ỦY BAN NHÂN DÂN TỈNH BÌNH PHƯỚC	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 3857 /UBND-NC V/v tăng cường công tác bảo vệ dữ liệu cá nhân	*Bình Phước, ngày 20 tháng 9 năm 2024*

Kính gửi:
- Các sở, ban, ngành, đoàn thể;
- UBND các huyện, thị xã, thành phố.

Ngày 17/4/2023, Chính phủ đã ban hành Nghị định số 13/2023/NĐ-CP về về bảo vệ dữ liệu cá nhân (Nghị định số 13/2023/NĐ-CP) gồm 04 chương, 44 điều, quy định đầy đủ các vấn đề liên quan tới bảo vệ dữ liệu cá nhân của cơ quan, tổ chức, cá nhân có liên quan. Nghị định đã xác lập quyền, nghĩa vụ của chủ thể dữ liệu; quy định về quy trình, cách thức áp dụng các biện pháp bảo vệ dữ liệu cá nhân của cơ quan, tổ chức, cá nhân có liên quan; xác định cơ quan chuyên trách bảo vệ dữ liệu cá nhân; lực lượng bảo vệ dữ liệu cá nhân; Cổng thông tin quốc gia về bảo vệ dữ liệu cá nhân; thủ tục hành chính về bảo vệ dữ liệu cá nhân.

Ngày 13/9/2023, UBND tỉnh đã ban hành Kế hoạch số 290/KH-UBND về triển khai thực hiện Nghị định số 13/2023/NĐ-CP trên địa bàn tỉnh. Đến nay, các cơ quan, đơn vị, địa phương đã chủ động xây dựng kế hoạch và tổ chức quán triệt, triển khai các nội dung của Nghị định tới toàn thể cán bộ, công chức, viên chức, đồng thời tiến hành rà soát, đánh giá, phân loại dữ liệu cá nhân và xác định nội dung, biện pháp bảo vệ dữ liệu. Tuy nhiên, việc quán triệt, triển khai thực hiện Nghị định ở một số cơ quan, đơn vị, địa phương còn chậm, chưa nêu cụ thể nhiệm vụ, giải pháp thực hiện, chế độ báo cáo chưa kịp thời dẫn đến khó khăn trong quá trình thống kê, đánh giá; ý thức của một bộ phận cán bộ, đảng viên chưa cao, chưa có biện pháp quản lý và kỹ thuật phù hợp để bảo vệ dữ liệu cá nhân; các tổ chức, doanh nghiệp thực hiện các hoạt động thu thập, lưu trữ, xử lý dữ liệu cá nhân của người dùng chưa áp dụng giải pháp kỹ thuật đủ mức để chống lộ lọt thông tin cũng như quy trình xử lý sự cố khi bị lộ, mất dữ liệu cá nhân.

Để quán triệt, triển khai thực hiện nghiêm túc các quy định của Nghị định số 13/2023/NĐ-CP trong các hoạt động có liên quan dữ liệu cá nhân trên địa bàn tỉnh; Chủ tịch UBND tỉnh yêu cầu Thủ trưởng các sở, ban, ngành, đoàn thể tỉnh; Chủ tịch UBND các huyện, thị xã, thành phố tập trung chỉ đạo, thực hiện các nội dung sau:

1. Nghiên cứu, tổ chức triển khai, thực hiện nghiêm các quy định về bảo vệ dữ liệu cá nhân qua nhiều hình thức khác nhau, trong đó chú trọng tổ chức phổ biến, quán triệt tới toàn bộ cán bộ, công chức, viên chức về quyền và nghĩa vụ, xác định trách nhiệm cần triển khai thực hiện, bảo đảm về tiến độ, thời gian theo quy định của pháp luật.

2. Chỉ đạo các đơn vị có hoạt động thu thập, xử lý dữ liệu cá nhân tiến hành rà soát tổng thể, phân loại dữ liệu cá nhân đã thu thập, đang xử lý, từ đó

xác định trách nhiệm bảo vệ tương ứng với từng loại dữ liệu cá nhân theo quy định của Nghị định số 13/2023/NĐ-CP.

3. Rà soát, đánh giá quy trình thu thập, xử lý dữ liệu cá nhân, đánh giá hiện trạng bảo vệ dữ liệu cá nhân (bao gồm các nội dung: chính sách, kỹ thuật, nhân lực, công nghệ) để đề xuất ban hành các biện pháp quản lý phù hợp với quy mô, mức độ xử lý dữ liệu cá nhân của cơ quan, đơn vị; xử lý nghiêm các hành vi chuyển giao dữ liệu cá nhân trái phép, mua bán dữ liệu cá nhân trái quy định của pháp luật.

