Ngày 30 tháng 6 năm 2023

Ý KIẾN CỦA LIÊN MINH PHẦN MỀM BSA ĐỐI VỚI NGHỊ ĐỊNH SỐ 13/2023/ND-CP VỀ BẢO VỆ DỮ LIỆU CÁ NHÂN

Kính Gửi: Bộ Công An

Thay mặt cho BSA | Liên Minh Phần Mềm (**BSA**),[1] chúng tôi xin gửi đến Quý Bộ lời chào trân trọng. BSA đã và đang rất tích cực, chủ động tham gia vào quá trình phát triển Luật An Ninh Mạng và các nghị định hướng dẫn thi hành Luật này. Cụ thể, BSA đã góp ý đối với Nghị Định 53 vào tháng 9 năm 2022[2] và đã tham dự Hội thảo do Bộ Công An (**BCA**) tổ chức vào tháng 11 năm 2022. BSA cũng đã góp ý về các đề xuất sửa đổi dự thảo Nghị Định 72 vào tháng 9 năm 2021[3] và tháng 12 năm 2021,[4] cũng như dự thảo Nghị Định Hướng Dẫn Luật An Ninh Mạng vào tháng 12 năm 2018.[5]

Chúng tôi viết thư này để thể hiện sự quan ngại đối với một số vấn đề trong Nghị Định số 13/2023/NĐ-CP về Bảo Vệ Dữ Liệu Cá Nhân (**Nghị Định BVDLCN**), được công bố vào ngày 17 tháng 4 năm 2023 và dự kiến sẽ có hiệu lực vào ngày 01 tháng 7 năm 2023. Chúng tôi rất mong Quý Bộ có thể lưu tâm giải quyết những vấn đề này thông qua các văn bản quy định thi hành hoặc có thêm hướng dẫn giải thích để các điều khoản trong Nghị Định BVDLCN có thể được thực hiện trên thực tế. Cụ thể, chúng tôi xin được nêu một số vấn đề như sau:

Các căn cứ bổ sung cho việc xử lý dữ liệu cá nhân

Điều 11 và 12 đặt ra cơ chế bảo vệ dữ liệu cá nhân dựa trên sự đồng ý, theo đó yêu cầu các cá nhân xem xét các thông tin có liên quan đến một loạt các hoạt động xử lý và thể hiện sự đồng ý đối với các hoạt động đó. Mặc dù Điều 17 đã quy định một số trường hợp ngoại lệ về việc xử lý dữ liệu cá nhân mà không cần sự đồng ý của chủ thể dữ liệu, chẳng hạn như để bảo vệ tính mạng và sức khỏe của các cá nhân trong trường hợp khẩn cấp, thực hiện nghĩa vụ theo hợp đồng và các lý do liên quan đến an ninh và quốc phòng, những ngoại lệ này hẹp hơn nhiều so với nhiều quy định pháp luật bảo vệ dữ liệu được áp dụng trên toàn cầu. Do đó, các công ty có hoạt động kinh doanh tại Việt Nam và người tiêu dùng tiếp cận các sản phẩm và dịch vụ tại Việt Nam có thể bị buộc phải yêu cầu và cung cấp sự đồng ý, dẫn đến cảm giác

[1] BSA là tổ chức ủng hộ hàng đầu cho ngành công nghiệp phần mềm toàn cầu trước các chính phủ và trên thị trường quốc tế. Các thành viên của BSA bao gồm: Adobe, Alteryx, Altium, Amazon Web Services, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cloudflare, CNC/Mastercam, Dassault, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, IBM, Informatica, Juniper Networks, Kyndryl, MathWorks, Microsoft, Nikon, Okta, Oracle, Prokon, PTC, Rockwell, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, và Zoom Video Communications, Inc.

