Ngày 29, tháng 03, năm 2024

Ý KIẾN ĐÓNG GÓP CỦA LIÊN MINH PHẦN MỀM

VỀ VIỆC XÂY DỰNG LUẬT BẢO VỆ DỮ LIỆU CÁ NHÂN

Kính gửi: Bộ Công an

Liên minh Phần mềm (**BSA**)[1] xin được cảm ơn Bộ Công an đã tạo cơ hội để chúng tôi đóng góp về việc xây dựng Luật Bảo vệ dữ liệu cá nhân (**Luật BVDLCN**). BSA là tổ chức tiên phong đại diện cho ngành công nghiệp phần mềm toàn cầu trước các chính phủ và trên thị trường quốc tế. Các thành viên của BSA là những công ty đổi mới hàng đầu thế giới, tạo ra các giải pháp phần mềm thúc đẩy nền kinh tế.

BSA đã và đang tích cực tham gia vào các hoạt động liên quan đến các quy định bảo vệ dữ liệu cá nhân tại Việt Nam. Chẳng hạn, BSA đã cho ý kiến về dự thảo Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân (**Nghị định BVDLCN**) trong tháng 4/2021[2] và tháng 6/2023.[3] BSA cũng đã tham dự Hội thảo lấy ý kiến đối với dự thảo Nghị định về xử lý vi phạm hành chính trong lĩnh vực an ninh mạng do Bộ Công an tổ chức vào tháng 11 năm 2022, đồng thời tham gia tích cực vào các diễn biến liên quan đến Luật An ninh mạng và các nghị định hướng dẫn thi hành. Ví dụ: ý kiến của BSA đối với các Nghị định số 53/2022/NĐ-CP vào tháng 9 năm 2022[4] và dự thảo Nghị định thay thế Nghị định số 72/2013/NĐ-CP vào tháng 9 năm 2021[5] và tháng 12 năm 2021[6].

BSA đánh giá cao việc Bộ Công an lấy ý kiến đóng góp của các bên liên quan về việc xây dựng Luật BVDLCN. Điều này sẽ tiếp nối thực tiễn tích cực đối với công tác tham vấn các bên liên quan, gồm cả ngành công nghiệp, trong quá trình Quý Bộ xây dựng một chế định bảo vệ dữ liệu cá nhân quốc gia. Việc thiết lập nên một chế định bảo vệ dữ liệu cá nhân quốc gia phù hợp với các thực tiễn tốt nhất toàn cầu là bước quan trọng để đạt được mục tiêu chung là xây dựng nền kinh tế số trong nước năng động và sáng tạo, đồng thời cho phép các doanh nghiệp Việt Nam tham gia vào nền kinh tế số toàn cầu. Chúng tôi khuyến nghị nên đối thoại tích cực hơn nữa với khu vực tư nhân và tiếp tục thảo luận công khai để đạt được các mục tiêu chung

[1] Các thành viên của BSA bao gồm: Adobe, Alteryx, Altium, Amazon Web Services, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cloudflare, CNC / Mastercam, Dassault, Databricks, DocuSign, Dropbox, Elastic, Graphisoft, Hubspot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Nikon, Okta, Oracle, PagerDuty, Palo Alto Networks, Prokon, Rockwell, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Workday, Zendesk và Zoom Video Communications, Inc.

[2] Ý kiến của BSA về Dự thảo Nghị định bảo vệ dữ liệu cá nhân Việt Nam, ngày 09 tháng 4 năm 2021 tại https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-draft-vietnam-personal-data-protection-decree.

[3] Ý kiến của BSA về Nghị định bảo vệ dữ liệu cá nhân số 13/2023/NĐ-CP, ngày 30 tháng 6 năm 2023 tại https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-draft-decree-superseding-decree-no-722013nd-cp.

[4] Ý kiến của BSA về Nghị định 53 thi hành Luật An ninh mạng, ngày 30 tháng 9 năm 2022 tại https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-decree-53-to-implement-the-law-on-cybersecurity.

[5] Ý kiến của BSA về Đề xuất sửa đổi Dự thảo Nghị định 72, ngày 06 tháng 9 năm 2021 tại https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-proposes-amendments-to-draft-decree-72.

[6] Ý kiến của BSA về Đề xuất sửa đổi đối với Dự thảo Nghị định 72 Ngày 30 tháng 12 năm 2021 tại https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-proposes-amendments-to-draft-decree-72-0.

này. Điều này có thể bao gồm sự hợp tác sâu sắc hơn giữa Bộ Công an và các cơ quan nhà nước với khu vực tư nhân, chẳng hạn như thông qua các cuộc đối thoại theo hình thức tọa đàm về cách xây dựng và thực hiện Luật BVDLCN sau này.

Thông qua bản góp ý này gửi Bộ Công an, chúng tôi mong muốn đưa ra các khuyến nghị với các nội dung chính sau:

- Định nghĩa các thuật ngữ chính: Thống nhất các định nghĩa với các định nghĩa của các tổ chức quốc tế, đảm bảo khả năng tương thích với các khu vực tài phán chính;
- Vai trò và trách nhiệm của bên kiểm soát và bên xử lý: Đảm bảo rằng vai trò và trách nhiệm của bên kiểm soát và bên xử lý được xác định rõ ràng, bao gồm cả việc đảm bảo rằng bên kiểm soát có trách nhiệm đáp ứng các yêu cầu của chủ thể dữ liệu;
- Cơ sở pháp lý để xử lý dữ liệu cá nhân ngoài việc thu thập sự đồng ý: Công nhận việc xử lý dữ liệu cá nhân dựa trên các cơ sở độc lập có phạm vi rộng hơn, bao gồm việc xử lý cần thiết vì lợi ích hợp pháp, việc thực hiện hợp đồng, tuân thủ nghĩa vụ pháp lý, bảo vệ lợi ích thiết yếu của chủ thể dữ liệu và việc thực hiện các nhiệm vụ được thi hành vì lợi ích chung;
- Chuyển dữ liệu cá nhân xuyên biên giới: Áp dụng cách tiếp cận dựa trên trách nhiệm giải trình, công nhận một loạt các cơ chế có thể tương tác như hợp đồng, quy tắc ràng buộc doanh nghiệp và các loại chứng nhận; và chỉ yêu cầu đánh giá tác động xử lý dữ liệu, chuyển dữ liệu xuyên biên giới theo yêu cầu của cơ quan có thẩm quyền về bảo vệ dữ liệu;
- Thông báo vi phạm về dữ liệu: Giới hạn nghĩa vụ chỉ thông báo cho chủ thể dữ liệu hoặc cơ quan bảo vệ dữ liệu nếu hành vi vi phạm về dữ liệu cá nhân có nguy cơ cao trong việc gây thiệt hại nghiêm trọng cho chủ thể dữ liệu;
- Quyền của chủ thể dữ liệu: Đảm bảo rằng bên kiểm soát dữ liệu cá nhân có đủ thời gian để đáp ứng yêu cầu của chủ thể dữ liệu và điều chỉnh thời gian đó theo thông lệ quốc tế tốt nhất, tức là 30 ngày; và
- Giai đoạn chuyển tiếp: Đưa ra giai đoạn chuyển tiếp trong vòng hai năm để thực hiện Luật BVDLCN, trong đó sẽ có thời gian ban hành các quy định và hướng dẫn thi hành cũng như cho phép các tổ chức có đủ thời gian để điều chỉnh hệ thống và quy trình đảm bảo tuân thủ Luật BVDLCN.

