CẬP NHẬT PHÁP LÝ HẰNG THÁNG
MONTHLY LEGAL UPDATE
4/2023

[English down below]

NGHỊ ĐỊNH 13/2023/NĐ-CP VỀ BẢO VỆ DỮ LIỆU CÁ NHÂN

Ngày 17/4/2023, Chính phủ đã ban hành Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân ("Nghị định 13") đã tạo nên một văn bản pháp lý hợp nhất và toàn diện đầu tiên về bảo vệ dữ liệu cá nhân tại Việt Nam. Nghị định 13 sẽ có hiệu lực thi hành kể từ ngày 1/7/2023 và sẽ có những tác động đáng kể đến hoạt động của công ty nói chung, cũng như hoạt động xử lý dữ liệu nói riêng của các phòng ban liên quan.

A. NHỮNG NỘI DUNG CHỦ YẾU CỦA NGHỊ ĐỊNH 13

1. Xác định vai trò trong quá trình xử lý dữ liệu cá nhân

Nghị định 13 phân biệt rõ ràng các vai trò khác nhau của các bên tham gia vào xử lý dữ liệu và quy định trách nhiệm riêng cho từng vai trò. Cụ thể:

Bên Kiểm soát dữ liệu cá nhân là tổ chức, cá nhân quyết định mục đích và phương tiện xử lý dữ liệu cá nhân. Bên kiểm soát dữ liệu đóng vai trò lớn hơn trong việc thông báo và hợp tác với cơ quan nếu có sự vi phạm dữ liệu cá nhân. Là người chịu trách nhiệm cuối cùng trước chủ thể dữ liệu và có nghĩa vụ chứng minh rằng đã có được sự đồng ý trước cho tất cả hoạt động xử lý.

Bên Xử lý dữ liệu cá nhân là tổ chức, cá nhân thực hiện việc một hoặc nhiều hoạt động tác động tới dữ liệu cá nhân, như: thu thập, ghi, phân tích, xác nhận, lưu trữ, chỉnh sửa, công khai, kết hợp, truy cập, truy xuất, thu hồi, mã hóa, giải mã, sao chép, chia sẻ, truyền đưa, cung cấp, chuyển giao, xóa, hủy dữ liệu cá nhân hoặc các hành động khác có liên quan. Thay mặt cho Bên Kiểm soát dữ liệu, thông qua một hợp đồng hoặc thỏa thuận với Bên Kiểm soát dữ liệu.

Bên Kiểm soát và xử lý dữ liệu cá nhân là tổ chức, cá nhân đồng thời quyết định mục đích, phương tiện và trực tiếp xử lý dữ liệu cá nhân.

Bên thứ ba là tổ chức, cá nhân không phải các đối tượng nêu trên nhưng được phép xử lý dữ liệu cá nhân. Định nghĩa này có thể mở rộng sang bất kỳ các bên tham gia vào việc xử lý dữ liệu cá nhân như: Cung cấp dịch vụ thanh toán, dịch vụ viễn thông.

Dẫn chiếu đến trường hợp của Daikin, hoạt động thu thập, quản lý, lưu trữ, xử lý thông tin được diễn ra thường xuyên. Đơn cử như việc vận hành công việc của các phòng ban như: phòng Nhân sự thu thập thông tin Người lao động, sau đó chuyển dữ liệu lên trang E-Office; Khối Service, Phòng Marketing, Call center thu thập thông tin của khách hàng,...Do đó, về vai trò, Công ty được xác định là Bên Kiểm soát dữ liệu cá nhân hoặc Bên kiểm soát và xử lý dữ liệu cá nhân; các phòng, ban có liên quan đến hoạt động thu thập, quản lý,... dữ liệu cá nhân là Bên xử lý dữ liệu; các đơn vị cung cấp dịch vụ viễn thông, bưu chính,... có thể

Lưu ý/*Note*

Để được hỗ trợ thêm, vui lòng liên hệ/ *for further support, please contact to*:
Anh Thư, Phòng Pháp lý/Legal Department: 028.62.504.888 (ext: 68414), email:
anhthu.bui@daikin.com.vn

hiểu là Bên thứ ba. Mỗi chủ thể cần phải xác định đúng (các) vai trò của mình và tuân thủ các nghĩa vụ khác nhau được áp dụng tương ứng với từng vai trò theo Nghị định 13.

2. Xác định dữ liệu cá nhân được xử lý

Dữ liệu cá nhân là các thông tin liên quan đến một con người cụ thể hoặc giúp xác định một con người cụ thể khi các thông tin này được sử dụng độc lập hoặc kết hợp với các thông tin khác có thể là thông tin trực tiếp, chữ số, chữ viết, hình ảnh, âm thanh, video và dữ liệu kỹ thuật số.

Nghị định 13 phân loại dữ liệu cá nhân thành hai (2) loại: (i) dữ liệu cá nhân cơ bản và (ii) dữ liệu cá nhân nhạy cảm; đồng thời liệt kê các dữ liệu chính yếu thuộc hai loại này.