[2] Việt Nam: Ý kiến của Liên Minh Phần Mềm BSA đối với Nghị Định 53 để Thực Thi Luật An Ninh Mạng

[3] Việt Nam: Ý kiến của Liên Minh Phần Mềm BSA đối với Đề xuất Sửa Đổi Dự Thảo Nghị Định 72 | BSA | Liên Minh Phần Mềm

[4] Việt Nam: Ý kiến của Liên Minh Phần Mềm BSA đối với Đề xuất Sửa Đổi Dự Thảo Nghị Định 72 | BSA | Liên Minh Phần Mềm

[5] Việt Nam: Ý kiến của Liên Minh Phần Mềm BSA đối với Dự Thảo Nghị Định hướng dẫn thi hành Luật An Ninh Mạng | BSA | Liên Minh Phần Mềm

300 Beach Road
#30-06 The Concourse
Singapore 199555

P: +65 6292 2072
F: +65 6292 6369
W: bsa.org

Regional Representative Office
UEN: S97RF0005K

quá tải khi cần quá nhiều sự đồng ý đối với rất nhiều hoạt động mà người tiêu dùng trông đợi một cách hợp lý, và/hoặc phù hợp với mục đích xử lý ban đầu.

Khuyến Nghị: Khi BCA thi hành Nghị Định BVDLCN thông qua các quy định và hướng dẫn, chúng tôi khuyến nghị cho phép các công ty xử lý dữ liệu mà không cần sự đồng ý của chủ thể dữ liệu đối với nhiều hoạt động. Ví dụ, một công ty nên được phép xử lý dữ liệu cá nhân khi cần thiết cho các mục đích lợi ích hợp pháp mà công ty theo đuổi, trừ khi những lợi ích đó ít quan trọng hơn các quyền và quyền tự do của chủ thể dữ liệu. Trên thế giới, căn cứ xử lý dữ liệu này thường được sử dụng liên quan đến các hoạt động như quá trình xử lý được thiết kế để ngăn chặn gian lận, lừa đảo, cải thiện sự an toàn, an ninh thông tin và mạng lưới trên hệ thống công nghệ thông tin của công ty hoặc cải thiện chức năng của sản phẩm/dịch vụ được chủ thể dữ liệu sử dụng, bên cạnh một số hoạt động thích hợp khác trong quá trình kinh doanh thông thường. Có một cách để áp dụng căn cứ xử lý vừa nêu, đó là thông qua diễn giải rộng hơn quy định về "sự đồng ý có điều kiện" được nêu rõ trong Điều 11(7) của Nghị Định BVDLCN, trong đó chủ thể dữ liệu có thể được xem là đã đồng ý có điều kiện đối với việc xử lý vì các mục đích hợp pháp, nếu nhận được thông báo thích hợp và việc xử lý đó không ảnh hưởng xấu đến các quyền và quyền tự do của chủ thể dữ liệu.

Đưa ra một khoảng thời gian khả thi để phản hồi các yêu cầu của chủ đề dữ liệu

Mặc dù chúng tôi hoan nghênh việc thiết lập các quyền cho chủ thể dữ liệu trong Nghị Định BVDLCN, nhưng các quy định trong Điều 14.3b, 15.2b, 16.5j có thể được hiểu là bắt buộc bên kiểm soát dữ liệu phản hồi các yêu cầu của chủ thể dữ liệu trong vòng 72 giờ.

Do quy định này không thực tế hoặc không thể thực hiện được trong nhiều trường hợp, chúng tôi khuyến nghị BCA làm rõ theo hướng chỉ phải đưa ra phản hồi sơ bộ ban đầu cho người tiêu dùng trong vòng 72 giờ, và có thể phản hồi đầy đủ sau đó, trong khoảng thời gian hợp lý. Dưới đây là một số vấn đề có thể phát sinh trên thực tế nếu hiểu quy định này theo hướng yêu cầu phải đưa ra phản hồi đầy đủ trong khoảng thời gian 72 giờ nêu trong Nghị Định BVDLCN.

