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.