Dữ liệu cá nhân cơ bản bao gồm: thông tin định danh thông thường, như họ và tên, thời gian sinh, thời gian chết, thông tin liên lạc, tình trạng hôn nhân và mối quan hệ gia đình, quốc tịch, hình ảnh của cá nhân, giới tính, số định danh cá nhân (số căn cước công dân, hộ chiếu, mã số thuế, số bảo hiểm xã hội/số thẻ bảo hiểm y tế, số giấy phép lái xe, số biển số xe), ngoài ra còn gồm thông tin về nhóm máu, tài khoản số và dữ liệu cá nhân phản ánh hoạt động, lịch sử hoạt động của cá nhân trên không gian mạng.

Dữ liệu cá nhân nhạy cảm được định nghĩa là dữ liệu cá nhân gắn liền với quyền riêng tư của cá nhân mà khi bị xâm phạm sẽ gây ảnh hưởng trực tiếp tới quyền và lợi ích hợp pháp của cá nhân, bao gồm: quan điểm chính trị và quan điểm tôn giáo, tình trạng sức khỏe và đời tư (ngoại trừ nhóm máu), dữ liệu sinh trắc học, dữ liệu di truyền, khuynh hướng tình dục, dữ liệu về tội phạm, dữ liệu khách hàng của tổ chức tín dụng, dịch vụ trung gian thanh toán, dữ liệu về vị trí của cá nhân được xác định qua dịch vụ định vị và các dữ liệu cá nhân nhạy cảm khác theo quy định của pháp luật Việt Nam.

Dựa trên cách diễn đạt của Điều 28, các tiêu chuẩn để xử lý dữ liệu cá nhân nhạy cảm nghiêm ngặt hơn so với các tiêu chuẩn dành cho dữ liệu cá nhân cơ bản. Cụ thể hơn, việc bảo vệ dữ liệu cá nhân nhạy cảm sẽ cần (i) tất cả các biện pháp quản lý và kỹ thuật cần thiết để bảo vệ dữ liệu cá nhân cơ bản, cộng với (ii) chỉ định Nhân viên bảo vệ dữ liệu ("DPO") và một cá nhân nội bộ, bộ phận bảo vệ dữ liệu ("DPD") (thông tin về DPD và DPO phải được thông báo cho cơ quan có thẩm quyền) và (iii) thông báo cho chủ thể dữ liệu rằng dữ liệu cá nhân nhạy cảm của họ được xử lý trừ những trường hợp cụ thể.

Yêu cầu (i) sự đồng ý của chủ thể dữ liệu, chủ thể dữ liệu phải được thông báo rằng dữ liệu được xử lý là dữ liệu cá nhân nhạy cảm (Điều 11.8); và (ii) chủ thể dữ liệu phải được thông báo rằng dữ liệu cá nhân nhạy cảm của họ sẽ được xử lý (Điều 28.3).

Do vậy, Công ty đề nghị các phòng ban chức năng không thu thập, lưu trữ các dữ liệu nhạy cảm nếu không thực sự cần thiết.

3. Hiệu lực của sự đồng ý

Dưới góc độ này, việc có được sự đồng ý của họ và thông báo trước về việc xử lý dữ liệu là bắt buộc, trừ các trường hợp ngoại lệ được mô tả trong Mục 5 bên dưới. Đặc biệt, Nghị định 13 quy định chi tiết các yêu cầu khác nhau để việc đồng ý có hiệu lực:

(i) Định dạng và hình thức đồng ý phù hợp: Phải thể hiện rõ ràng và cụ thể bằng văn bản, giọng nói, đánh dấu vào ô đồng ý, cú pháp đồng ý qua tin nhắn, chọn các thiết lập kỹ thuật đồng ý hoặc qua

một hành động khác thể hiện được điều này. Ngoài ra, sự đồng ý phải được thể hiện ở một định dạng có thể được in, sao chép bằng văn bản, bao gồm cả dưới dạng điện tử hoặc định dạng kiểm chứng được. Nhưng những hình thức như cài đặt mặc định, ô chọn đã được đánh dấu trước điều khoản và điều kiện chung không được coi là đồng ý.

(ii) Sự tự nguyện và nhận thức của chủ thể dữ liệu: Sự đồng ý cũng phải được đưa ra một cách tự nguyện dựa trên sự hiểu biết rõ ràng của chủ thể dữ liệu về các hoạt động xử lý, bao gồm (i) mục đích xử lý; (ii) loại dữ liệu cá nhân được xử lý; (iii) các chủ thể được xử lý dữ liệu cá nhân; và (iv) quyền và nghĩa vụ của chủ thể dữ liệu.

(iii) Cho cùng một mục đích: Trong trường hợp xử lý dữ liệu cho nhiều mục đích, sự đồng ý có thể dành cho một hoặc nhiều mục đích nêu ra. Việc đồng ý một phần hoặc đồng ý có điều kiện kèm theo tùy thuộc vào quyết định của chủ thể dữ liệu.

(iv) Sự im lặng hoặc không phản hồi không được coi là sự đồng ý.

(v) Hiệu lực: Sự đồng ý có hiệu lực cho tới khi chủ thể dữ liệu có quyết định khác (rút lại sự đồng ý) hoặc khi cơ quan nhà nước có thẩm quyền yêu cầu bằng văn bản.