Thứ nhất, đối với tất cả các yêu cầu của chủ thể dữ liệu, khi phản hồi yêu cầu truy cập, cần phải xác minh danh tính của người yêu cầu và đảm bảo rằng đó thực sự là chủ thể dữ liệu yêu cầu chỉnh sửa, xóa hoặc cung cấp dữ liệu cá nhân của họ. Trong quá trình này, các công ty có thể sẽ phải yêu cầu chủ thể dữ liệu cung cấp thêm thông tin, và điều này có thể không khả thi trong khoảng thời gian 72 giờ, đặc biệt nếu có liên quan đến nhiều múi giờ khác nhau.

Thứ hai, trong nhiều trường hợp, yêu cầu của chủ thể dữ liệu sẽ không rõ ràng. Trong những trường hợp này, công ty phải làm rõ với chủ thể dữ liệu về phạm vi của yêu cầu cụ thể. Trong trường hợp yêu cầu xóa, điều quan trọng là công ty phải hiểu dữ liệu cá nhân cụ thể mà người tiêu dùng đang yêu cầu xóa, vì dữ liệu đó không thể khôi phục được sau khi đã xóa.

Thứ ba, ngay cả khi công ty nhận được yêu cầu rõ ràng từ chủ thể dữ liệu có danh tính mà công ty có thể dễ dàng xác thực, việc phản hồi từng yêu cầu cũng vẫn sẽ mất thời gian để thực hiện đúng cách. Do các công ty có thể sẽ nhận được một số lượng lớn yêu cầu, nên việc phản hồi từng yêu cầu trong vòng 72 giờ là không thực tế. Ví dụ, nếu một yêu cầu từ chủ thể dữ liệu đến vào tối thứ Sáu sau khi đã hết giờ làm việc, một tổ chức sẽ có ít hơn một ngày làm việc để phản hồi yêu cầu nếu quy định 72 giờ được hiểu theo nghĩa là giờ theo lịch thay vì giờ kinh doanh.

Khuyến Nghị: Cần làm rõ, thống nhất cách hiểu thời gian phản hồi 72 giờ là để áp dụng cho phản hồi sơ bộ ban đầu của bên kiểm soát đối với chủ thể dữ liệu, đồng thời cho phép cung cấp phản hồi đầy đủ sau đó. Ví dụ, việc cung cấp phản hồi đầy đủ cho yêu cầu của chủ thể dữ liệu trong vòng 30 ngày là phù hợp với thông lệ quốc tế. Quy Định Chung Về Bảo Vệ Dữ Liệu Cá Nhân của Liên Minh Châu Âu (GDPR) cho phép bên kiểm soát có 30 ngày để phản hồi yêu cầu truy cập chủ thể dữ liệu. Tương tự, Đạo Luật Bảo Vệ Dữ Liệu Cá Nhân của Singapore (PDPA) cũng cho phép các tổ chức có 30 ngày để phản hồi yêu cầu truy cập từ chủ thể dữ liệu.

Chuyển dữ liệu ra nước ngoài

Mặc dù chúng tôi hoan nghênh việc loại bỏ yêu cầu địa phương hóa dữ liệu có trong dự thảo trước đó của Nghị Định BVDLCN, nhưng chúng tôi vẫn lo ngại rằng nội dung được thông qua tại Nghị Định BVDLCN vẫn sẽ dẫn đến kết quả tương tự: hạn chế nghiêm trọng việc chuyển dữ liệu quốc tế.

Theo Nghị Định BVDLCN, việc chuyển dữ liệu cá nhân ra nước ngoài chỉ có thể tiến hành thông qua một cơ chế duy nhất: sự đồng ý. Hơn nữa, ngoài sự đồng ý của chủ thể dữ liệu, mỗi lần chuyển dữ liệu đều phải có: (1) đánh giá tác động chuyển dữ liệu và (2) báo cáo đánh giá tác động chuyển dữ liệu đó cho BCA, với yêu cầu nộp cả các bản cập nhật và sửa đổi tương ứng. Trên thực tế, những điều khoản này sẽ tạo ra những rào cản đáng kể đối với việc chuyển dữ liệu ra nước ngoài.