Chúng tôi hy vọng rằng những đề xuất này sẽ giúp Bộ Công an hoàn thiện các báo cáo của mình: (1) Báo cáo đánh giá tác động của chính sách trong đề nghị xây dựng luật Bảo vệ dữ liệu cá nhân (**Dự thảo Báo cáo Tác động chính sách**) và (2) Báo cáo Đánh giá thực trạng quan hệ xã hội liên quan bảo vệ dữ liệu cá nhân (**Dự thảo Báo cáo thực trạng bảo vệ dữ liệu cá nhân**)[7]. Chúng tôi hy vọng mình sẽ là nguồn lực cho Bộ Công an trong quá trình Quý Bộ xây dựng Luật BVDLCN toàn diện, chắc chắn và phù hợp với các thông lệ quốc tế tốt nhất, thống nhất các

[7] Tài liệu Lấy ý kiến công chúng đối với dự thảo hồ sơ do Bộ Công an cung cấp, ngày 01 tháng 3 năm 2024tại https://bocongan.gov.vn/pbgdpl/van-ban-moi/du-thao-ho-so-de-nghi-xay-dung-luat-bao-ve-du-lieu-ca-nhan-t1282.html.

quy định bảo vệ dữ liệu của Việt Nam, bảo vệ quyền và lợi ích hợp pháp của các tổ chức và chủ thể dữ liệu, đồng thời hỗ trợ sự phát triển của nền kinh tế số năng động và sáng tạo.

Định Nghĩa Các Thuật Ngữ Chính

BSA ủng hộ mục đích trong Dự thảo Báo cáo Tác động chính sách cho Luật BVDLCN rằng Luật BVDLCN sẽ đưa ra các định nghĩa chính[8], bao gồm các thuật ngữ "dữ liệu cá nhân", "chủ thể dữ liệu", "xử lý dữ liệu cá nhân", "sự đồng ý", "bên kiểm soát dữ liệu cá nhân", "bên xử lý dữ liệu cá nhân" và "chuyển dữ liệu cá nhân ra nước ngoài". Điều quan trọng là các thuật ngữ được sử dụng trong Luật BVDLCN phải phù hợp với các quy định và thông lệ quốc tế tốt nhất, và nổi bật hiện nay về bảo vệ dữ liệu cá nhân[9].

Khuyến nghị: Định nghĩa của các thuật ngữ chính như vậy cần phù hợp với các định nghĩa được sử dụng bởi các tổ chức quốc tế như ASEAN tại Khung Bảo vệ Dữ liệu của ASEAN[10] và OECD trong Khung Quyền riêng tư của OECD[11]. Các thuật ngữ này cũng phải tương thích với các định nghĩa ở các khu vực tài phán quan trọng như EU, Nhật Bản và Singapore.

Vai Trò Và Trách Nhiệm Của Bên Kiểm Soát Và Bên Xử Lý

BSA hết sức ủng hộ khuyến nghị của Dự thảo Báo cáo Tác động chính sách khi xác định bên kiểm soát dữ liệu cá nhân và bên xử lý dữ liệu cá nhân[12]. Sự khác biệt rõ rệt giữa hai loại chức năng này là nền tảng cho pháp luật bảo vệ dữ liệu và quyền riêng tư trên toàn thế giới[13].

Bên kiểm soát dữ liệu cá nhân, là bên xác định phương tiện và mục đích xử lý dữ liệu cá nhân, phải chịu trách nhiệm chính trong việc đáp ứng các nghĩa vụ về cách thức và lý do dữ liệu cá nhân được thu thập và sử dụng. Bên xử lý dữ liệu cá nhân, là bên xử lý dữ liệu thay mặt cho bên kiểm soát, nên sử dụng các biện pháp bảo mật hợp lý và phù hợp để ngăn chặn việc truy cập, sử dụng hoặc tiết lộ trái phép dữ liệu cá nhân, nếu không thì phải có trách nhiệm tuân theo hướng dẫn của bên kiểm soát theo thỏa thuận hợp đồng của hai bên. Bên kiểm soát và bên xử lý nên có quyền tự do đàm phán các điều khoản hợp đồng phản ánh các vai trò khác nhau này.

Mặc dù chúng tôi ủng hộ việc công nhận vai trò riêng biệt của bên kiểm soát dữ liệu cá nhân và bên xử lý dữ liệu cá nhân trong khuôn khổ Nghị định BVDLCN, Điều 39.4 của Nghị định này vẫn quy định bên xử lý dữ liệu cá nhân phải chịu trách nhiệm với chủ thể dữ liệu về thiệt hại gây ra bởi việc xử lý dữ liệu cá nhân. Trong thực tế, điều này tạo ra xung đột giữa vai trò của bên xử lý dữ liệu trong việc hỗ trợ bên kiểm soát dữ liệu và trách nhiệm chính của bên kiểm soát dữ liệu đối với chủ thể dữ liệu. Theo định nghĩa, bên kiểm soát dữ liệu cá nhân sẽ

[8] Dự thảo Báo cáo Tác động chính sách, đoạn III.1.4.2. trang 11-12.
[9] Dự thảo Báo cáo Tác động chính sách, đoạn I.3. trên trang 3.
[10] Hội nghị Bộ trưởng Công nghệ thông tin và Viễn thông ASEAN (TELMIN), Khung bảo vệ dữ liệu cá nhân, ngày 25 tháng 11 năm 2016 tại https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf.
[11] Khung quyền riêng tư của OECD, ngày 11 tháng 7 năm 2013 tại:https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf .
[12] Dự thảo Báo cáo Tác động chính sách, đoạn III.1.4.2. trên trang 11-12.
[13] BSA, Bên kiểm soát và Bên xử lý: Sự khác biệt biệt sâu sắc về quyền riêng tư, có sẵn bằng tiếng Anh và tiếng Việt tại https://www.bsa.org/policy-filings/the-global-standard-distinguishing-between-controllers-and-processors-in-luật về quyền riêng tư.

xác định cách thức và lý do tại sao thông tin cá nhân của chủ thể dữ liệu nên được xử lý. Theo đó, bên xử lý dữ liệu cá nhân sẽ xử lý thông tin đó thay mặt và theo hướng dẫn của bên kiểm soát dữ liệu cá nhân. Do đó, bên xử lý đang tuân theo hướng dẫn của bên kiểm soát và không nên phải chịu trách nhiệm về thiệt hại gây ra cho chủ thể dữ liệu do tuân theo các hướng dẫn đó. Chúng tôi khuyến nghị nên đảm bảo rằng Luật BVDLCN không trộn lẫn trách nhiệm của hai vai trò này và do đó không quy định bên xử lý dữ liệu phải chịu trách nhiệm của bên kiểm soát dữ liệu, bao gồm cả các trường hợp như được mô tả ở trên.