Điều này dẫn đến yêu cầu, khi thu thập thông tin nhân sự, thông tin khách hàng, thông tin người dùng qua website hoặc các phương tiện điện tử, Công ty phải yêu cầu người cung cấp thông tin đánh dấu (x) vào ô đồng ý hoặc ký vào form mẫu đồng ý cung cấp thông tin. Người cung cấp thông tin phải biết được và đồng ý các mục đích sử dụng; Loại dữ liệu được sử dụng; Thông tin về tổ chức cá nhân có liên quan tới việc xử lý; Hậu quả và thiệt hại không mong muốn có thể xảy ra; Thời gian bắt đầu và kết thúc xử lý dữ liệu. Quá trình xử lý dữ liệu phải đảm bảo (i) đúng quy định của pháp luật; (ii) minh bạch; (iii) chỉ được phép thực hiện cho các mục đích đã tuyên bố; (iv) giới hạn trong mục đích và phạm vi nhất định; (v) sử dụng dữ liệu được cập nhật, bổ sung phù hợp với mục đích; (vi) phải bảo mật; (vii) đảm bảo dữ liệu chỉ được lưu trữ trong khoảng thời gian phù hợp; (viii) các tổ chức chịu trách nhiệm giải trình về tính tuân thủ. Do vậy, Công ty cần rà soát, xem xét lại các chính sách, điều khoản sử dụng trên các website của Công ty cũng như các quy trình nội bộ để chắc chắn có được sự đồng ý của người cung cấp trước khi thu thập và xử lý dữ liệu cá nhân.

4. Quyền của chủ thể dữ liệu:

Các quyền của chủ thể dữ liệu được quy định, bao gồm: (i) quyền được biết; (ii) quyền đồng ý; (iii) quyền truy cập; (iv) quyền rút lại sự đồng ý; (v) quyền xóa dữ liệu; (vi) quyền hạn chế xử lý dữ liệu; (vii) quyền cung cấp dữ liệu; (viii) quyền phản đối xử lý dữ liệu; (ix) quyền khiếu nại, tố cáo, khởi kiện; (x) quyền yêu cầu bồi thường thiệt hại; và (xi) quyền tự bảo vệ.

Trong số các quyền trên, việc thực hiện quyền truy cập dữ liệu phải tuân thủ các quy trình, định dạng nghiêm ngặt và đảm bảo nội dung yêu cầu.

Một thay đổi đáng chú ý khác trong Nghị định 13 là giới hạn thời gian nghiêm ngặt (72 giờ) được đặt ra để xử lý yêu cầu của chủ thể dữ liệu liên quan đến một số quyền nêu trên, bao gồm: (i) quyền hạn chế xử lý dữ liệu; (ii) quyền phản đối xử lý dữ liệu; (iii) quyền cung cấp dữ liệu; (iv) quyền truy cập; và (v) quyền xóa dữ liệu.

Lưu ý/*Note*

Để được hỗ trợ thêm, vui lòng liên hệ/ *for further support, please contact to*:
Anh Thư, Phòng Pháp lý/Legal Department: 028.62.504.888 (ext: 68414), email: anhthu.bui@daikin.com.vn

Nghị định 13 yêu cầu Bên Kiểm soát dữ liệu cá nhân và Bên Kiểm soát và xử lý dữ liệu cá nhân phải đảm bảo an toàn dữ liệu cá nhân và thông báo cho cơ quan chức năng về bất kỳ vi phạm quy định về bảo vệ dữ liệu cá nhân trong vòng 72 giờ sau khi xảy ra hành vi vi phạm. Trường hợp thông báo chậm thì Bên Kiểm soát dữ liệu cá nhân phải đưa ra lý do.

Như vậy, các bộ phận liên quan cần phối hợp với phòng IT để xây dựng và chỉnh sửa hệ thống cho phép người dùng có đầy đủ các quyền nêu trên để đảm bảo tuân thủ. Đồng thời, có biện pháp hỗ trợ để ghi nhận và báo cáo thông tin vi phạm cho cơ quan chức năng trong thời hạn cho phép.

5. Các trường hợp xử lý dữ liệu không cần sự đồng ý của chủ thể dữ liệu:

Sự đồng ý của chủ thể dữ liệu được miễn trừ trong các trường hợp sau:

(i) Trong trường hợp khẩn cấp, cần xử lý ngay dữ liệu cá nhân có liên quan để bảo vệ tính mạng, sức khỏe của chủ thể dữ liệu hoặc người khác

(ii) Việc công khai dữ liệu cá nhân theo quy định của luật

(iii) Việc xử lý dữ liệu của cơ quan nhà nước có thẩm quyền trong trường hợp tình trạng khẩn cấp về quốc phòng, an ninh quốc gia, trật tự an toàn xã hội, thảm họa lớn, dịch bệnh nguy hiểm; khi có nguy cơ đe dọa an ninh, quốc phòng nhưng chưa đến mức ban bố tình trạng khẩn cấp; phòng, chống bạo loạn, khủng bố, phòng, chống tội phạm và vi phạm pháp luật theo quy định của luật

