KPMG

Bản tin nhanh về Pháp luật

Tháng 4 năm 2023

Nghị định 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân đã được ban hành

Vào ngày 17/4/2023, Chính phủ đã ban hành Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân ("**Nghị định 13**") sau một thời gian dài chờ đợi. Nghị định 13 sẽ có hiệu lực từ ngày **01/7/2023**. Cùng với Luật An ninh mạng (Luật số 24/2018/QH14) ngày 12 tháng 6 năm 2018 và văn bản hướng dẫn thi hành đầu tiên là Nghị định số 53/2022/NĐ-CP ngày 15 tháng 8 năm 2022, Nghị định 13 là văn bản pháp lý thứ ba được ban hành trong kế hoạch của Chính phủ nhằm tăng cường khung pháp lý điều chỉnh các hoạt động trên không gian mạng. Nghị định 13 quy định chi tiết hơn về nghĩa vụ bảo vệ dữ liệu và an ninh mạng đối với các hoạt động xử lý dữ liệu cá nhân.

Ai cần phải tuân thủ?

Nghị định 13 áp dụng cho mọi tổ chức, cá nhân trong nước hoặc nước ngoài có liên quan đến việc xử lý dữ liệu cá nhân tại Việt Nam (ví dụ: nhân viên, khách hàng, nhà cung cấp, người dùng hoặc cá nhân khác), kể cả khi việc xử lý dữ liệu cá nhân được thực hiện bên ngoài Việt Nam.

Mặc dù có các yêu cầu tương tự so với Quy định chung về bảo vệ dữ liệu của Liên minh Châu Âu ("**GDPR**"), nhưng Nghị định 13 có một số điểm khác biệt đáng kể, chẳng hạn như các yêu cầu đối với chuyển dữ liệu cá nhân ra nước ngoài, hình thức lấy sự đồng ý của chủ thể dữ liệu, báo cáo đánh giá tác động và căn cứ hợp pháp để xử lý dữ liệu cá nhân.

Các công ty đã ban hành các chính sách và triển khai các hoạt động quản lý quyền riêng tư theo GDPR hoặc theo các quy định về quyền riêng tư khác sẽ không đương nhiên được xem là đã tuân thủ theo Nghị định 13. Với việc Nghị định 13 sẽ có hiệu lực vào ngày 01/7/2023, các doanh nghiệp cần bắt đầu rà soát các chính sách nội bộ và thực tiễn quản lý quyền riêng tư của mình ngay lập tức để xác định các khoảng vênh giữa các chính sách nội bộ và hoạt động triển khai của mình với yêu cầu của Nghị định 13, để lên kế hoạch hành động tương ứng.

Cần làm gì để tuân thủ?

Chúng tôi đã phác thảo trong bảng dưới đây một số yêu cầu tuân thủ chính của Nghị định 13. Xin lưu ý rằng nhiều điều khoản trong Nghị định này được diễn đạt chung chung và việc diễn giải các điều khoản đó gặp nhiều khó khăn. Do thời gian còn lại để triển khai thực hiện Nghị định 13 khá ngắn, chúng tôi hi vọng rằng Bộ Công an sẽ sớm có hướng dẫn cụ thể hơn về cách hiểu và thi hành Nghị định 13. Những hướng dẫn này sẽ hỗ trợ các nỗ lực tuân thủ của doanh nghiệp. Chúng tôi sẽ tiếp tục theo dõi chặt chẽ và cung cấp thông tin cập nhật về việc ban hành những hướng dẫn chi tiết này. Trong thời gian chờ đợi, các doanh nghiệp có thể triển khai thực hiện ngay các công việc sau để tuân thủ Nghị định 13.