Khuyến nghị: Khác với Nghị định BVDLCN, Luật BVDLCN cần làm rõ rằng các trách nhiệm đối với chủ thể dữ liệu phải do bên kiểm soát dữ liệu cá nhân - bên xác định cách thức và lý do xử lý thông tin cá nhân của chủ thể dữ liệu - nắm giữ. Bên xử lý dữ liệu cá nhân nên tiếp tục xử lý dữ liệu cá nhân tuân theo các biện pháp bảo mật hợp lý và phù hợp cũng như các biện pháp bảo vệ theo hợp đồng để bảo vệ dữ liệu cá nhân. Bên kiểm soát và bên xử lý dữ liệu cá nhân xác định rõ hơn vai trò riêng biệt của mỗi bên thông qua các thỏa thuận hợp đồng phản ánh các chức năng và khả năng khác nhau của mỗi bên.

Cơ Sở Pháp Lý Để Xử Lý Dữ Liệu Cá Nhân Ngoài Sự Đồng Ý

BSA hết sức ủng hộ ý kiến đề xuất tại Dự thảo Báo cáo Tác động chính sách rằng có những lý do chính đáng để xử lý dữ liệu cá nhân khi không cần sự đồng ý của chủ thể dữ liệu[14]. Luật BVDLCN nên công nhận và cho phép xử lý dữ liệu vì nhiều lý do hợp lệ, bao gồm các mục đích kinh doanh hợp pháp phù hợp với bối cảnh giao dịch hoặc kỳ vọng của chủ thể dữ liệu. Các mục đích hợp lệ khác bao gồm xử lý liên quan đến việc thực hiện hợp đồng; vì lợi ích công cộng hoặc lợi ích thiết yếu của chủ thể dữ liệu; cần thiết tuân thủ nghĩa vụ pháp lý; hoặc dựa trên sự đồng ý của chủ thể dữ liệu. Luật BVDLCN nên đảm bảo các cơ sở xử lý dữ liệu được soạn thảo theo cách không hạn chế khả năng của một tổ chức sử dụng chúng một cách độc lập hoặc vì các nỗ lực an ninh mạng hợp pháp, việc thực hiện các biện pháp để phát hiện hoặc ngăn chặn gian lận hoặc đánh cắp danh tính, khả năng bảo vệ thông tin mật, hoặc thực hiện hoặc bảo vệ khiếu nại pháp lý.

Chúng tôi khuyến nghị Bộ Công an áp dụng cách tiếp cận đối với các vấn đề này trong Luật BVDLCN khác với cách tiếp cận của Nghị định BVDLCN hiện hành. Theo Nghị định BVDLCN, Điều 11 và Điều 12 đặt ra chế định bảo vệ dữ liệu cá nhân dựa trên sự đồng ý, yêu cầu các cá nhân xem xét nhiều yêu cầu đồng ý cho một loạt các hành động xử lý. Mặc dù Điều 17 tạo ra một số ngoại lệ đối với các yêu cầu đồng ý này, chẳng hạn như bảo vệ tính mạng và sức khỏe của các cá nhân trong trường hợp khẩn cấp, thực hiện nghĩa vụ hợp đồng và lý do liên quan đến an ninh và quốc phòng, những ngoại lệ này hẹp hơn nhiều so với các luật bảo vệ dữ liệu được áp dụng trên toàn cầu. Do đó, các doanh nghiệp tại Việt Nam và người tiêu dùng tiếp cận các sản phẩm và dịch vụ tại Việt Nam trên cơ sở Nghị định BVDLCN có thể bị buộc phải lặp lại liên tục việc yêu cầu và cung cấp sự đồng ý, dẫn đến tình trạng quá tải đồng ý, ngay cả đối với những hoạt động mà người tiêu dùng có thể kỳ vọng một cách hợp lý hoặc phù hợp với các mục đích ban đầu của việc xử lý.

[14] Dự thảo Báo cáo Tác động chính sách, đoạn II.2.3. trang 10; đoạn III.3.4.2. trang 19; đoạn III.4.4.2. trang 23.

Khuyến nghị: Luật BVDLCN nên công nhận các doanh nghiệp có thể xử lý dữ liệu mà không cần sự đồng ý của chủ thể dữ liệu cho một số hoạt động. Ví dụ: doanh nghiệp nên được phép xử lý dữ liệu cá nhân khi cần thiết vì các mục đích và lợi ích hợp pháp mà doanh nghiệp đó theo đuổi, trừ khi các lợi ích đó ít quan trọng hơn quyền và tự do của chủ thể dữ liệu. Trên toàn cầu, cơ sở cho việc xử lý dữ liệu thường được sử dụng liên quan đến các hoạt động bao gồm xử lý nhằm ngăn chặn gian lận, cải thiện an ninh mạng và thông tin của hệ thống CNTT của doanh nghiệp, hoặc cải thiện chức năng của sản phẩm hoặc dịch vụ được chủ thể dữ liệu sử dụng, cùng với các hoạt động liên quan khác trong quá trình kinh doanh thông thường. Cụ thể, chúng tôi khuyến nghị Luật BVDLCN nên công nhận việc xử lý dữ liệu cá nhân cho các lợi ích hợp pháp, nếu có thông báo thích hợp và việc xử lý đó không ảnh hưởng xấu đến quyền và tự do của chủ thể dữ liệu. Chúng tôi cũng ủng hộ công nhận một loạt các căn cứ độc lập để xử lý dữ liệu cá nhân ngoài sự đồng ý, bao gồm xử lý cần thiết để thực hiện hợp đồng, xử lý cần thiết để tuân thủ các nghĩa vụ pháp lý, xử lý cần thiết để bảo vệ lợi ích thiết yếu của chủ thể dữ liệu và xử lý cần thiết để thực hiện các nhiệm vụ được thực hiện vì lợi ích công cộng.