(iv) Việc xử lý dữ liệu để thực hiện nghĩa vụ theo hợp đồng của chủ thể dữ liệu với cơ quan, tổ chức, cá nhân có liên quan theo quy định của luật

(v) Việc xử lý dữ liệu để phục vụ hoạt động của cơ quan nhà nước đã được quy định theo luật chuyên ngành

Chiếu theo quy định này thì có thể hiểu rằng: trường hợp thu thập thông tin, cung cấp thông tin,...để thực hiện nghĩa vụ theo hợp đồng của Người lao động, nhà cung cấp, khách hàng,.. với Công ty thì sẽ không cần sự đồng ý của họ mới được xử lý. Ví dụ như trường hợp của Hợp đồng vận chuyển hàng hóa của Daikin có thể hiện thông tin của người vận chuyển, lúc này nếu phát sinh yêu cầu phải xử lý thông tin nói trên thì Daikin sẽ được miễn trừ việc xin chấp thuận của chủ thể dữ liệu.

6. Nghĩa vụ lập hồ sơ đánh giá tác động xử lý dữ liệu

Nghị định 13 đặt ra yêu cầu phải lập và ban hành hồ sơ đánh giá tác động xử lý dữ liệu bằng văn bản trong mọi trường hợp, với các nội dung bắt buộc theo biểu mẫu được ban hành kèm theo Nghị định này.

Cụ thể, Bên kiểm soát; Bên kiểm soát và xử lý lập hồ sơ bao gồm: (i) thông tin chi tiết, liên lạc của Bên kiểm soát, bên kiểm soát và xử lý dữ liệu; (ii) họ tên, chi tiết liên lạc của tổ chức được phân công nhiệm vụ bảo vệ dữ liệu cá nhân và nhân viên bảo vệ dữ liệu cá nhân; (iii) mục đích xử lý dữ liệu; (iv) các loại dữ liệu cá nhân được xử lý; (v) tổ chức, cá nhân nhận dữ liệu cá nhân ở nước ngoài; (vi) trường hợp chuyển dữ liệu cá nhân ra nước ngoài; (vii) Thời gian xử lý dữ liệu, thời gian dự kiến để xóa, hủy dữ liệu cá nhân nếu có; (viii) mô tả chung về biện pháp bảo vệ dữ liệu cá nhân được áp dụng; (ix) đánh giá mức độ ảnh hưởng của việc xử lý dữ liệu cá nhân, hậu quả, thiệt hại không mong muốn có thể xảy ra, các biện pháp giảm thiểu hoặc loại bỏ nguy cơ, tác hại đó.

Lưu ý/*Note*

Để được hỗ trợ thêm, vui lòng liên hệ/ *for further support, please contact to*:
Anh Thư, Phòng Pháp lý/Legal Department: 028.62.504.888 (ext: 68414), email: anhthu.bui@daikin.com.vn

Hồ sơ phải được chuẩn bị sẵn sàng để phục vụ cho việc kiểm tra của Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao (A05) trong thời hạn 60 ngày, kể từ ngày bắt đầu xử lý dữ liệu. Tuy nhiên, nếu có bất kỳ sự thay đổi nào đối với dữ liệu cá nhân mà các tổ chức xử lý thì cần điều chỉnh hồ sơ đánh giá tác động cho phù hợp.

Do đó, nội bộ Daikin có rất nhiều bộ phận, phòng ban trong Công ty phải tiến hành lập hồ sơ đánh giá tác động với các nội dung nói trên. Đơn cử như Phòng nhân sự trong hoạt động thu thập thông tin Người lao động để tải lên hệ thống E-Office, hay Khối Service khi tiến hành thu thập thông tin người dùng để chuyển cho các nhà cung cấp ở nước ngoài xử lý và hoặc các hệ thống quản lý thông tin nhân sự, khách hàng, đối tác của Công ty.

7. Chuyển dữ liệu ra nước ngoài:

Tương tự, việc chuyển dữ liệu ra nước ngoài sẽ đặt ra yêu cầu gửi hồ sơ đánh giá tác động cho A05 để cơ quan này đánh giá sau khi chuyển giao. Cụ thể, bên chuyển giao dữ liệu cá nhân của người Việt Nam phải (i) chuẩn bị hồ sơ đánh giá tác động chuyển dữ liệu ra nước ngoài với các nội dung bắt buộc, (ii) gửi hồ sơ đến A05 trong vòng 60 ngày kể từ ngày bắt đầu xử lý dữ liệu để cơ quan này đánh giá, và (iii) thông báo cho A05 về việc chuyển dữ liệu ra nước ngoài và thông tin chi tiết về người phụ trách sau khi hoàn tất việc chuyển giao. Cuối cùng, hồ sơ này phải luôn được cập nhật để cơ quan có thẩm quyền kiểm tra.