Hạng mục	Hành động tuân thủ cần thực hiện	Mô tả
Xác định vai trò trong quá trình xử lý dữ liệu cá nhân	Phân công trách nhiệm kèm theo quy trình cho mọi hoạt động xử lý dữ liệu cho các đơn vị có liên quan Rà soát lại việc xử lý dữ liệu và kỹ thuật ghi, ví dụ: xử lý theo thời gian thực, xử lý giao dịch, xử lý theo lô hay xử lý đa tiến trình	Tương ứng với các định nghĩa trong GDPR, Nghị định 13 phân biệt rõ ràng các vai trò khác nhau của những 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** là tổ chức hoặc 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 các cơ quan nếu có sự vi phạm dữ liệu cá nhân. Bên Kiểm soát dữ liệu 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 các hoạt động xử lý. **Bên Xử lý dữ liệu** là tổ chức hoặc cá nhân giao kết hợp đồng với Bên Kiểm soát dữ liệu về việc thực hiện việc xử lý dữ liệu cá nhân dưới sự hướng dẫn của Bên Kiểm soát dữ liệu. Bên Xử lý dữ liệu có trách nhiệm thông báo cho Bên Kiểm soát dữ liệu về các vi phạm cũng như phối hợp với các cơ quan có thẩm quyền trong việc điều tra khi có vi phạm. **Bên Kiểm soát và xử lý dữ liệu** là một vai trò kép, theo đó phải tuân thủ các nghĩa vụ của cả Bên Kiểm soát dữ liệu lẫn Bên Xử lý dữ liệu. **Bên thứ ba** là tổ chức hoặc cá nhân không phải Bên Kiểm soát dữ liệu và Bên Xử lý dữ liệu nhưng được phép xử lý dữ liệu cá nhân. Định nghĩa này có thể mở rộng sang bất kỳ ai tham gia vào việc xử lý dữ liệu cá nhân, chẳng hạn như các bên cung cấp dịch vụ thanh toán, dịch vụ viễn thông, v.v.
Xác định loại dữ liệu cá nhân được xử lý	Xây dựng hoặc rà soát mô hình quản lý dữ liệu nội bộ và quy tắc vận hành, đồng thời thiết lập hệ thống quản lý và phân loại dữ liệu cho các loại dữ liệu cá nhân khác nhau	**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. Nghị định 13 áp dụng các nghĩa vụ xử lý và bảo vệ bổ sung đối với việc xử lý dữ liệu cá nhân nhạy cảm.
Xác định căn cứ pháp lý cho việc xử lý dữ liệu cá nhân	Trách nhiệm chứng minh rằng dữ liệu có được xử lý hợp pháp hay không thuộc về bên xử lý dữ liệu. Cần xem xét lại liệu thông lệ, chính sách, các khóa đào tạo và nhật ký hệ thống hiện tại có thể chứng minh việc tuân thủ quy định này hay không. Các quy tắc và chính sách nội bộ có thể bao gồm những mục như: quy tắc và quy trình xử lý dữ liệu cá nhân; ủy quyền cho nhân sự xử lý dữ liệu, quy tắc và quy trình trong trường hợp vi phạm quy định về bảo vệ dữ liệu cá nhân và quy trình khắc phục vi phạm này.	Tương tự GDPR, Nghị định 13 yêu cầu các tổ chức phải có sự đồng ý trước từ phía cá nhân để xử lý dữ liệu của cá nhân đó, và phải tuân thủ các nguyên tắc được nêu trong Điều 3, tức là: quá trình xử lý dữ liệu phải (i) đúng quy định pháp luật; (ii) minh bạch; (iii) chỉ được 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; và (vi) phải bảo mật; đồng thời (vii) đảm bảo dữ liệu chỉ được lưu trữ trong khoảng thời gian phù hợp và (viii) các tổ chức chịu trách nhiệm giải trình về tính tuân thủ này. Đáng chú ý, Nghị định 13 nghiêm cấm việc mua bán bất kỳ dữ liệu nào dưới mọi hình thức nhằm khắc phục tình trạng mua bán danh sách dữ liệu đã xảy ra trong quá khứ. Về cơ bản, trừ một vài trường hợp ngoại lệ, sự đồng ý của chủ thể dữ liệu là bắt buộc để có thể xử lý hợp pháp dữ liệu cá nhân cho mọi hoạt động, bao gồm tiếp thị và quảng cáo chéo. Bên cạnh đó, mỗi khi tổ chức thay đổi phương thức xử lý dữ liệu cá nhân thì cũng phải có được sự đồng ý mới từ phía chủ thể dữ liệu.

