ỦY BAN NHÂN DÂN
HUYỆN NHÀ BÈ
TRƯỜNG TIỂU HỌC TẠ UYÊN

Số: 292 /KH-THTU

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Nhà Bè, ngày 10 tháng 10 năm 2024

KẾ HOẠCH
Triển khai thực hiện Nghị định số 13/2023/NĐ-CP ngày 17 tháng 4 năm 2023 của Chính phủ về bảo vệ dữ liệu cá nhân

Thực hiện Kế hoạch số 1707/KH-GDĐT ngày 04 tháng 10 năm 2024 của Phòng Giáo dục và Đào tạo huyện Nhà Bè triển khai thực hiện Nghị định số 13/2023/NĐ-CP ngày 17 tháng 4 năm 2023 của Chính phủ về bảo vệ dữ liệu cá nhân trên địa bàn huyện Nhà Bè;

Trường Tiểu học Tạ Uyên xây dựng kế hoạch triển khai thực hiện với các nội dung như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

Triển khai thực hiện nghiêm túc, hiệu quả các quy định về bảo vệ dữ liệu cá nhân trên môi trường mạng theo Nghị định số 13/2023/NĐ-CP ngày 17 tháng 4 năm 2023 của Chính phủ về Bảo vệ dữ liệu cá nhân (sau đây gọi tắt là Nghị định số 13); nâng cao nhận thức, trách nhiệm của viên chức, người lao động có liên quan đến hoạt động xử lý dữ liệu cá nhân trong việc bảo vệ dữ liệu cá nhân trên môi trường mạng.

2. Yêu cầu

Tăng cường công tác quản lý thông tin liên quan đến dữ liệu cá nhân trên môi trường mạng; phân công cụ thể nhiệm vụ từng thành viên trong nhà trường để tổ chức triển khai thực hiện đảm bảo hiệu quả.

Bảo đảm sự phối hợp chặt chẽ giữa nhà trường và các cơ quan chức năng trong công tác quản lý thông tin liên quan đến dữ liệu cá nhân trên môi trường mạng; kịp thời đôn đốc, hướng dẫn và tháo gỡ những khó khăn, vướng mắc trong quá trình tổ chức triển khai thực hiện.

II. NỘI DUNG CÔNG TÁC TRỌNG TÂM

1. Tuyên truyền, phổ biến, quán triệt và triển khai thực hiện Nghị định số 13/2023/NĐ-CP tại trường bằng hình thức phù hợp; đồng thời tuyên truyền, phổ biến trên thông tin điện tử, mạng xã hội để toàn thể viên chức, người lao động và học sinh biết, thực hiện theo đúng quy định, nhất là phổ biến các kiến thức, kỹ năng nhằm bảo vệ dữ liệu cá nhân.

2. Hoạt động thu thập, xử lý dữ liệu cá nhân tại trường

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.

Rà soát, đánh giá quy trình thu thập, xử lý dữ liệu cá nhân, đề xuất ban hành các biện pháp quản lý phù hợp với quy mô, mức độ xử lý dữ liệu cá nhân của viên chức, người lao động, học sinh; xử lý nghiêm các hành vi chuyển giao dữ liệu cá nhân trái phép, mua bán dữ liệu cá nhân nếu phát hiện.

Phân công nhân sự phụ trách bảo vệ dữ liệu cá nhân bằng văn bản có hiệu lực pháp lý.

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.

3. Triển khai, thực hiện các quy định về bảo vệ dữ liệu cá nhân trong nhà trường; kịp thời phát hiện, ngăn chặn các hoạt động chuyển giao trái phép, mua bán dữ liệu cá nhân và xử lý nghiêm các hành vi vi phạm về bảo vệ dữ liệu cá nhân theo quy định pháp luật.

III. TỔ CHỨC THỰC HIỆN

1. Hiệu trưởng

Xây dựng kế hoạch triển khai thực hiện đến toàn thể cán bộ, giáo viên, người lao động trong nhà trường.

Tăng cường công tác quản lý nhà nước đối với bảo vệ dữ liệu cá nhân tại trường theo đúng quy định của pháp luật về bảo vệ dữ liệu cá nhân. Phân công viên chức triển khai thực hiện nhiệm vụ theo dõi, hướng dẫn bảo vệ dữ liệu cá nhân tại đơn vị.