4. Chỉ định *(bằng văn bản có hiệu lực pháp lý)* bộ phận có chức năng bảo vệ dữ liệu cá nhân, chỉ định nhân sự phụ trách bảo vệ dữ liệu cá nhân nếu cơ quan, tổ chức, cá nhân xử lý dữ liệu cá nhân nhạy cảm và trao đổi 01 bản chính văn bản nêu trên về Cơ quan chuyên trách bảo vệ dữ liệu cá nhân (qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Công an tỉnh).

5. Thông báo vi phạm quy định về bảo vệ dữ liệu cá nhân trong trường hợp phát hiện xảy ra vi phạm quy định bảo vệ dữ liệu cá nhân về Cơ quan chuyên trách bảo vệ dữ liệu cá nhân chậm nhất 72 giờ sau khi xảy ra hành vi vi phạm theo Mẫu số 03 tại Phụ lục của Nghị định số 13/2023/NĐ-CP.

6. Lập hồ sơ đánh giá tác động xử lý dữ liệu cá nhân, hồ sơ đánh giá tác động truyền dữ liệu cá nhân ra nước ngoài và gửi Cơ quan chuyên trách bảo vệ dữ liệu cá nhân theo 02 hình thức: trực tiếp tại Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Công an tỉnh hoặc theo đường bưu chính sau 60 ngày kể từ ngày xử lý dữ liệu cá nhân hoặc chuyển dữ liệu cá nhân ra nước ngoài.

7. Áp dụng các biện pháp bảo vệ dữ liệu cá nhân (bao gồm cả biện pháp kỹ thuật, tuân thủ, hành chính) phù hợp, tương xứng với mức độ bảo vệ của tổ chức, doanh nghiệp, tầm quan trọng của dữ liệu hoặc các tiêu chuẩn mà tổ chức, doanh nghiệp cần đáp ứng.

8. Công an tỉnh phối hợp với các sở, ban, ngành, đoàn thể tỉnh, UBND các huyện, thị xã, thành phố tăng cường triển khai công tác tuyên truyền, hướng dẫn bảo vệ dữ liệu cá nhân; đồng thời, triển khai đấu tranh với hoạt động chuyển giao trái phép, mua bán dữ liệu cá nhân, xử lý nghiêm các hành vi vi phạm theo quy định của pháp luật.

Yêu cầu các cơ quan, đơn vị, địa phương nhanh chóng triển khai, thực hiện. Trong quá trình thực hiện nếu có khó khăn, vướng mắc báo cáo UBND tỉnh (qua Công an tỉnh, số điện thoại: 0693.460.505) để được hướng dẫn.

(Gửi kèm: Phụ lục một số nội dung chi tiết liên quan đến công tác bảo vệ dữ liệu cá nhân)./.

Nơi nhận:
- CT, PCT UBND tỉnh;
- Như trên;
- LĐVP, PNC;
- Lưu: VT, TH106-CV.

CHỦ TỊCH

Trần Tuệ Hiền

PHỤ LỤC

Một số nội dung chi tiết liên quan đến công tác bảo vệ dữ liệu cá nhân

(Kèm theo Công văn số: 3857../UBND-NC ngày 20../9/2024 của UBND tỉnh)

1. Xác định các nội dung cần triển khai cho các tổ chức, doanh nghiệp (05 bước)

Bước 1: Tổ chức tuyên truyền, phổ biến về nội dung bảo vệ dữ liệu cá nhân cho các tổ chức, doanh nghiệp, cá nhân. Cá nhân nắm được các quyền và nghĩa vụ bảo vệ dữ liệu cá nhân của mình. Các tổ chức, doanh nghiệp nắm được trách nhiệm tuân thủ dựa trên các vai trò trong luồng xử lý dữ liệu cá nhân. Công an tỉnh tham mưu tổ chức hội nghị, các buổi tuyên truyền, hướng dẫn trên địa bàn, phổ biến nội dung phù hợp với từng đối tượng, loại hình tổ chức, doanh nghiệp cụ thể.

Bước 2: Đánh giá tuân thủ về bảo vệ dữ liệu cá nhân trên 03 khía cạnh: công nghệ (hệ thống kỹ thuật), quy trình (chức năng, nhiệm vụ và quy trình xử lý dữ liệu), chính sách (các văn bản chính sách mà tổ chức, doanh nghiệp) đang áp dụng. Trên cơ sở đó, xác định các vấn đề mà tổ chức, cá nhân đang còn thiếu sót, cần bổ sung và áp dụng.