Điều này đòi hỏi các bộ phận có liên quan đến hoạt động chuyển dữ liệu ra nước ngoài trong công ty như: Bộ phận Service khi tiến hành thu thập thông tin người dùng để chuyển cho các nhà cung cấp ở nước ngoài xử lý, ngoài việc lập hồ sơ đánh giá tác động xử lý dữ liệu thì còn phải gửi hồ sơ này về cho Bộ phận chuyên trách bảo vệ dữ liệu. Sau đó, bộ phận chuyên trách này có trách nhiệm gửi hồ sơ đến A05 trong vòng 60 ngày kể từ ngày bắt đầu xử lý dữ liệu để cơ quan này đánh giá, và thông báo cho A05 về việc chuyển dữ liệu ra nước ngoài, kèm theo thông tin chi tiết về người phụ trách sau khi hoàn tất việc chuyển giao.

8. Bảo vệ dữ liệu cá nhân trong kinh doanh dịch vụ tiếp thị và giới thiệu sản phẩm quảng cáo

Bên kinh doanh dịch vụ tiếp thị và/hoặc giới thiệu sản phẩm quảng cáo chỉ được sử dụng dữ liệu cá nhân của khách hàng được thu thập qua hoạt động kinh doanh của mình để kinh doanh dịch vụ tiếp thị, giới thiệu sản phẩm quảng cáo khi có sự đồng ý của chủ thể dữ liệu. Chủ thể dữ liệu cần được thông báo về nội dung, phương thức, hình thức, tần suất giới thiệu sản phẩm.

Việc này tác động không nhỏ đến hoạt động của Khối Service (vận hành website, call center), phòng Marketing và các phòng ban phụ trách các dự án có thu thập thông tin người dùng, nên vui lòng lưu ý khi tiến hành hoạt động tiếp thị hoặc giới thiệu sản phẩm quảng cáo vì các bộ phận này sẽ có trách nhiệm chứng minh việc sử dụng dữ liệu cá nhân của khách hàng được giới thiệu sản phẩm đúng với quy định.

9. Nhân sự chuyên trách bảo vệ dữ liệu

Nghị định 13 ra đời, đồng nghĩa với việc các doanh nghiệp phải thừa nhận vai trò của Nhân sự chuyên trách bảo vệ dữ liệu. Điều này như một trong các biện pháp bảo vệ dữ liệu cá nhân nhạy cảm, nên dẫn đến Bên kiểm soát, bên xử lý, bên kiểm soát và xử lý phải chỉ định một bộ phận bảo vệ dữ liệu cá nhân và một nhân sự bảo vệ dữ liệu. Đồng thời thông báo cho A05 về hai đối tượng nêu trên.

Lưu ý/*Note*

Để được hỗ trợ thêm, vui lòng liên hệ/ *for further support, please contact to*:
Anh Thư, Phòng Pháp lý/Legal Department: 028.62.504.888 (ext: 68414), email:
anhthu.bui@daikin.com.vn

Điều 24 Nghị đinh 23/2023, ngụ ý rằng sự cần thiết phải chỉ định DPO và DPD cũng có thể áp dụng cho việc xử lý dữ liệu cá nhân cơ bản. Điều này là do, theo Điều 24, thông tin về DPO và DPD phải luôn được đưa vào Hồ sơ đánh giá tác động bảo vệ dữ liệu ("Hồ sơ DPIA"), mà Người kiểm soát/Người xử lý/Người kiểm soát-Người xử lý (bất kể loại nào) phải thiết lập và giữ sẵn. Vì một bản sao của Hồ sơ DPIA phải được nộp cho cơ quan có thẩm quyền, điều này về cơ bản có nghĩa là thông tin về DPO và DPD cũng được báo cáo cho cơ quan có thẩm quyền.

Cho nên, việc cử một nhân sự chuyên trách gần như là một yêu cầu bắt buộc khi xử lý thông tin mà Nghị định 13 đặt ra. Ngay cả khi quy định một cách không minh thị thì

B. KẾ HOẠCH HÀNH ĐỘNG

1. Công ty phải thành lập bộ phận có chức năng bảo vệ dữ liệu cá nhân, chỉ định nhân sự phụ trách bảo vệ dữ liệu cá nhân và trao đổi thông tin về bộ phận và cá nhân phụ trách bảo vệ dữ liệu cá nhân với Cơ quan chuyên trách bảo vệ dữ liệu cá nhân.

2. Các phòng, ban, khối liên quan đến việc thu thập và xử lý thông tin dữ liệu cá nhân như HR, Service, Marketing, IT, ... chủ động rà soát hoạt động thu thập, xử lý dữ liệu cá nhân mà phòng mình phụ trách, đồng thời, có trách nhiệm thực hiện các công việc sau (i) Có được sự đồng ý của chủ thể dữ liệu về việc thu thập và xử lý thông tin cho các mục đích cụ thể; (ii) Rà soát và cập nhật các chính sách, điều khoản liên quan đến việc thu thập, xử lý dữ liệu cá nhân; (iii) lập báo cáo đánh giá tác động xử lý dữ liệu cá nhân trong vòng 60 ngày kể từ ngày bắt đầu xử lý dữ liệu; (iv) lập và gửi báo cáo đánh giá tác động xử lý dữ liệu cá nhân cho A05 trong thời gian 60 ngày kể từ ngày tiến hành xử lý dữ liệu cá nhân khi chuyển dữ liệu ra nước ngoài.