Chuyển Dữ Liệu Cá Nhân Xuyên Biên Giới

BSA hết sức ủng hộ tầm quan trọng của việc tạo điều kiện thuận lợi cho việc chuyển dữ liệu cá nhân xuyên biên giới. Chúng tôi đánh giá cao sự ghi nhận về tầm quan trọng của việc chuyển dữ liệu quốc tế trong cả Dự thảo Báo cáo Tác động chính sách và Dự thảo Báo cáo thực trạng bảo vệ dữ liệu cá nhân, ví dụ: các cam kết của Việt Nam trong các hiệp định và thỏa thuận quốc tế như Hiệp định Đối tác Toàn diện và Tiến bộ xuyên Thái Bình Dương (**CPTPP**) và Hiệp định Thương mại Tự do Việt Nam - Liên minh châu Âu (**EVFTA).**

Luật BVDLCN nên cho phép và khuyến khích chuyển dữ liệu toàn cầu, làm nền tảng cho nền kinh tế toàn cầu. Các tổ chức chuyển dữ liệu trên toàn cầu nên thực hiện các thủ tục để đảm bảo dữ liệu được truyền ra bên ngoài quốc gia tiếp tục được bảo vệ. Khi có sự khác biệt giữa các cơ chế bảo vệ dữ liệu, các chính phủ nên tạo ra các công cụ để thu hẹp những khoảng cách đó theo cách vừa bảo vệ quyền riêng tư vừa tạo điều kiện thuận lợi cho việc chuyển dữ liệu toàn cầu. Các khuôn khổ bảo vệ dữ liệu không nên áp đặt các yêu cầu nội địa hóa dữ liệu đối với cả khu vực công hoặc tư nhân, bởi vì các yêu cầu đó có thể làm cản trở các nỗ lực thực hiện các biện pháp bảo mật hiệu quả, cản trở đổi mới kinh doanh và hạn chế các dịch vụ có sẵn cho người tiêu dùng.

Khuyến nghị: Luật BVDLCN nên áp dụng cách tiếp cận dựa trên trách nhiệm giải trình để hỗ trợ chuyển dữ liệu xuyên biên giới, theo đó tổ chức chuyển dữ liệu vẫn chịu trách nhiệm đảm bảo rằng tổ chức tiếp nhận bảo vệ dữ liệu cá nhân được chuyển giao theo cùng tiêu chuẩn được quy định tại pháp luật Việt Nam. Ngoài ra, Luật BVDLCN nên công nhận một loạt các cơ chế có thể tương thích để chuyển dữ liệu cá nhân xuyên biên giới, chẳng hạn như hợp đồng, bao gồm các hợp đồng mẫu như: Điều khoản hợp đồng mẫu ASEAN; các chương trình nội bộ như các quy tắc ràng buộc của doanh nghiệp; và các chứng nhận như các Hệ thống Quy tắc Bảo vệ quyền riêng tư xuyên biên giới toàn cầu của APEC (**CBPR**).

Cách tiếp cận này sẽ áp dụng một sự thay đổi quan trọng khi so sánh với Nghị định BVDLCN hiện hành vốn chỉ dựa trên sự đồng ý cho phép chuyển dữ liệu cá nhân xuyên biên giới. Hơn

nữa, theo Nghị định BVDLCN, ngoài sự đồng ý của chủ thể dữ liệu, mỗi lần chuyển dữ liệu lại cần phải: (1) đánh giá tác động của việc chuyển dữ liệu; và (2) báo cáo đánh giá tác động của việc chuyển dữ liệu gửi tới Bộ Công an, với yêu cầu gửi cập nhật và sửa đổi cho phù hợp. Trên thực tế, các điều khoản này tạo ra những rào cản đáng kể đối với việc chuyển dữ liệu xuyên biên giới.

Như đã lưu ý trong các lần góp ý trước đây của chúng tôi, các hạn chế về chuyển dữ liệu xuyên biên giới có tác động tiêu cực đến nền kinh tế trong nước khi ngăn cản các doanh nghiệp và tổ chức trong nước không thể tận dụng đầy đủ các công nghệ và dịch vụ tiên tiến trên thị trường toàn cầu. Ví dụ, các hạn chế về chuyển dữ liệu xuyên biên giới có thể ngăn cản các doanh nghiệp trong nước, bao gồm các 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 điện toán đám mây và công nghệ thông tin hàng đầu thế giới từ các nhà cung cấp dịch vụ cung cấp dịch vụ của họ từ bên ngoài Việt Nam. Các dịch vụ này thường cung cấp khả năng bảo mật hàng đầu. Các doanh nghiệp trong nước phải chịu hạn chế chuyển dữ liệu rất khó có thể tiếp cận các dịch vụ đó, làm giảm khả năng cạnh tranh của họ, đặc biệt là trên bình diện quốc tế và khiến họ gặp nhiều rủi ro về dữ liệu và an ninh mạng hơn. Các hạn chế về chuyển dữ liệu quốc tế cũng sẽ đòi hỏi nhiều nguồn lực đối với các cơ quan chính phủ trong hoạt động quản lý. Nghĩa vụ báo cáo đánh giá tác động bổ sung trong Nghị định BVDLCN làm tiêu tốn nguồn lực của cả các doanh nghiệp đang tiến hành hoạt động thương mại quốc tế và Bộ Công an, trong khi có rất ít cải thiện (nếu có) trong việc bảo vệ thông tin cá nhân. Mặc dù chúng tôi ủng hộ các quy định bảo vệ quyền riêng tư và an ninh, nhưng những hạn chế khắt khe của Nghị định BVDLCN đối với việc chuyển dữ liệu xuyên biên giới lại làm giảm bớt việc bảo vệ dữ liệu và làm tăng rủi ro bị xâm phạm dữ liệu bằng cách hạn chế việc tiếp cận các sản phẩm và dịch vụ bảo vệ quyền riêng tư và an ninh.

Khuyến nghị: Chúng tôi đặc biệt khuyến nghị Luật BVDLCN cần được soạn thảo để nhằm hỗ trợ việc chuyển dữ liệu quốc tế. Cụ thể, luật này cần cho phép các doanh nghiệp chuyển dữ liệu ra quốc tế dựa trên các cơ sở pháp lý không chỉ giới hạn ở sự đồng ý của chủ thể dữ liệu và sử dụng các cơ chế không yêu cầu các doanh nghiệp phải thực hiện đánh giá tác động chuyển dữ liệu riêng lẻ cho mỗi lần chuyển dữ liệu. Ngoài ra, nếu đánh giá tác động xử lý dữ liệu và chuyển dữ liệu xuyên biên giới nào được yêu cầu cho các trường hợp cụ thể thì các đánh giá này chỉ nên được gửi cho Bộ Công an hoặc cơ quan bảo vệ dữ liệu liên quan khi có yêu cầu thay vì bắt buộc trong mọi trường hợp. Điều này sẽ phù hợp với thực tiễn tốt nhất trên thế giới và sẽ giúp cả các doanh nghiệp và cơ quan quản lý tập trung nguồn lực tốt hơn vào những trường hợp quan trọng.

