph Whitlock (josephw@bsa.org).