Phối hợp Công an xã Phước Kiển triển khai công tác bảo vệ dữ liệu cá nhân trên lĩnh vực giáo dục, đào tạo.

2. Phó hiệu trưởng

Phổ biến nội dung, quy định của Nghị định số 13/2023/NĐ-CP tại đơn vị về bảo vệ dữ liệu cá nhân để thực hiện theo đúng quy định; tham mưu xây dựng và triển khai thực hiện các quy định, nhiệm vụ bảo vệ dữ liệu cá nhân tại đơn vị theo quy định tại Nghị định số 13/2023/NĐ-CP.

3. Đoàn thể

Phối hợp nhà trường tuyên truyền phổ biến nội dung, quy định của Nghị định số 13/2023/NĐ-CP đến CB, GV, NV biết các quy định về bảo vệ dữ liệu cá nhân để thực hiện theo đúng quy định; xây dựng và triển khai thực hiện các quy định, nhiệm vụ bảo vệ dữ liệu cá nhân đến công đoàn viên, đoàn viên theo quy định tại Nghị định số 13/2023/NĐ-CP thông qua các buổi sinh hoạt, các buổi họp định kỳ.

4. Giáo viên

Tuyên truyền, phổ biến nội dung quy định của Nghị định số 13/2023/NĐ-CP phù hợp với lứa tuổi đến phụ huynh và học sinh.

Lồng ghép giáo dục kĩ năng công dân số để học sinh biết bảo vệ các thông tin cá nhân.

Trên đây là Kế hoạch Kế hoạch triển khai thực hiện Nghị định số 13/2023/NĐ-CP ngày 17 tháng 4 năm 2023 của Chính phủ về bảo vệ dữ liệu cá của Trường Tiểu học Tạ Uyên./.

Nơi nhận:
- Phòng GDĐT "để báo cáo";
- CB, GV, NV "để thực hiện";
- Lưu: VT.

HIỆU TRƯỞNG

ỦY BAN NHÂN DÂN HUYỆN NHÀ BÈ TP. HỒ CHÍ MINH
TRƯỜNG TIỂU HỌC TẠ UYÊN

Lê Văn Hòa

ỦY BAN NHÂN DÂN
HUYỆN NHÀ BÈ
TRƯỜNG TIỂU HỌC TẠ UYÊN

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

PHỤ LỤC
Biện pháp, giải pháp triển khai công tác bảo vệ dữ liệu cá nhân theo Nghị định số 13/2023/ND-CP của Chính phủ

(Kèm theo Kế hoạch số 292 /KH-THTU ngày 10 tháng 10 năm 2024 của Trường Tiểu học Tạ Uyên)

1. Xác định các nội dung cần triển khai cho các cơ quan, tổ chức, doanh nghiệp, cá nhân

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.

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

Quy trình như sau:

- 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 ra các yêu cầu mà tổ chức phải hoặc nên triển khai áp dụng, gồm có các yêu cầu của Nghị định số 13 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 số 13. Trên cơ sở đó, xây dựng báo cáo đánh giá tuân thủ.

3. Về xác định các biện pháp quản lý theo Nghị định số 13

Nghị định số 13 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:

- 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;

- 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;

- Mã hoá dữ liệu ở trạng thái nghỉ (được lưu trữ) và đang truyền (trong quá trình truyền);

- 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;

- 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;

- 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;

- 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;

- 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;

- Đào tạo và nâng cao nhận thức của nhân viên về các chính sách bảo vệ dữ liệu và các phương pháp tốt nhất;

- Quản lý rủi ro nhà cung cấp nhằm đánh giá và quản lý rủi ro liên quan đến nhà cung cấp, bên thứ ba;

- 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

Nghị định số 13 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:

- 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;

- 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;

- Sử dụng tường lửa để kiểm soát lưu lượng mạng và ngăn chặn truy cập trái phép vào hệ thống;

- 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;

- 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;

- 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;

- 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;

- 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;

- 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;

- 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;

- Quản lý bản vá: Luôn cập nhật phần mềm và hệ thống bằng các bản vá bảo mật, những kẻ tấn công có thể khai thác các lỗ hổng trong phần mềm lỗi thời;

- 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

- Việc xây dựng Sơ đồ luồng xử lý dữ liệu cá nhân không nằm trong quy định của Nghị định số 13, 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./.