Thông Báo Vi Phạm Về Dữ liệu

BSA hỗ trợ tạo ra một hệ thống thông báo vi phạm về dữ liệu cá nhân áp dụng cho tất cả các doanh nghiệp và tổ chức. Các điều khoản vi phạm về dữ liệu được xây dựng phù hợp khuyến khích việc áp dụng các thực tiễn bảo mật dữ liệu mạnh mẽ và cho phép các cá nhân thực hiện hành động để tự bảo vệ mình trong trường hợp dữ liệu của họ bị xâm phạm. Khi xây dựng các điều khoản thông báo vi phạm dữ liệu, điều quan trọng là cần nhận định được rằng không phải tất cả các vi phạm về dữ liệu đều đại diện cho các mối đe dọa như nhau. Trong nhiều trường hợp, một sự cố có thể không gây ra rủi ro thực tế, đặc biệt khi những nỗ lực hợp lý, kịp thời được thực hiện, dữ liệu của các cá nhân không bị xâm phạm. Để đảm bảo chủ thể dữ liệu và cơ quan cơ quan bảo vệ dữ liệu không nhận được nhiều thông báo liên quan đến các sự cố không tạo ra rủi ro gây hại đáng kể đối với chủ thể dữ liệu, nghĩa vụ thông báo chỉ nên được thực hiện nếu xuất hiện sự cố gây ra nguy cơ cao về việc đánh cắp danh tính hoặc gian lận tài chính do truy cập trái phép, phá hủy, sử dụng, sửa đổi hoặc tiết lộ dữ liệu cá nhân. Ví dụ: nghĩa vụ thông báo không nên áp dụng cho các trường hợp dữ liệu không thể sử dụng được, không thể đọc được hoặc không thể giải mã được đối với bên thứ ba không được phép, thông qua các thực tiễn hoặc phương pháp (ví dụ: mã hóa) được công nhận rộng rãi là thực tiễn hoặc tiêu chuẩn ngành hiệu quả. Cuối cùng, để đảm bảo người dùng nhận được thông báo có ý nghĩa trong trường hợp vi phạm, điều quan trọng là bên kiểm soát dữ liệu phải có đủ thời gian để thực hiện đánh giá rủi ro kỹ lưỡng để xác định phạm vi rủi ro bảo mật, ngăn chặn tiết lộ thêm và xác định các rủi ro tiềm ẩn đối với chủ thể dữ liệu do sự cố. Do đó, sẽ là phản tác dụng nếu đưa vào điều khoản "xâm phạm dữ liệu" quy định một thời hạn cố định cho việc thông báo.

Khuyến nghị: Chúng tôi khuyến nghị việc áp dụng nghĩa vụ thông báo cho chủ thể dữ liệu hoặc cơ quan quản lý dữ liệu chỉ đối với các xâm phạm dữ liệu cá nhân có nguy cơ gây thiệt hại đáng kể như là đánh cắp danh tính hoặc gian lận tài chính do truy cập, phá hủy, sử dụng, sửa đổi hoặc tiết lộ dữ liệu cá nhân trái phép. Bên kiểm soát dữ liệu cá nhân không nên bị yêu cầu phải thực hiện bất kỳ thông báo nào nếu không có nguy cơ cao gây thiệt hại đáng kể, kể cả nếu dữ liệu bị xâm phạm được lưu trữ theo cách mà một bên thứ ba trái phép không thể sử dụng, không thể đọc hoặc không thể giải mã thông qua các thực tiễn hoặc phương pháp được công nhận rộng rãi là thực tiễn và tiêu chuẩn hiệu quả của ngành công nghiệp.

Quyền Của Chủ Thể Dữ Liệu

BSA hoan nghênh việc đề xuất liên quan đến việc thiết lập quyền chủ thể dữ liệu cho các cá nhân trong Dự thảo Báo cáo Tác động chính sách[15]. Chủ thể dữ liệu phải được biết nếu các tổ chức xử lý dữ liệu cá nhân liên quan đến họ cũng như bản chất và việc sử dụng dữ liệu đó. Các cá nhân có quyền yêu cầu về tính chính xác của dữ liệu đó và, khi thích hợp, có quyền yêu cầu chỉnh sửa hoặc xóa dữ liệu. Chủ thể dữ liệu cũng cần có quyền yêu cầu một bản sao dữ liệu cá nhân mà họ cung cấp cho tổ chức hoặc được tạo ra bởi chính họ.

Khi các quyền này được thực hiện, các tổ chức nên linh hoạt trong việc xác định các phương tiện và định dạng thích hợp để cung cấp thông tin cho chủ thể dữ liệu. Bên kiểm soát dữ liệu cá nhân – bên xác định phương tiện và mục đích xử lý dữ liệu cá nhân - phải chịu trách nhiệm chính trong việc đáp ứng các yêu cầu này. Bên kiểm soát phải có khả năng từ chối các yêu

[15] Dự thảo Báo cáo Tác động chính sách, đoạn III.2.4.2 trang 14.

cầu đó khi gánh nặng hoặc chi phí làm như vậy sẽ không hợp lý hoặc không tương xứng với các rủi ro đối với quyền của chủ thể dữ liệu; để tuân thủ các yêu cầu pháp lý; bảo đảm an ninh mạng; để bảo vệ thông tin bí mật thương mại; cho mục đích nghiên cứu; hoặc để tránh vi phạm quyền riêng tư và các quyền cũng như lợi ích khác của chủ thể dữ liệu. Bên kiểm soát cũng nên thực hiện các quy trình xác minh an toàn để xác thực chủ thể dữ liệu đưa ra yêu cầu nhằm xử lý rủi ro của việc tiết lộ thông tin không đúng cách.

Chúng tôi khuyến khích Luật BVDLCN áp dụng cách tiếp cận đối với quyền chủ thể dữ liệu có thể được thực hiện một cách khả thi và phù hợp với thông lệ quốc tế tốt nhất. Hiện tại, Khoản 3 Điều 14, Khoản 2 Điều, Khoản 5 Điều 16 trong Nghị định BVDLCN có thể được hiểu là yêu cầu bên kiểm soát phải đáp ứng một số yêu cầu của chủ thể dữ liệu trong vòng 72 giờ. Như đã nêu ra trong bản góp ý trước đây của chúng tôi[16], khung thời gian ngắn như vậy đặt ra những thách thức như: xác minh danh tính của người yêu cầu; làm rõ yêu cầu của chủ thể dữ liệu; đảm bảo chủ thể dữ liệu hiểu hậu quả từ yêu cầu của họ (chẳng hạn như trong trường hợp yêu cầu xóa); và có thể quản lý một khối lượng lớn các yêu cầu đó. Điều này cũng không phù hợp với các khuôn khổ pháp luật bảo vệ dữ liệu hàng đầu trên toàn cầu, cho phép bên kiểm soát có ít nhất 30 ngày để trả lời các yêu cầu về quyền của chủ thể dữ liệu, với khả năng được gia hạn.

Khuyến nghị: Đảm bảo bên kiểm soát dữ liệu cá nhân có đủ tính linh hoạt và thời gian để phản hồi các yêu cầu của chủ thể dữ liệu và điều chỉnh tính linh hoạt và thời gian cho phù hợp với các thông lệ quốc tế tốt nhất, tức là trong vòng 30 ngày. Quy định bảo vệ dữ liệu chung của EU (**GDPR)** cho phép bên kiểm soát 30 ngày phản hồi yêu cầu truy cập chủ thể dữ liệu. Tương tự, Đạo luật bảo vệ dữ liệu cá nhân Singapore (**PDPA)** cũng cho phép các tổ chức có 30 ngày để phản hồi yêu cầu truy cập từ chủ thể dữ liệu.