3. Bộ phận IT kết hợp với Nhà cung cấp dịch vụ xử lý dữ liệu như E-Office, SAP, cũng như Khối Service phải phối hợp với đơn vị quản lý website để đặt ra một cơ chế, phương thức để đảm bảo sự đồng ý của chủ thể dữ liệu có thể được in hoặc sao chép bằng văn bản (định dạng điện tử có thể được chấp nhận). Nếu dựa vào các điều kiện khác để xử lý dữ liệu thì đánh giá xem chủ thể dữ liệu có được thông báo hay không. Khi sự đồng ý được sử dụng làm cơ sở pháp lý để xử lý dữ liệu cá nhân, cần có cơ chế để các cá nhân rút lại sự đồng ý của họ và cho phép việc rút lại có thể được in hoặc sao chép khi cần. Đồng thời, hệ thống phải có khả năng thông báo cho cá nhân về hậu quả hoặc thiệt hại có thể xảy ra khi rút lại sự đồng ý.

Lưu ý/*Note*

Để được hỗ trợ thêm, vui lòng liên hệ/ *for further support, please contact to*:
Anh Thư, Phòng Pháp lý/Legal Department: 028.62.504.888 (ext: 68414), email:
anhthu.bui@daikin.com.vn

DECREE 13/2023/ND-CP ON PROTECTION OF PERSONAL DATA

On April 17, 2023, the Government issued Decree 13/2023/ND-CP on the Protection of Personal Data Protection ("Decree 13") creating the first unified and comprehensive legal document on personal data protection in Vietnam. Decree 13 will take effect from July 1, 2023 and will have significant impacts on the company's operations in general, as well as the data processing activities in particular of relevant departments.

C. MAJOR CONTENTS OF DECREE 13

1. Identify role in the processing of personal data

Decree 13 clearly distinguishes between the different roles of data process and have accorded separate responsibilities for each role. Specifically:

Data Controller refers to an organization or individual that decides the purpose and means of processing personal data. Data Controller has the higher responsibility to notify and cooperate with the authorities in case of personal data breaches. The Data Controller is ultimately accountable to the data subject and bears the burden of proving prior consent is obtained for all processing activities.

Data Processor refers to an organization or individual that is engaged under a contract by the Data Controller to process personal data in accordance with the instructions of the Data Controller. Data Processor is responsible for notifying the Data Controller of any breaches and cooperating with the authority in case of breaches and investigations.

Data Controller cum Processor is a hybrid role and will need to comply with the obligations of both Data Controller and Data Processor.

Third parties, on the other hand, refers to individuals or entities other than the Data Controller or Data Processor that are allowed to process personal data. This definition may broadly refer to anyone that is permitted to be involved in personal data handling such as payment service providers, telecommunication service providers, etc.

Leading to Daikin's case, information collection, management, storage and processing activities take place regularly. For example, the operation of departments such as: Human Resources Department collects employee information, then transfers the data to the E-Office page; Service Division, Marketing Department, Call center collect customer information,... Therefore, regarding the role, the Company is identified as the Controller of personal data or the Party that controls and processes personal data. ; departments and divisions related to the collection, management,... personal data are the data processor; telecommunications, postal service providers, ... can be understood as the Third Party. Each entity needs to properly define its role(s) and comply with the different obligations that apply to each role under Decree 13.

2. Identify types of the personal data processed

Lưu ý/*Note*

Để được hỗ trợ thêm, vui lòng liên hệ/ *for further support, please contact to*:
Anh Thư, Phòng Pháp lý/Legal Department: 028.62.504.888 (ext: 68414), email: anhthu.bui@daikin.com.vn

Personal data refers to information associated with a particular person or helps identify a natural person when used independently or combined with other information that can be the direct information, numbers, text, images, audio, video, and digital data.

Decree 13 classifies personal data into two (2) types: (i) basic and (ii) sensitive personal data, and provides a non-exhaustive list of each classification.

Basic personal data includes: usual identification information e.g., name, date of birth, date of death, contact details, marital status and family relationship, ethnicity, personal image, gender, personal identification numbers (citizen identification number, passport, tax code, social/medical insurance code, driving license number, vehicle plate number) but also including blood type, digital accounts and data reflecting individuals' activity history on cyberspace.

Sensitive personal data is defined as personal data associated with an individual's privacy and when violated will directly affect the individual's legitimate rights and interests and includes political and religious views, health conditions (except blood type), biometric data, genetic data, sexual orientation, criminal records, customer data of credit institutions, intermediate payment services, geographic location and other types of sensitive personal data as stipulated by Vietnamese laws.

Based on the wording of Article 28 on the protection of sensitive personal data, the standards for processing sensitive personal data appear to be a bit stricter than those for basic personal data. More specifically, the protection of sensitive personal data would necessitate (i) all of the managerial and technical measures required for the protection of basic personal data, plus (ii) the appointment of a Data Protection Officer ("DPO") and an internal personal data protection department ("DPD") (information on the DPD and the DPO should be notified to the authority), and (iii) notification to data subjects that their sensitive personal data is processed except in specified cases.