Hạng mục	Hành động tuân thủ cần thực hiện	Mô tả
	Cần đặt ra một cơ chế 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) Cần đánh giá xem hình thức đồng ý có tuân thủ các yêu cầu tại Nghị định 13 hay không 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	Sự đồng ý có giá trị nếu nó được đưa ra thông qua một hành động cho thấy sự chủ động và tự nguyện của chủ thể dữ liệu (như ký tên, đánh dấu vào ô đồng ý, nhấp vào nút), sau khi cá nhân được cung cấp đầy đủ thông tin về cách thức và mức độ xử lý dữ liệu. Những hình thức như cài đặt mặc định, ô chọn đã được đánh dấu trước, điều khoản và điều kiện chung, việc im lặng hoặc không phản hồi sẽ không được xem là sự đồng ý. Cá nhân có quyền rút lại sự đồng ý của mình bất cứ lúc nào. Xử lý dữ liệu mà không có sự đồng ý chỉ được giới hạn cho các trường hợp sau: a. để bảo vệ tính mạng, sức khỏe của chủ thể dữ liệu hoặc người khác b. công khai dữ liệu cá nhân nhằm thực hiện theo quy định của luật c. xử lý dữ liệu thực hiện bởi cơ quan nhà nước trong trường hợp (i) tình trạng khẩn cấp hoặc khi có nguy cơ đe dọa đến quốc phòng, an ninh quốc gia; phòng, chống bạo loạn, khủng bố, phòng, chống tội phạm và vi phạm pháp luật; hoặc (ii) nhằm phục vụ cho hoạt động của cơ quan theo quy định. d. ghi âm, ghi hình và xử lý dữ liệu cá nhân thu được từ hoạt động ghi âm, ghi hình tại nơi công cộng (có thông báo trước) bởi cơ quan, tổ chức có thẩm quyền với mục đích bảo vệ an ninh quốc gia, trật tự an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân; e. để thực hiện nghĩa vụ theo hợp đồng (trừ trường hợp phục vụ tiếp thị và quảng cáo cho mục đích kinh doanh) của chủ thể dữ liệu theo quy định của luật. Ngoài yêu cầu về sự đồng ý chung, quy định còn đặt ra các yêu cầu về sự đồng ý cụ thể từ các bên liên quan trong các trường hợp sau: a. xử lý dữ liệu của trẻ em từ đủ 7 tuổi trở lên phải có sự đồng ý của trẻ và người giám hộ; b. đối với dữ liệu của người bị tuyên bố là mất tích hoặc người đã chết sẽ cần có sự đồng ý của người thân.
Thực hiện cơ chế để cá nhân có thể rút lại sự đồng ý	Đánh giá và cập nhật các cơ chế hiện hành để đảm bảo quyền này; đào tạo nhân sự chịu trách nhiệm xử lý các yêu cầu của chủ thể dữ liệu và nâng cao nhận thức bảo vệ dữ liệu cá nhân 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 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.	Khi có yêu cầu rút lại sự đồng ý phát sinh, tổ chức cần phải thông báo cho cá nhân về hậu quả hoặc thiệt hại có thể xảy đến từ việc rút lại sự đồng ý.
Yêu cầu về thông báo xử lý dữ liệu cá nhân	Rà soát và cập nhật các chính sách bảo mật hiện có hoặc xây dựng các chính sách bảo mật mới bao gồm tối thiểu các yêu cầu theo quy định của Nghị định 13 để cung cấp cho các cá nhân trong thời gian sớm nhất Tham khảo ý kiến của cố vấn pháp lý để đảm bảo việc tuân thủ	Nghị định 13 yêu cầu các tổ chức cung cấp thông báo tuân thủ cho các cá nhân trước khi xử lý dữ liệu cá nhân của họ. Thông báo về quyền riêng tư sẽ cần bao gồm loại, mục đích và phương pháp xử lý; danh tính của Bên xử lý dữ liệu cá nhân hoặc bên thứ ba có liên quan; rủi ro trong quá trình xử lý, thời gian xử lý.
Triển khai hệ thống xử lý yêu cầu của chủ thể dữ liệu	Một hệ thống mà thông qua đó chủ thể dữ liệu có thể thực hiện các quyền của họ và nhân sự phụ trách có thể nhận, đánh giá, xác thực và phản hồi các yêu cầu này	Nghị định 13 đưa ra một số quyền nhất định của chủ thể dữ liệu (ví dụ như: quyền truy cập, quyền hạn chế xử lý dữ liệu, quyền phản đối xử lý dữ liệu, quyền chỉnh sửa dữ liệu, quyền xóa dữ liệu, v.v.) và yêu cầu bên phụ trách dữ liệu phải đảm bảo các quyền này. Mọi yêu cầu hạn chế hoặc phản đối xử lý dữ liệu được thực hiện trong 72 giờ sau khi có yêu cầu của chủ thể dữ liệu.