Như đã lưu ý trong các lần góp ý trước đây của chúng tôi, các hạn chế đối với việc chuyển dữ liệu ra nước ngoài sẽ có những tác động tiêu cực đến nền kinh tế trong nước vì chúng không cho phép các doanh nghiệp trong nước và các tổ chức khác được hưởng lợi đầy đủ từ các công nghệ và dịch vụ tiên tiến hiện có trên thị trường toàn cầu. Để lấy ví dụ, các hạn chế đối với việc chuyển dữ liệu ra nước ngoài có thể ngăn cản các doanh nghiệp trong nước, gồm cả doanh nghiệp vừa và nhỏ (**SME**) và các tổ chức lớn hơn như bệnh viện, hãng hàng không, và ngân hàng, sử dụng các giải pháp công nghệ thông tin và điện toán đám mây hàng đầu thế giới từ các nhà cung cấp dịch vụ bên ngoài Việt Nam. Các dịch vụ như vậy thường cung cấp khả năng đảm bảo an toàn dữ liệu tốt nhất. Do các hạn chế đó, các công ty trong nước sẽ khó có thể tiếp cận các dịch vụ như vậy, từ đó làm giảm khả năng cạnh tranh của các công ty này, đặc biệt là trên phạm vi quốc tế, và khiến họ gặp rủi ro lớn về an toàn dữ liệu. Việc thực thi quy định này sẽ không chỉ yêu cầu các cơ quan nhà nước phải bỏ ra nhiều nguồn lực trong việc quản lý và xem xét quá một số lượng rất lớn các thủ tục hành chính dưới hình thức đánh giá tác động, và sẽ dẫn đến gánh nặng trong quản lý hành chính và chi phí vận hành cho các doanh nghiệp trong nước và quốc tế đầu tư tại Việt Nam. Mặc dù chúng tôi ủng hộ các nỗ lực nhằm đảm bảo dữ liệu được bảo vệ tương xứng với rủi ro mà các hành vi xâm phạm dữ liệu gây ra, nhưng những hạn chế nặng nề của Nghị Định BVDLCN đối với việc chuyển dữ liệu ra nước ngoài có thể làm giảm khả năng bảo vệ dữ liệu và làm tăng nguy cơ dữ liệu đó có thể bị xâm phạm, khi khả năng tiếp cận các dịch vụ bảo vệ quyền riêng tư và các sản phẩm và dịch vụ bảo mật bị hạn chế.

Khuyến Nghị: Cần tiếp cận theo hướng quy định về trách nhiệm để hỗ trợ việc chuyển dữ liệu ra nước ngoài, theo đó, tổ chức chuyển dữ liệu vẫn chịu trách nhiệm đảm bảo rằng tổ chức nhận dữ liệu phải bảo vệ dữ liệu cá nhân được chuyển theo cùng tiêu chuẩn được yêu cầu theo luật pháp Việt Nam. Ở mức tối thiểu, chúng tôi đặc biệt khuyến nghị BCA ban hành văn bản hướng dẫn thi hành cho phép các công ty chuyển dữ liệu ra quốc tế trên cơ sở không dựa vào sự đồng ý của chủ thể dữ liệu và tránh yêu cầu các công ty tiến hành đánh

giá tác động chuyển dữ liệu riêng lẻ. Theo đó, chúng tôi khuyến nghị nên công nhận các cơ chế có tính tương tác đối với việc chuyển dữ liệu ra nước ngoài, chẳng hạn như hợp đồng, bao gồm hợp đồng mẫu như Điều Khoản Hợp Đồng Mẫu của ASEAN (ASEAN Model Contractual Clauses); các kế hoạch nội bộ như các quy định có tính ràng buộc của doanh nghiệp; và các cơ chế chứng nhận như hệ thống Quy Tắc Bảo Mật Xuyên Biên Giới của APEC (APEC Cross-Border Privacy Rules (**CBPR**)).