Giai Đoạn Chuyển Tiếp

Như đã ghi nhận trong cả Dự thảo Báo cáo Tác động chính sách và Dự thảo Báo cáo thực trạng bảo vệ dữ liệu cá nhân, hiện nay có rất ít sự thống nhất trong các luật và quy định nội địa liên quan đến bảo vệ dữ liệu cá nhân tại Việt Nam. Với việc ban hành Luật Bảo vệ dữ liệu cá nhân và các quy định, hướng dẫn thi hành kèm theo, chúng ta có thể đối mặt với nhiều vấn đề và thách thức khi thi hành với các quy trình và thực tiễn bảo vệ dữ liệu mới. Các cơ quan chính phủ, các tổ chức bao gồm các doanh nghiệp lớn và nhỏ và chủ thể dữ liệu sẽ cần thời gian để điều chỉnh theo sự thay đổi. Chúng tôi cũng đặc biệt khuyến nghị Chính phủ tham khảo ý kiến của các bên liên quan trong suốt giai đoạn chuyển tiếp, để tạo điều kiện chia sẻ thông tin về các vấn đề phát sinh khi thực hiện.

[16] Ý kiến của BSA về Nghị định bảo vệ dữ liệu cá nhân số 13/2023/NĐ-CP, ngày 30 tháng 6 năm 2023 tại https://www.bsa.org/policy-filings/vietnam-bsa-comments-on-draft-decree-superseding-decree-no-722013nd-cp.

<u>Khuyến nghị</u>: Chúng tôi kiến nghị nên đưa ra một giai đoạn chuyển tiếp trong vòng hai năm kể từ khi Luật BVDLCN được ban hành cho đến khi Luật Bảo vệ Dữ liệu Cá nhân bắt đầu có hiệu lực. Điều này sẽ tạo thời gian cho bất kỳ quy định và hướng dẫn thi hành nào được ban hành và cho phép các tổ chức có đủ thời gian để điều chỉnh hệ thống và quy trình của họ để tuân thủ Luật BVDLCN.

Giai đoạn chuyển tiếp trong vòng hai năm khi đưa ra các quy định mới về bảo vệ dữ liệu cá nhân là phù hợp với thực tiễn tại các khu vực tài phán khác. Tại Singapore, Đạo luật Bảo vệ dữ liệu cá nhân đã được thông qua năm 2012 và có hiệu lực vào năm 2014. Tại Liên minh Châu Âu, Nghị viện Châu Âu thông qua GDPR vào tháng 4/2016 và có hiệu lực vào tháng 5/2018. Tại Thái Lan, Luật Bảo vệ dữ liệu cá nhân đã được thông qua năm 2019 và có hiệu lực vào năm 2022, qua đó cung cấp một giai đoạn chuyển chuyển tiếp trong vòng ba năm.

Kết Luận Và Các Tài Liệu Khác

Chúng tôi xin cảm ơn Bộ Công an đã xem xét các ý kiến của chúng tôi về việc xây dựng Luật BVDLCN và hy vọng rằng Bộ Công an sẽ tích cực xem xét các khuyến nghị của chúng tôi. Ngoài các khuyến nghị trên, BSA đã phát triển tài liệu Thực tiễn tốt nhất về quyền riêng tư toàn cầu[17] có sẵn bằng tiếng Anh và tiếng Việt , Bộ Công an có thể xem xét như một nguồn tài liệu bổ sung. Chúng tôi xin được đính kèm một bản sao trong Phụ lục.

Chúng tôi mong rằng Bộ Công an tiếp tục tham gia đối thoại với khu vực tư nhân và tiếp tục thảo luận công khai để đạt được các mục tiêu chung để phát triển nền kinh tế số năng động và cạnh tranh. Điều này có thể bao gồm sự hợp tác sâu rộng hơn giữa Bộ Công an cùng các cơ quan chính phủ khác với khu vực tư nhân như thông qua các cuộc đối thoại về cách thức xây dựng Luật Bảo vệ dữ liệu cá nhân. Xin vui lòng liên hệ với chúng tôi nếu Quý Bộ cần làm rõ hay cần cung cấp thêm thông tin. Một lần nữa, xin cảm ơn Quý Bộ đã dành thời gian xem xét.

Trân trọng

Wong Wai San

Wong Wai San
Quản lý cấp cao, Chính sách – APAC

[17] Các thực tiễn tốt nhất về quyền riêng tư của BSA Global năm 2018 tại https://www.bsa.org/policy-filings/2018-bsa-global-privacy-best-practices.

NHỮNG PHƯƠNG PHÁP BẢO MẬT TỐT NHẤT ÁP DỤNG CHUNG

BSA là đơn vị ủng hộ hàng đầu cho ngành phần mềm toàn cầu, ngành tiên phong trong việc phát triển những sáng kiến đổi mới tiên tiến, trong đó có điện toán đám mây, phân tích dữ liệu và trí tuệ nhân tạo. Những công nghệ có phần mềm hỗ trợ ngày càng phụ thuộc vào dữ liệu, trong một số trường hợp là dữ liệu cá nhân, để tiến hành hoạt động. Do đó, việc bảo vệ dữ liệu cá nhân là một trong những yếu tố quan trọng được ưu tiên đối với các thành viên BSA. Chúng tôi cũng nhận ra đó là một phần thiết yếu trong việc tạo dựng niềm tin nơi khách hàng. Với mục đích ấy, BSA thúc đẩy một phương thức lấy người dùng làm trọng tâm để tiếp cận vấn đề về quyền riêng tư, cung cấp cho người tiêu dùng những cơ chế góp phần kiểm soát dữ liệu cá nhân của họ. BSA cũng ủng hộ các khuôn khổ bảo vệ dữ liệu đảm bảo việc sử dụng dữ liệu cá nhân phù hợp với kỳ vọng của người tiêu dùng, đồng thời cho phép các công ty theo đuổi lợi ích kinh doanh chính đáng.