Bước 3: Xây dựng, hoàn thiện quy trình, quy định, chính sách bảo vệ dữ liệu cá nhân. Nghiên cứu, bổ sung, ban hành các quy định (hồ sơ, hợp đồng, văn bản, thỏa thuận, quy chế, quy định, khung chính sách nội bộ); áp dụng các biện pháp kỹ thuật (bảo vệ, kiểm tra, đánh giá, khắc phục sự cố, phòng, chống tấn công) tùy theo quy mô của từng tổ chức, doanh nghiệp.

Bước 4: Chỉ định bộ phận bảo vệ dữ liệu cá nhân nếu có xử lý dữ liệu cá nhân nhạy cảm. Áp dụng biện pháp bảo vệ dữ liệu cá nhân dựa trên kết quả đánh giá tuân thủ.

Bước 5: Thực hiện thủ tục hành chính về bảo vệ dữ liệu cá nhân, đánh giá tác động xử lý dữ liệu cá nhân như một bản cam kết trước pháp luật về hoạt động xử lý dữ liệu cá nhân của tổ chức, doanh nghiệp mình. Đồng thời, triển khai tổng thể các giải pháp bảo vệ dữ liệu cá nhân. Thông báo xảy ra vi phạm với Cơ quan chuyên trách bảo vệ dữ liệu cá nhân khi xảy ra vấn đề.

2. Về xác định các nội dung cần triển khai trong đánh giá tuân thủ liên quan tới hệ thống kỹ thuật nhằm bảo vệ dữ liệu cá nhân

- Xác định vị trí lưu trữ dữ liệu (Data Matrix): giúp thực hiện các biện pháp bảo vệ, quy trình, chính sách và tác vụ liên quan tới dữ liệu cá nhân.

- Xác định Sơ đồ luồng dữ liệu (Data Flow Diagram): chỉ ra nguồn gốc, các bên tham gia vào quá trình xử lý dữ liệu cá nhân.

- Xác định Sơ đồ mạng (Network Diagram): chỉ ra các vùng mạng cần phải quan tâm bảo vệ hơn do nơi đó có các hệ thống có xử lý dữ liệu cá nhân.

- Xác định nơi chứa thông tin chi tiết về các thành phần thuộc các hệ thống

có tham gia vào quá trình xử lý dữ liệu hoặc có thể tác động đến an ninh an toàn của dữ liệu cá nhân.

- Xác định phạm vi cần tuân thủ: xác định phạm vi cần tuân thủ hoặc là chỉ xem xét các hệ thống có xử lý dữ liệu cá nhân hoặc mở rộng ra xem xét các hệ thống có kết nối đến hoặc có thể tác động đến an ninh mạng của các hệ thống xử lý dữ liệu cá nhân.

- Xác định danh mục tuân thủ (List of Requirement): liệt kê các yêu cầu mà tổ chức phải hoặc nên triển khai áp dụng, gồm có các yêu cầu của Nghị định 13/2023/NĐ-CP hoặc các văn bản luật liên quan hoặc các tiêu chuẩn quốc tế có thể áp dụng.

- Xác định mẫu và xây dựng báo cáo đánh giá tuân thủ (Gap & Remediate): xác định mẫu đánh giá theo tiêu chuẩn lấy mẫu. Nơi ghi nhận các điểm phát hiện, các phương án khuyến nghị khắc phục phải/nên bổ sung để tuân thủ Nghị định 13/2023/NĐ-CP. Từ đó, xây dựng báo cáo đánh giá tuân thủ.

3. Về xác định các biện pháp quản lý theo Nghị định số 13/2023/NĐ-CP

Nghị định số 13/2023/NĐ-CP không đưa ra các biện pháp quản lý cụ thể nhằm tạo sự linh hoạt trong bảo vệ dữ liệu cá nhân của các tổ chức, doanh nghiệp. Tùy thuộc vào quy mô, tài chính của doanh nghiệp để có mức áp dụng phù hợp. Các biện pháp nêu dưới đây nhằm mục đích khuyến khích theo tiêu chuẩn chung nhằm bảo đảm phù hợp với tình hình, thực trạng của các doanh nghiệp tại Việt Nam.