Chúng tôi cũng khuyến nghị rằng mọi đánh giá về tác động của quá trình xử lý dữ liệu và chuyển dữ liệu ra nước ngoài chỉ nên được gửi tới BCA khi có yêu cầu, chứ không nên bắt buộc trong mọi trường hợp. Điều này là phù hợp với các thông lệ quốc tế và giúp tiết kiệm nguồn lực của cả doanh nghiệp và Chính phủ khi tham gia vào các trường hợp thực sự quan trọng, cần thiết.

Vai trò và trách nhiệm của bên kiểm soát và bên xử lý

Chúng tôi hết sức ủng hộ việc Nghị Định BVDLCN công nhận vai trò riêng biệt của bên kiểm soát dữ liệu cá nhân và bên xử lý dữ liệu cá nhân. Sự khác biệt đã có từ lâu giữa hai loại công ty này là nền tảng của luật bảo vệ dữ liệu và quyền riêng tư trên toàn thế giới.[6]

Tuy nhiên, chúng tôi còn một số lo ngại đối với nghĩa vụ của bên xử lý dữ liệu cá nhân theo Điều 39.4 Nghị Định BVDLCN. Điều khoản này quy định bên xử lý dữ liệu cá nhân phải chịu trách nhiệm trước chủ thể dữ liệu về những thiệt hại do quá trình xử lý dữ liệu cá nhân gây ra. Trên thực tế, hầu hết các thỏa thuận kinh doanh đều quy định bên kiểm soát dữ liệu cá nhân kiểm soát mối quan hệ với chủ thể dữ liệu chứ không phải bên xử lý dữ liệu cá nhân. Hầu hết các bên kiểm soát dữ liệu cá nhân không muốn các bên xử lý dữ liệu cá nhân thay mặt bên kiểm soát đó liên hệ với chủ thể dữ liệu. Vì vậy, trên thực tế, Nghị Định sẽ phù hợp hơn nếu bên kiểm soát dữ liệu cá nhân chịu trách nhiệm trước chủ thể dữ liệu về những thiệt hại do việc xử lý dữ liệu cá nhân gây ra.

Khuyến Nghị: Văn bản hướng dẫn thi hành cần làm rõ rằng trách nhiệm đối với chủ thể dữ liệu thuộc về bên kiểm soát dữ liệu cá nhân. Bên kiểm soát dữ liệu cá nhân và bên xử lý dữ liệu cá nhân cũng nên được phép phân chia trách nhiệm trong các hợp đồng giữa họ với nhau.

Thông báo vi phạm

Điều 23 quy định nghĩa vụ thông báo cho BCA và các cơ quan khác trong trường hợp vi phạm các quy định thi hành Nghị Định. Tuy nhiên, quy định này không đặt ra ngưỡng mức độ nghiêm trọng cho các thông báo đó. Do đó, quy định tại Nghị Định có thể được hiểu là cả các vi phạm có rủi ro thấp cho chủ thể dữ liệu cũng cần phải được thông báo. Điều này sẽ dẫn đến sự quá tải thông báo cho cả BCA và bên kiểm soát dữ liệu cá nhân, làm giảm hiệu quả của nghĩa vụ thông báo.