Khi các nước trên thế giới xem xét việc phát triển các khuôn khổ bảo vệ dữ liệu, nhiều quốc gia đã tìm cách xác định những phương pháp tốt nhất mang tính tổng quát để tiếp cận các vấn đề này. BSA ủng hộ việc thực hiện các phương pháp tốt nhất giúp tăng cường tính minh bạch trong việc thu thập và sử dụng dữ liệu cá nhân; cho phép và tôn trọng các lựa chọn được thực hiện khi có đầy đủ thông tin bằng cách cung cấp cơ chế quản lý việc thu thập và sử dụng dữ liệu cá nhân; mang lại cho người tiêu dùng quyền kiểm soát dữ liệu cá nhân của chính mình; cung cấp chế độ bảo mật mạnh mẽ; và thúc đẩy việc sử dụng dữ liệu vì mục đích kinh doanh chính đáng. **Dưới đây, chúng tôi nêu bật những phương pháp tốt nhất có thể góp phần đạt những mục tiêu này và đóng vai trò hướng dẫn hữu ích cho việc phát triển và sửa đổi các khuôn khổ bảo vệ dữ liệu trên toàn cầu.**

VẤN ĐỀ	PHƯƠNG PHÁP TỐT NHẤT
Phạm vi lãnh thổ	Các khuôn khổ bảo vệ dữ liệu phải điều chỉnh hành vi có tính kết nối đủ chặt chẽ với quốc gia. Luật này phải được áp dụng ở những nơi: (1) được nhắm mục tiêu cụ thể về dân cư; (2) dữ liệu cá nhân được xử lý phải được thu thập có chủ đích từ các chủ thể dữ liệu trong nước đó tại thời điểm thu thập; và (3) việc thu thập do một thức thể được thành lập tại quốc gia đó thực hiện thông qua một thỏa thuận ổn định, tạo ra mức độ hoạt động thức tế và hiệu quả.
Định nghĩa về dữ liệu cá nhân	Phạm vi thông tin được bao gồm trong định nghĩa dữ liệu cá nhân phải là thông tin có liên quan đến người tiêu dùng đã xác định hoặc có thể xác định được. Người tiêu dùng có thể xác định được là người tiêu dùng ta có thể xác định một cách trực tiếp hoặc gián tiếp thông qua nỗ lực hợp lý, bằng cách tham chiếu đến yếu tố nhận dạng như tên người tiêu dùng, số nhận dạng, dữ liệu vị trí, mã số nhận dạng trực tuyến hay một hoặc nhiều yếu tố cụ thể về đặc điểm cơ thể, sinh lý hoặc di truyền của người tiêu dùng đó. Phạm vi thông tin được bao gồm phải liên quan đến dữ liệu cá nhân mà nếu bị xử lý sai sẽ có tác động đáng kể đến quyền riêng tư của người tiêu dùng.. Không đưa vào phạm vi dữ liệu trong khuôn khổ những dữ liệu mất tính chất xác định thông qua các biện pháp kỹ thuật và tổ chức mạnh mẽ nhằm giảm đáng kể nguy cơ tái xác định.

VẤN ĐỀ	PHƯƠNG PHÁP TỐT NHẤT
Mối nguy hại	Các khuôn khổ bảo vệ dữ liệu cần tạo ra những phương pháp bảo vệ chống lại nguy cơ gây hại cho người tiêu dùng. Mối nguy hại có thể nhận biết được cần phản ánh tổn thương về thể chất, ảnh hưởng xấu đến sức khỏe, tổn thất về tài chính hoặc tiết lộ dữ liệu cá nhân nhạy cảm nằm ngoài kỳ vọng hợp lý của người tiêu dùng và có khả năng đáng kể sẽ để lại hậu quả bất lợi rõ ràng.
Tính minh bạch	Các đơn vị kiểm soát dữ liệu cần cung cấp tài liệu giải thích rõ ràng, dễ tìm đọc về phương pháp xử lý dữ liệu cá nhân, trong đó bao gồm những danh mục dữ liệu cá nhân họ thu thập, những loại bên thứ ba mà họ chia sẻ dữ liệu và nội dung mô tả quy trình các đơn vị này duy trì để xem xét, yêu cầu thay đổi, yêu cầu bản sao hoặc xóa dữ liệu cá nhân.
Nêu rõ mục đích	Dữ liệu cá nhân phải phù hợp với mục đích thu thập và thu được bằng những cách thức hợp pháp. Các đơn vị kiểm soát phải thông báo cho người tiêu dùng mục đích họ thu thập dữ liệu cá nhân và phải sử dụng dữ liệu cá nhân của người tiêu dùng theo đúng như đã giải thích, theo bối cảnh giao dịch hoặc kỳ vọng hợp lý của người tiêu dùng hoặc theo cách phù hợp với mục đích thu thập dữ liệu ban đầu. Các đơn vị kiểm soát phải ứng dụng các hệ thống quản lý nhằm đảm bảo dữ liệu cá nhân được sử dụng và chia sẻ theo đúng các mục đích đã nêu.
Chất lượng dữ liệu	Dữ liệu cá nhân phải phù hợp với mục đích sử dụng và trong phạm vi cần thiết nhằm phục vụ các mục đích đó, phải chính xác, đầy đủ và cập nhật.
Căn cứ xử lý	Các khuôn khổ bảo vệ dữ liệu phải công nhận và cho phép xử lý dữ liệu vì nhiều lý do hợp lệ, trong đó có mục đích kinh doanh chính đáng phù hợp với bối cảnh giao dịch hoặc kỳ vọng của người tiêu dùng. Các mục đích hợp lệ khác bao gồm công tác xử lý liên quan đến việc thực hiện hợp đồng; vì lợi ích công cộng hoặc lợi ích thiết yếu của người tiêu dùng; tính cần thiết nhằm tuân thủ nghĩa vụ pháp lý; hoặc được người tiêu dùng chấp thuận. Các khuôn khổ bảo vệ dữ liệu không được hạn chế những nỗ lực đảm bảo an ninh mạng chính đáng của các tổ chức; việc thực hiện các biện pháp phát hiện hoặc ngăn chặn hành vi đánh cắp hoặc gian lận danh tính; khả năng bảo vệ thông tin bí mật; hoặc việc thực hiện hoặc bảo vệ các khiếu nại pháp lý.
Sự chấp thuận	Các đơn vị kiểm soát phải cho phép người tiêu dùng đưa ra lựa chọn khi đã nắm đủ thông tin, đồng thời nếu thiết thức và phù hợp, phải cho người tiêu dùng có khả năng chọn không cho phép xử lý dữ liệu cá nhân của họ. Trong trường hợp có thể chấp thuận, sử chấp thuận phải được cung cấp vào thời điểm và theo phương thức phù hợp với bối cảnh giao dịch hoặc mối quan hệ của tổ chức với người tiêu dùng.
Xử lý dữ liệu cá nhân nhạy cảm	Một số loại dữ liệu, chẳng hạn như thông tin tài khoản giao dịch tài chính hoặc tình trạng sức khỏe, có thể mang tính chất đặc biệt nhạy cảm. Nếu việc xử lý dữ liệu nhạy cảm dẫn đến những rủi ro cao về quyền riêng tư, các đơn vị kiểm soát phải cho phép người tiêu dùng mà họ thu thập dữ liệu nhạy cảm khẳng định sử chấp thuận rõ ràng.