Các tổ chức, doanh nghiệp có thể nghiên cứu áp dụng các biện pháp quản lý như sau: (1) phân loại và kiểm kê dữ liệu dựa trên độ nhạy cảm của nó (ví dụ: công khai, nội bộ, bí mật) giúp ưu tiên triển khai các biện pháp bảo vệ cho mức độ quan trọng của dữ liệu; (2) kiểm soát truy cập nhằm hạn chế quyền truy cập vào dữ liệu cá nhân dựa trên vai trò và quyền nhằm ngăn chặn người dùng trái phép truy cập thông tin nhạy cảm; (3) mã hoá dữ liệu ở trạng thái nghỉ (được lưu trữ) và đang truyền (trong quá trình truyền); (4) ẩn danh: thay thế thông tin nhận dạng bằng mã định danh duy nhất nhằm giảm rủi ro nhận dạng trực tiếp, đồng thời cho phép phân tích dữ liệu; (5) kiểm tra và đánh giá thường xuyên nhằm xác định các lỗ hổng và đảm bảo tuân thủ các quy định bảo vệ dữ liệu; (6) kế hoạch ứng phó sự cố: xây dựng kế hoạch xử lý các sự cố hoặc vi phạm dữ liệu cho phép phản hồi nhanh chóng, giảm thiểu thiệt hại và thông báo cho các bên bị ảnh hưởng; (7) đánh giá tác động đến quyền riêng tư (PIA) hoặc đánh giá tuân thủ bảo vệ dữ liệu cá nhân (GAP) giúp xác định và giảm thiểu rủi ro sớm trong vòng đời dự án; (8) xử lý dữ liệu an toàn, đúng cách (ví dụ: băm nhỏ tài liệu vật lý, xóa bộ nhớ kỹ thuật số) giúp ngăn chặn truy cập trái phép vào dữ liệu bị loại bỏ; (9) đào tạo và nâng cao nhận thức của nhân viên về các chính sách bảo vệ dữ liệu và các phương pháp tốt nhất; (10) quản lý rủi ro nhà cung cấp nhằm đánh giá và quản lý rủi ro liên quan đến nhà cung cấp, bên thứ ba; (11) triển khai các biện pháp an ninh vật lý như bảo mật trung tâm dữ liệu, máy chủ và bộ nhớ vật lý ngăn chặn truy cập trái phép vào phần cứng chứa dữ liệu cá nhân.

4. Về xác định các biện pháp kỹ thuật theo Nghị định số 13/2023/NĐ-CP

Nghị định số 13/2023/NĐ-CP không đưa ra các biện pháp kỹ thuật cụ thể nhằm tạo sự linh hoạt trong bảo vệ dữ liệu cá nhân của các tổ chức, doanh nghiệp. Tùy thuộc vào quy mô, tài chính của doanh nghiệp để có mức áp dụng phù hợp. Các biện pháp nêu dưới đây nhằm mục đích khuyến khích theo tiêu chuẩn chung nhằm bảo đảm phù hợp với tình hình, thực trạng của các doanh nghiệp tại Việt Nam. Về giải pháp kỹ thuật, các tổ chức, doanh nghiệp cân nhắc triển khai các biện pháp sau: (1) phân tích rủi ro: bắt đầu bằng cách đánh giá rủi ro liên quan đến việc xử lý dữ liệu cá nhân nhằm xác định mối đe dọa tiềm ẩn và lỗ hổng cụ thể đối với tổ chức, doanh nghiệp; (2) có chính sách bảo mật thông tin nêu rõ các mục tiêu, trách nhiệm và quy trình bảo mật để bảo vệ dữ liệu cá nhân; (3) sử dụng tường lửa để kiểm soát lưu lượng mạng và ngăn chặn truy cập trái phép vào hệ thống; (4) phần mềm chống vi-rút: thường xuyên quét hệ thống để tìm phần mềm độc hại và vi-rút, luôn cập nhật phần mềm chống vi-rút để phát hiện và loại bỏ các mối đe dọa; (5) mã hóa: mã hóa dữ liệu nhạy cảm cả khi truyền (sử dụng các giao thức như HTTPS) và khi lưu trữ (lưu trữ dữ liệu một cách an toàn), bảo đảm ngay cả khi dữ liệu bị chặn, dữ liệu vẫn không thể đọc được nếu không có khóa giải mã; (6) ẩn danh hoặc đặt biệt danh cho dữ liệu cá nhân nếu có thể, thay thế thông tin nhận dạng bằng mã định danh duy nhất, giảm nguy cơ nhận dạng trực tiếp; (7) kiểm soát truy cập: giới hạn quyền truy cập vào dữ liệu cá nhân dựa trên vai trò và trách nhiệm, triển khai các cơ chế xác thực mạnh mẽ (ví dụ: xác thực đa yếu tố) để ngăn chặn truy cập trái phép; (8) sao lưu và phục hồi: thường xuyên sao lưu dữ liệu và thiết lập quy trình khôi phục đáng tin cậy, đảm bảo rằng các bản sao lưu được an toàn và có thể truy cập được trong trường hợp có sự cố; (9) giám sát và ghi nhật ký: theo dõi nhật ký hệ thống để phát hiện các hoạt động đáng ngờ, ghi nhật ký giúp theo dõi ai đã truy cập dữ liệu và khi nào, hỗ trợ điều tra sự cố; (10) kiểm tra thường xuyên: tiến hành đánh giá bảo mật, quét lỗ hổng và kiểm tra thâm nhập, xác định điểm yếu và giải quyết chúng kịp thời; (11) quản lý bản và: luôn cập nhật phần mềm và hệ thống bằng các bản và bảo mật, những kẻ tấn công có thể khai thác các lỗ hổng trong phần mềm lỗi thời; (12) bảo mật vật lý: bảo mật quyền truy cập vật lý vào máy chủ, trung tâm dữ liệu và thiết bị lưu trữ, chỉ giới hạn quyền vào cho những người có thẩm quyền.