It is required that (i) when obtaining consent from the data subject, the data subjects must be informed that the data to be processed is sensitive personal data (Article 11.8); and (ii) the data subjects must be notified that their sensitive personal data will be processed (Article 28.3).

Therefore, the Company recommends that functional departments do not collect and store sensitive data if it is not really necessary.

3. Effect of consent

In this respect, their consent and prior notice of data processing is required, with the exception of the exceptions described in Section 5 below. In particular, Decree 13 details the various requirements for consent to take effect:

(i) Appropriate format and form of consent: Must be clearly and specifically expressed in writing, voice, check the consent box, consent syntax via text message, select consent technical settings or via Another action demonstrates this. In addition, consent must be expressed in a format that can be printed, reproduced in writing, including in electronic or verifiable formats. Default setting, pre-ticked boxes, general terms and conditions or silence or non-response will not be considered as consent.

Lưu ý/*Note*

Để được hỗ trợ thêm, vui lòng liên hệ/ *for further support, please contact to*:
Anh Thư, Phòng Pháp lý/Legal Department: 028.62.504.888 (ext: 68414), email: anhthu.bui@daikin.com.vn

(ii) Data Subject Voluntary and Consciousness: Consent must also be given voluntarily based on the data subject's clear understanding of the processing activities, including (i) the purpose of data processing; (ii) the type of personal data to be processed; (iii) the organization or individual involved in the processing; and (iv) rights and obligations of data subjects.

(iii) For the same purpose: In the case of data processing for multiple purposes, consent can be for one or more of the stated purposes. Partial or conditional consent is at the discretion of the data subject.

(iv) Silence or non-response is not considered consent.

(v) Validity: Consent is valid until the data subject decides otherwise (withdrawal of consent) or when requested in writing by a competent authority.

Therefore, the Company needs to review the policies and terms of use on the Company's websites as well as internal processes to ensure the consent of the provider before collecting and processing personal data..

4. The data subject's rights

The rights of the data subject are specified, including: (i) the right to know; (ii) the right to consent; (iii) access rights; (iv) the right to withdraw consent; (v) the right to delete data; (vi) the right to restrict data processing; (vii) the right to provide data; (viii) the right to object to data processing; (ix) the right to complain, denounce and initiate lawsuits; (x) the right to claim damages; and (xi) the right to self-defense.

Among the above rights, the exercise of data access rights is subject to strict procedures, formatting, and required content assurance.

Another notable change in Decree 13 is the strict time limit (72 hours) set for processing data subject requests related to some of the above rights, including: (i) the right to restrict data processing; (ii) the right to object to data processing; (iii) the right to provide data; (iv) the right to access; and (v) the right to delete data.

Decree 13 requires the Controller of personal data and the Controller and processor of personal data to ensure the safety of personal data and notify the authorities of any violations of regulations on protection of personal data within 72 hours of the breach. In case of late notification, the Controller of personal data must give reasons.

As such, relevant departments need to coordinate with the IT department to build and modify a system that allows users to have full rights mentioned above to ensure compliance. At the same time, there are support measures to record and report violating information to the authorities within the allowed time limit.

5. Cases of data processing without the consent of the data subject:

Consent of data subjects is exempted in the following cases:

(i) In urgent cases where it is necessary to immediately process relevant personal data to protect the life or health of the data subject or others;

(ii) Where the public disclosure of personal data is in accordance with the law

Lưu ý/*Note*

Để được hỗ trợ thêm, vui lòng liên hệ/ *for further support, please contact to*:
Anh Thư, Phòng Pháp lý/Legal Department: 028.62.504.888 (ext: 68414), email: anhthu.bui@daikin.com.vn

(iii) When the processing of data is done by competent state agencies in the event of a state of emergency on national defense, security, social order and safety, major disaster, or dangerous epidemic; or when there is a risk that threatens security and national defense but not to the extent where it is necessary to declare a state of emergency; or to prevent and combat riots, terrorism, crimes and violations of the law

(iv) To fulfill the contractual obligations of the data subject with relevant agencies, organizations and individuals as prescribed by law; or

(v) To serve the activities of state agencies as prescribed by sector-specific laws.

According to this regulation, it can be understood that: in case of collecting information, providing information, ... to fulfill contractual obligations of employees, suppliers, customers, ... Our company will not need their consent to be processed. For example, in the case of Daikin's Carriage Contract, which may show the carrier's information, if there is a request to process the above information, Daikin will be exempted from asking for the owner's consent.

6. Obligation to document the impact of data processing

Decree 13 requires the preparation and issuance of written data processing impact assessment dossiers in all cases, with mandatory contents according to the form issued with this Decree.

Specifically, the Controller; Data Controller cum Processor prepare documents includes: (i) details, contact information of the Controller, Data Controller cum Processor; (ii) full name, contact details of the organization assigned to protect personal data and personal data protection officer; (iii) data processing purposes; (iv) the types of personal data processed; (v) organizations and individuals that receive personal data abroad; (vi) the case of transferring personal data abroad; (vii) Data processing time, expected time to delete or destroy personal data, if any; (viii) a general description of the personal data protection measures applied; (ix) assessment of the impact of the processing of personal data, possible consequences, unwanted damage, measures to reduce or eliminate such risk or harm.

