KPMG

Cập Nhật Pháp Luật

Tháng 6 năm 2021

Cập nhật pháp luật - Dự thảo Nghị định về bảo vệ dữ liệu cá nhân tại Việt Nam và những điều mà doanh nghiệp cần biết

Tổng quan

Gần đây, Chính phủ đã công bố bản dự thảo thứ hai cho Nghị định về bảo vệ dữ liệu cá nhân tại Việt Nam. Nghị định về bảo vệ dữ liệu cá nhân, dự kiến có hiệu lực vào tháng 12 năm 2021, đưa ra nhiều quy định và yêu cầu tuân thủ mới và sẽ tác động tới nhiều tổ chức và doanh nghiệp hoạt động trong lĩnh vực liên quan tới dữ liệu cá nhân.

Phạm vi điều chỉnh rộng

Phạm vi điều chỉnh của dự thảo Nghị định bao gồm mọi dữ liệu cá nhân của công dân Việt Nam bất kể việc xử lý dữ liệu đó được thực hiện ở trong hay ngoài Việt Nam. Thêm vào đó, hoạt động "xử lý dữ liệu cá nhân" mang ý nghĩa rất rộng, bao hàm *"một hoặc nhiều hành động tác động tới dữ liệu cá nhân, bao gồm thu thập, ghi, phân tích, lưu trữ, thay đổi, tiết lộ, cấp quyền truy cập, truy xuất, thu hồi, mã hóa, giải mã, sao chép, chuyển giao, xóa, hủy dữ liệu cá nhân hoặc các hành động khác có liên quan"*. Điều này đồng nghĩa với việc các tổ chức nước ngoài, cơ quan, cá nhân, kể cả các mạng xã hội quốc tế và trang thông tin điện tử nước ngoài sẽ đều phải tuân thủ theo quy định của Nghị định này nếu có bất kỳ hoạt động nào liên quan đến dữ liệu cá nhân của công dân Việt Nam.

Thành lập Ủy ban bảo vệ dữ liệu cá nhân

Dự thảo Nghị định quy định về việc thành lập Ủy ban bảo vệ dữ liệu cá nhân đặt tại Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao trực thuộc Bộ Công an. Chức năng, nhiệm vụ chính của Ủy ban bảo vệ dữ liệu cá nhân là giám sát và đảm bảo việc tuân thủ các quy định về bảo vệ dữ liệu cá nhân được nêu tại Nghị định. Ủy ban bảo vệ dữ liệu cá nhân có quyền thanh tra, kiểm tra việc tuân thủ không quá 2 lần/năm tại một tổ chức/công ty, nhưng có quyền thực hiện điều tra bổ sung trong trường hợp có nghi ngờ về việc vi phạm quy định về bảo vệ dữ liệu cá nhân.

Một cổng thông tin quốc gia về bảo về dữ liệu cá nhân sẽ được thành lập để đăng tải các đánh giá và xếp hạng của Ủy ban bảo vệ dữ liệu cá nhân đối với các cơ quan và tổ chức về độ tin cậy trong việc bảo vệ dữ liệu cá nhân.

Dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm

Một nội dung đáng chú ý là dự thảo Nghị định lần này đưa ra một định nghĩa thống nhất cho khái niệm dữ liệu cá nhân mà trước đây được sử dụng rài rác ở các luật và quy định khác. Cụ thể, dữ liệu cá nhân được phân thành 2 loại:

– Dữ liệu cá nhân cơ bản: bao gồm những dữ liệu không chỉ dùng để xác định nhân thân như tên, ngày sinh, ngày mất, số điện thoại, trình độ học vấn, tình trạng hôn nhân, dân tộc, giới tính, mà còn nhóm máu và các dữ liệu phản ánh lịch sử hoạt động trên mạng;

– Dữ liệu cá nhân nhạy cảm: bao gồm những dữ liệu về quan điểm chính trị và tôn giáo, tình trạng sức khỏe, sinh trắc học, di truyền, xu hướng tình dục, tiền án, tài chính, vị trí địa lý thực tế và các mối quan hệ xã hội.