VẤN ĐỀ	PHƯƠNG PHÁP TỐT NHẤT
Khả năng kiểm soát của người tiêu dùng	Người tiêu dùng phải có quyền yêu cầu thông tin về việc các tổ chức có dữ liệu cá nhân liên quan đến họ hay không và dữ liệu đó mang tính chất gì. Họ phải có quyền thắc mắc về tính chính xác của dữ liệu đó, và nếu thích hợp thì yêu cầu sửa hoặc xóa dữ liệu. Người tiêu dùng cũng phải có quyền sở hữu bản sao dữ liệu cá nhân mà người tiêu dùng cung cấp cho tổ chức hoặc do người tiêu dùng tạo ra. Các tổ chức sẽ có quyền linh hoạt quyết định phương thức và dạng thức phù hợp để cung cấp thông tin này cho người tiêu dùng. Các đơn vị kiểm soát sẽ quyết định phương thức và mục đích xử lý dữ liệu cá nhân, đồng thời phải chịu trách nhiệm chính trong việc phản hồi các yêu cầu này. Các đơn vị kiểm soát có quyền từ chối yêu cầu khi áp lực hoặc chi phí đáp ứng yêu cầu là không hợp lý hoặc không cân xứng với những nguy cơ đối với quyền riêng tư của người tiêu dùng; để tuân thủ các yêu cầu pháp lý; để đảm bảo an ninh mạng; để thực hiện mục đích khác nhằm bảo vệ thông tin thương mại bí mật; để phục vụ mục đích nghiên cứu; hoặc để tránh vi phạm quyền riêng tư, quyền tự do ngôn luận hoặc các quyền khác của người tiêu dùng khác. Các đơn vị kiểm soát cũng cần thực hiện các quy trình xác minh an toàn để xác thực người tiêu dùng đưa ra yêu cầu nhằm loại bỏ nguy cơ gây thiệt hại do tiết lộ thông tin cho sai người.
Biện pháp bảo mật và việc thông báo trường hợp vi phạm	Các đơn vị kiểm soát và đơn vị xử lý phải sử dụng các biện pháp bảo mật hợp lý và thỏa đáng — tương ứng với khối lượng và mức độ nhạy cảm của dữ liệu, quy mô và độ phức tạp của doanh nghiệp cùng chi phí các công cụ có sẵn — được thiết kế nhằm ngăn chặn việc truy cập, phá hủy, sử dụng, sửa đổi và tiết lộ trái phép dữ liệu cá nhân. Các đơn vị kiểm soát phải thông báo cho người tiêu dùng càng sớm càng tốt nếu phát hiện tình huống vi phạm dữ liệu cá nhân liên quan đến việc thu được trái phép dữ liệu cá nhân chưa mã hóa hoặc chưa biên tập, ẩn chứa nguy cơ đáng kể xảy ra hành vi đánh cắp danh tính hoặc lừa đảo về tài chính. Những trường hợp vi phạm như vậy phải được báo cáo cho cơ quan giám sát một cách thường xuyên cùng với các biện pháp an ninh do các tổ chức thực hiện nhằm đáp ứng yêu cầu về trách nhiệm giải trình.
Yêu cầu về trách nhiệm giải trình	Các đơn vị kiểm soát phải xây dựng chính sách và thủ tục mang lại các biện pháp bảo vệ được nêu ở đây, bao gồm cả việc chỉ định người điều phối chương trình thực hiện các biện pháp bảo vệ này cũng như tiến hành huấn luyện và quản lý nhân viên; thường xuyên theo dõi và đánh giá việc thực hiện các chương trình đó; và khi cần thiết thì điều chỉnh các phương pháp giải quyết vấn đề phát sinh. Trong phạm vi áp dụng các biện pháp này, các đơn vị kiểm soát cần tiến hành đánh giá rủi ro định kỳ khi xử lý dữ liệu nhạy cảm, và khi xác định nguy cơ gây tổn hại đáng kể thì cần ghi lại việc thực hiện các biện pháp bảo vệ thích hợp. Chính phủ không nên áp đặt yêu cầu báo cáo đánh giá rủi ro hoặc tham vấn trước với cơ quan quản lý để tránh tạo gánh nặng hành chính không cần thiết và trì hoãn việc phân phối dịch vụ có giá trị mà không mang lại lợi ích tương ứng cho việc bảo vệ quyền riêng tư.

VẤN ĐỀ	PHƯƠNG PHÁP TỐT NHẤT
Truyền dữ liệu trên phạm vi quốc tế	Các khuôn khổ bảo vệ dữ liệu cần cho phép và khuyến khích các luồng dữ liệu di chuyển toàn cầu vì đây là yếu tố củng cố nền kinh tế toàn cầu. Các tổ chức truyền dữ liệu trên toàn cầu cần thực hiện các quy trình đảm bảo dữ liệu truyền ra ngoài quốc gia tiếp tục được bảo vệ. Khi có sự khác biệt giữa các hệ thống bảo vệ dữ liệu, các chính phủ nên tạo ra công cụ giúp thu hẹp khoảng cách sao cho có thể vừa bảo vệ quyền riêng tư vừa tạo điều kiện thuận lợi cho việc truyền dữ liệu trên phạm vi toàn cầu. Các khuôn khổ bảo vệ dữ liệu cần cấm các yêu cầu bản địa hóa dữ liệu ở cả khu vực công và tư vì làm như vậy có thể làm thất bại những nỗ lực thực hiện các biện pháp an ninh, cản trở quá trình đổi mới kinh doanh và giới hạn các dịch vụ có thể cung cấp cho người tiêu dùng.
Nghĩa vụ của các đơn vị kiểm soát và đơn vị xử lý/ Phân bổ trách nhiệm pháp lý	Các đơn vị kiểm soát dữ liệu, chính là đơn vị quyết định phương thức và mục đích xử lý dữ liệu cá nhân, phải là bên chịu trách nhiệm chính trong việc đảm bảo thực hiện các nghĩa vụ về bảo mật và quyền riêng tư theo pháp luật. Các đơn vị xử lý dữ liệu, là đơn vị phụ trách xử lý dữ liệu thay mặt cho các đơn vị kiểm soát, phải chịu trách nhiệm tuân theo hướng dẫn của đơn vị kiểm soát theo thỏa thuận hợp đồng giữa các bên. Các đơn vị kiểm soát dữ liệu và đơn vị xử lý dữ liệu cần có sự linh hoạt trong việc thương lượng điều khoản hợp đồng riêng mà không cần dùng những từ ngữ mang tính chất bắt buộc, quy định của pháp luật.
Biện pháp khắc phục và hình phạt	Một đơn vị điều tiết trung tâm phải có các công cụ và nguồn lực cần thiết để đảm bảo thực thi hiệu quả. Các biện pháp khắc phục và hình phạt phải thích đáng với tác hại của việc vi phạm các luật về bảo vệ dữ liệu. Không nên phạt dân sự tùy tiện hay dựa vào các yếu tố thiếu tính kết nối đáng kể với bối cảnh xảy ra mối nguy hại tiềm ẩn. Hình phạt hình sự không phải là biện pháp thỏa đáng đối với hành vi vi phạm các luật về bảo vệ dữ liệu.