Hạng mục	Hành động tuân thủ cần thực hiện	Mô tả
Nhân sự phụ trách bảo vệ dữ liệu cá nhân	Bổ nhiệm nhân sự phụ trách bảo vệ dữ liệu cá nhân hoặc chỉ định bộ phận có chức năng tương tự	Thời gian ân hạn 2 năm chỉ áp dụng cho trường hợp thành lập doanh nghiệp siêu nhỏ, doanh nghiệp nhỏ, doanh nghiệp vừa, công ty khởi nghiệp không trực tiếp tham gia cung cấp dịch vụ xử lý dữ liệu cá nhân. Ngoài ra, các tổ chức đều được yêu cầu bổ nhiệm nhân sự phụ trách bảo vệ dữ liệu cá nhân.
Bảo vệ dữ liệu và thông báo /báo cáo vi phạm quy định về bảo vệ dữ liệu	Tùy theo vai trò của đơn vị phụ trách dữ liệu, hệ thống phát hiện, phụ trách và thông báo cho các cơ quan có liên quan và chủ thể dữ liệu bị ảnh hưởng trong trường hợp vi phạm quy định tại Nghị định 13 Rà soát các hợp đồng với Bên Xử lý dữ liệu cá nhân để kiểm tra xem hợp đồng đó có các nghĩa vụ và trách nhiệm liên quan đến bảo vệ và bảo mật dữ liệu hay không và làm rõ cách phân bổ trách nhiệm pháp lý giữa các bên	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. Mặt khác, Bên Xử lý dữ liệu cá nhân phải thông báo cho Bên Kiểm soát dữ liệu cá nhân một cách nhanh nhất có thể sau khi nhận thấy có sự vi phạm quy định về bảo vệ dữ liệu cá nhân để họ có thể đáp ứng yêu cầu 72 giờ này. Trường hợp thông báo chậm thì Bên Kiểm soát dữ liệu cá nhân phải đưa ra lý do.
Báo cáo đánh giá tác động cho cơ quan có thẩm quyền để xử lý dữ liệu cá nhân và chuyển dữ liệu cá nhân ra ngước ngoài	Rà soát mẫu đánh giá tác động bảo vệ dữ liệu cá nhân và đánh giá rủi ro hiện có hoặc phát triển theo mẫu của Nghị định 13. Các báo cáo sẽ cần được lưu trữ và sẵn sàng khi có yêu cầu kiểm tra. Có cơ chế để đảm bảo rằng các báo cáo này được lập và nộp mỗi khi hoạt động xử lý trong vòng 60 ngày kể từ ngày tiến hành xử lý dữ liệu cá nhân hoặc khi có sự thay đổi đối với hoạt động xử lý	Cả Bên Kiểm soát dữ liệu và Bên Xử lý dữ liệu đều phải tiến hành đánh giá tác động bảo vệ dữ liệu cá nhân đối với tất cả các hoạt động xử lý của mình, bao gồm tự xử lý dữ liệu cá nhân cơ bản và nhạy cảm hoặc bằng cách ký hợp đồng với bên xử lý dữ liệu cá nhân hoặc cung cấp thông tin cho bên thứ ba hoặc chuyển dữ liệu cá nhân ra nước ngoài và gửi trong vòng 60 ngày kể từ khi bắt đầu hoạt động xử lý dữ liệu. Hồ sơ đánh giá tác động xử lý dữ liệu cá nhân phải bao gồm: thông tin của cả Bên Kiểm soát dữ liệu cá nhân và Bên Xử lý dữ liệu cá nhân và nhân sự phụ trách xử lý dữ liệu cá nhân nội bộ của họ, người nhận dữ liệu cá nhân và quốc tịch của họ, loại và mục đích của dữ liệu cá nhân được xử lý, thời gian lưu giữ, các biện pháp bảo vệ dữ liệu và đánh giá rủi ro và các biện pháp giảm thiểu rủi ro đối với hoạt động xử lý. Đơn vị phụ trách dữ liệu sẽ cần đảm bảo rằng các báo cáo đánh giá tác động luôn có sẵn để Bộ Công an xem xét và được cập nhật, bổ sung trong trường hợp có bất kỳ thông tin nào trong đó thay đổi. Nếu phát hiện có vi phạm hoặc nếu việc chuyển dữ liệu cá nhân vi phạm lợi ích hoặc an ninh quốc gia, Bộ Công an có toàn quyền ngăn chặn mọi hoạt động chuyển dữ liệu cá nhân ra nước ngoài.
Thanh tra và kiểm tra	Có cơ chế và nhân sự được giao nhiệm vụ giải quyết các yêu cầu thanh tra, kiểm tra của các cơ quan chức năng	Nghị định 13 trao cho các cơ quan quyền hành khá rộng trong việc tiến hành thanh tra và kiểm tra các hoạt động và chính sách quản lý dữ liệu cá nhân của bất kỳ đơn vị xử lý dữ liệu nào trên cơ sở hàng năm hoặc nhiều hơn khi cần thiết.

Liên hệ với chúng tôi

Hà Nội

Tầng 46, Tòa tháp Keangnam Landmark 72,
E6 Phạm Hùng, Mễ Trì, Nam Từ Liêm

T +84 (24) 3946 1600

Tp. Hồ Chí Minh

Tầng 10, Tòa nhà Sun Wah,
115 Nguyễn Huệ, Bến Nghé, Quận 1

T +84 (28) 3821 9266

Đà Nẵng

Lô D3, Tầng 5, Tòa nhà Indochina Riverside Towers,
74 Bạch Đằng, Hải Châu I, Hải Châu

T +84 (236) 351 9051

Quét mã QR để truy cập website: kpmg.com.vn

Email: kpmghcmc@kpmg.com.vn