Khuyến Nghị: Các quy định thi hành nên đặt ngưỡng thông báo phù hợp để chỉ những trường hợp vi phạm dữ liệu cá nhân có nguy cơ cao mới cần báo cáo cho BCA. Ví dụ, thông báo có thể phù hợp trong các trường hợp liên quan đến việc thu thập trái phép dữ liệu cá nhân chưa được mã hóa hoặc chưa được xử lý để che đi những nội dung nhạy

[6] Xem BSA, Bên kiểm soát và Bên xử lý: Sự khác biệt lâu đời về quyền riêng tư, có tại https://www.bsa.org/files/policy-filings/10122022controllerprodistinction.pdf.

cảm, qua đó có rủi ro gây hại nghiêm trọng cho chủ thể dữ liệu. Việc tạo ra một ngưỡng rõ ràng cho nghĩa vụ thông báo này giúp các thông báo tập trung vào các vi phạm có rủi ro cao sẽ cho phép BCA và bên kiểm soát dữ liệu cá nhân tập trung nỗ lực và nguồn lực của mình vào việc giải quyết các vi phạm đó một cách thích hợp.

Khoảng Thời Gian Chuyển Tiếp

Nghị Định BVDLCN dự kiến có hiệu lực vào ngày 01 tháng 7 năm 2023. Vì vậy, các công ty có rất ít thời gian để tuân thủ theo các quy định của Nghị định này. Điều này có thể đặc biệt gây ra nhiều khó khăn vì Nghị Định còn quy định nhiều vấn đề cần được hướng dẫn thi hành, bao gồm cả hướng dẫn do BCA ban hành.

Khuyến Nghị: Chúng tôi đặc biệt khuyến nghị gia hạn ngày có hiệu lực của Nghị Định BVDLCN. Ví dụ, BCA có thể mở rộng phạm vi được hưởng thời gian ân hạn tại Điều 43.2 cho tất cả các tổ chức, cho tất cả các tổ chức một khoảng thời gian chuyển tiếp kéo dài hai năm để điều chỉnh các hệ thống và quy trình của họ nhằm tuân thủ Nghị Định BVDLCN. Ngoài ra, BCA có thể ban hành hướng dẫn công nhận rằng việc thực thi Nghị Định BVDLCN sẽ không bắt đầu cho đến ít nhất một năm sau khi BCA ban hành hướng dẫn thực hiện Nghị Định.

Khoảng thời gian chuyển tiếp kéo dài hai năm để đưa ra các quy định bảo vệ dữ liệu cá nhân mới là phù hợp với thông lệ ở các khu vực tài phán khác. Tại Liên Minh Châu Âu, Nghị Viện Châu Âu đã thông qua GDPR vào tháng 4 năm 2016, với khoảng thời gian hai năm trước khi có hiệu lực vào tháng 5 năm 2018. Tại Singapore, Đạo Luật Bảo Vệ Dữ Liệu Cá Nhân được ban hành vào năm 2012 và có hiệu lực vào năm 2014. Tại Thái Lan, Đạo Luật Bảo Vệ Dữ Liệu Cá Nhân được ban hành vào năm 2019 và có hiệu lực vào năm 2022, với khoảng thời gian chuyển tiếp kéo dài ba năm.

Kết Luận

Chúng tôi xin cảm ơn BCA đã xem xét những góp ý của chúng tôi đối với Nghị Định BVDLCN và mong rằng BCA sẽ tích cực thực hiện các kiến nghị của chúng tôi. Chúng tôi rất mong rằng BCA sẽ tiếp tục tham gia đối thoại với khu vực tư nhân và tiếp tục thảo luận cởi mở để đạt được các mục tiêu chung nhằm phát triển nền kinh tế kỹ thuật số năng động và cạnh tranh. Các cuộc thảo luận này có thể bao gồm việc hợp tác chặt chẽ hơn giữa BCA và các cơ quan nhà nước khác với khu vực tư nhân, chẳng hạn như thông qua các cuộc thảo luận bàn tròn về cách thức thực thi Nghị Định BVDLCN.

Vui lòng liên hệ với chúng tôi nếu Quý Bộ cần chúng tôi làm rõ hoặc cần thêm bất cứ thông tin nào. Một lần nữa xin cảm ơn Quý Bộ vì đã dành thời gian xem xét các khuyến nghị.

Trân trọng,

Wong Wai San

Wong Wai San
Quản Lý Cấp Cao, Chính Sách – APAC