5. Về xây dựng Sơ đồ luồng xử lý dữ liệu cá nhân theo Nghị định số 13/2023/NĐ-CP

Việc xây dựng Sơ đồ luồng xử lý dữ liệu cá nhân không nằm trong quy định của Nghị định số 13/2023/NĐ-CP, nhưng là phương pháp kỹ thuật tiêu chuẩn nhất trong giai đoạn hiện nay giúp tổ chức, doanh nghiệp xác định chính xác vai trò, trách nhiệm của mình và các bên có liên quan trong xử lý dữ liệu cá nhân. Trong các báo cáo đánh giá tuân thủ, việc xây dựng Sơ đồ luồng xử lý dữ liệu cá nhân đóng vai trò quan trọng khi đưa ra các nhận xét, đánh giá, khuyến nghị.

Để xây dựng được sơ đồ luồng xử lý dữ liệu cá nhân, các tổ chức, doanh nghiệp vẽ sơ đồ theo các nội dung: mô hình tổ chức; vai trò xử lý dữ liệu cá nhân

của từng bộ phận trong mô hình tổ chức; xác định ngành nghề, lĩnh vực kinh doanh; xác định sản phẩm, dịch vụ kinh doanh dựa trên ngành nghề, lĩnh vực kinh doanh; xác định loại hình hợp đồng mà sản phẩm, dịch vụ đó kinh doanh; xác định mục đích xử lý dữ liệu cá nhân theo loại hình hợp đồng; xác định hoạt động xử lý dữ liệu cá nhân theo mục đích xử lý dữ liệu cá nhân.

6. Về việc phối hợp triển khai công tác bảo vệ dữ liệu cá nhân

- Chức năng quản lý nhà nước về bảo vệ dữ liệu cá nhân. Chính phủ giao Bộ Công an thống nhất quản lý nhà nước về bảo vệ dữ liệu cá nhân; giao Cơ quan chuyên trách bảo vệ dữ liệu cá nhân (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an) có trách nhiệm giúp Bộ Công an thực hiện quản lý nhà nước về bảo vệ dữ liệu cá nhân.

- Việc tiếp nhận và xử lý thủ tục hành chính liên quan bảo vệ dữ liệu cá nhân được thực hiện qua 03 hình thức: trực tiếp và bưu chính (tại Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Bộ Công an, qua Bộ phận Tiếp nhận và Trả kết quả về bảo vệ dữ liệu cá nhân, E2 Dương Đình Nghệ, Dịch Vọng Hậu, Cầu Giấy, Hà Nội hoặc Phòng an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao Công an tỉnh Bình Phước, số 12 Trần Hưng Đạo, phường Tân Phú, thành phố Đồng Xoài, tỉnh Bình Phước; trực tuyến: tại Cổng thông tin quốc gia về bảo vệ dữ liệu cá nhân (pdp.gov.vn, baovedlcn.gov.vn) sau khi Cổng thông tin được công bố và chính thức đi vào hoạt động.

- Về việc phối hợp thực hiện các hoạt động liên quan tới triển khai bảo vệ dữ liệu cá nhân: Công an tỉnh là đầu mối phối hợp với các sở, ban, ngành, đoàn thể tỉnh; UBND các huyện, thị xã, thành phố trong các hoạt động liên quan triển khai công tác bảo vệ dữ liệu cá nhân trên địa bàn toàn tỉnh./.