Dossier must be prepared for inspection by the Department of Cybersecurity and High-Tech Crime Prevention (A05) within 60 days from the date of data processing. However, if there are any changes to the personal data that organizations process, the impact assessment profile should be adjusted accordingly.

Therefore, there are many departments and divisions within Daikin internally that must conduct impact assessment documents with the above contents. For example, the Human Resources Department in collecting employee information to upload to the E-Office system, or the Service Department when collecting user information to transfer to overseas suppliers for processing and or information management systems of the Company's personnel, customers and partners.

7. Cross-Border Transfer of Personal Data:

Similarly, transferring data abroad will require the submission of impact assessment records to A05 for review after the transfer. Specifically, the party transferring the personal data of Vietnamese people must (i) prepare a dossier of assessment of the impact of data transfer abroad with mandatory contents, (ii) send the dossier to A05 within 60 day from the date of the personal data processing for review by this agency,

and (iii) notify A05 of the data transfer abroad and details of the person in charge upon completion of the transfer . Finally, this record must always be updated for inspection by the competent authority.

This requires departments related to overseas data transfer activities in the company such as: Service Department when collecting user information to transfer to overseas suppliers for processing, in addition to: the preparation of the data processing impact assessment dossier, it must also be sent to the Data Protection Department. Then, this specialized department is responsible for sending the dossier to A05 within 60 days from the date of data processing for this agency to evaluate, and notify A05 of the data transfer abroad . along with detailed information about the person in charge after completing the transfer .

8. Protection of personal data in the business of marketing services and recommending advertising products

The party providing marketing services and/or introducing advertising products may only use the personal data of customers collected through its business activities to provide marketing services, introduce advertising products, and sell advertising products. reported with the consent of the data subject. The data subject should be informed about the content, method, form and frequency of product introduction.

This has a significant impact on the operation of Service Division (website operation, call center), Marketing department and departments in charge of projects that collect user information, so please pay attention when conducting activities. marketing or recommending promotional products because these departments will be responsible for demonstrating that the use of personal data of customers who are recommending the product is in accordance with the regulations.

9. Personnel in charge of data protection

Decree 13 was born, which means that businesses have to acknowledge the role of a Data Protection Officer. This, as one of the measures to protect sensitive personal data, should result in the Controller, processor, controller and processor having to appoint a personal data protection department and an employee data protection. At the same time, notify A05 about the above two objects.

Article 24 of Decree 23/2023 implies that the necessity to appoint a DPO and a DPD may nevertheless also apply to the processing of basic personal data. This is because, according to Article 24, information on the DPO and DPD must always be included in the Data Protection Impact Assessment Profile ("DPIA Profile"), which Controllers/Processors/Controller-Processors (regardless of the type) have to establish and keep available. Since once copy of the DPIA Profile must be submitted to the authority, this essentially means that information on the DPO and DPD is also reported to the authority.

Therefore, the appointment of a full-time staff is almost a mandatory requirement when handling information that Decree 13 sets forth. Even if it is not explicitly stated

D. ACTION PLAN

1. The company must establish a department with the function of protecting personal data, appoint personnel in charge of personal data protection and exchange information about the department and individual in charge of personal data protection with the Personal Data Protection Authority.

Lưu ý/*Note*

Để được hỗ trợ thêm, vui lòng liên hệ/ *for further support, please contact to*:
Anh Thư, Phòng Pháp lý/Legal Department: 028.62.504.888 (ext: 68414), email:
anhthu.bui@daikin.com.vn

2. Departments, departments and divisions related to the collection and processing of personal data such as HR, Service, Marketing, IT, ... proactively review activities of collecting and processing personal data which the department is in charge of, and at the same time, is responsible for performing the following tasks (i) Obtaining the consent of the data subject on the collection and processing of information for specific purposes; (ii) Review and update policies and terms related to the collection and processing of personal data; (iii) prepare a personal data processing impact assessment report within 60 days from the date of commencement of data processing; (iv) prepare and send a personal data processing impact assessment report to A05 within 60 days from the date of processing of personal data when transferring data abroad.

3. The IT department in conjunction with the Data Processing Service Provider such as E-Office, SAP, as well as the Service Division must coordinate with the website management unit to set out a mechanism and method to ensure the The consent of the data subject may be printed or reproduced in writing (electronic format may be accepted). If other conditions are based on data processing, evaluate whether the data subject is informed. Where consent is used as the legal basis for processing personal data, there should be a mechanism for individuals to withdraw their consent and to allow the withdrawal to be printed or reproduced as needed. . At the same time, the system must be able to notify the individual of possible consequences or damages when consent is withdrawn.

Lưu ý/*Note*

Để được hỗ trợ thêm, vui lòng liên hệ/ *for further support, please contact to*:
Anh Thư, Phòng Pháp lý/Legal Department: 028.62.504.888 (ext: 68414), email: anhthu.bui@daikin.com.vn