Các chủ thể muốn có quyền được xử lý các dữ liệu cá nhân nhạy cảm sẽ phải tuân thủ các quy định nghiêm ngặt hơn, ví dụ như quy định hạn chế về tiết lộ thông tin và yêu cầu đăng ký với Ủy ban bảo vệ dữ liệu cá nhân khi xử lý dữ liệu cá nhân nhạy cảm (được giải thích rõ hơn ở bên dưới).

Các yêu cầu tuân thủ đối với bên xử lý dữ liệu

Bên xử lý dữ liệu cá nhân phải tuân thủ các quy định sau đây:

(i) Phải có sự đồng ý trên tinh thần tự nguyện từ chủ thể dữ liệu và sự đồng ý phải được trình bày ở một định dạng mà có thể in, sao chép bằng văn bản.

Đáng lưu ý là sự im lặng hoặc không phản hồi của chủ thể dữ liệu không được xem là sự đồng ý.

Sự đồng ý sẽ có hiệu lực trong suốt thời gian tồn tại của chủ thể dữ liệu, trừ trường hợp chủ thể dữ liệu có quyết định khác. Tuy nhiên, đối với các hoạt động của cơ quan nhà nước, sự đồng ý của chủ thể dữ liệu sẽ có hiệu lực trong 20 năm sau khi chủ thể dữ liệu chết.

(ii) Phải thông báo cho chủ thể dữ liệu về mọi hoạt động xử lý dữ liệu, trừ trường hợp:

- Chủ thể dữ liệu đã đồng ý toàn bộ với nội dung và việc xử lý dữ liệu cá nhân;
- Việc xử lý dữ liệu cá nhân được quy định bởi pháp luật;
- Việc xử lý dữ liệu cá nhân không ảnh hưởng đến quyền và lợi ích của chủ thể dữ liệu và việc thông báo cho chủ thể dữ liệu là không thể;
- Việc xử lý dữ liệu cá nhân cho mục đích phục vụ nghiên cứu khoa học và thống kê.

(iii) Phải đăng ký với Ủy ban bảo vệ dữ liệu cá nhân trước khi (a) xử lý dữ liệu cá nhân nhạy cảm, và (b) chuyển dữ liệu cá nhân qua biên giới.

Hồ sơ đăng ký phải bao gồm:

- Đơn đăng ký gồm các nội dung bao gồm, nhưng không bị giới hạn bởi, thông tin chi tiết của bên xử lý dữ liệu, mục đích xử lý/chuyển dữ liệu, loại và nguồn của dữ liệu, mô tả chi tiết về các biện pháp bảo vệ dữ liệu;
- Bản báo cáo đánh giá tác động, bao gồm mô tả chi tiết về các hoạt động xử lý dữ liệu, đánh giá tác hại tiềm ẩn có thể gây ra đối với chủ thể dữ liệu và các biện pháp bảo vệ được đề xuất để giảm thiểu các mối nguy hại đó;
- Các văn bản liên quan khác.

Ngoài việc phải được sự chấp thuận từ phía Ủy ban bảo vệ dữ liệu cá nhân, việc chuyển dữ liệu cá nhân của công dân Việt Nam qua biên giới cần phải thỏa mãn thêm các điều kiện sau:

- Có được sự đồng ý từ chủ thể dữ liệu;
- Bản gốc của dữ liệu được lưu trữ tại Việt Nam; và
- Bên xử lý dữ liệu phải văn bản chứng minh rằng quốc gia hay vùng lãnh thổ nhận chuyển dữ liệu có mức bảo vệ dữ liệu cá nhân bằng hoặc cao hơn mức được yêu cầu bởi Nghị định.

Ngoài ra, bên xử lý dữ liệu sẽ phải thiết lập một hệ thống lưu trữ lịch sử chuyển dữ liệu trong ba năm.

Hi vọng Chính phủ sẽ quy định về khoản thời gian chuyển tiếp phù hợp để các bên xử lý dữ liệu có đủ thời gian chuẩn bị cho việc đáp ứng các yêu cầu của quy định, đồng thời cơ quan có thẩm quyền sẽ phân bổ đủ nguồn lực để có thể giải quyết nhanh chóng các hồ sơ đăng ký từ các doanh nghiệp có ý định lưu trữ dữ liệu ở nước ngoài.

(iv) Phải áp dụng các biện pháp vật lý, kỹ thuật, và quản lý để bảo vệ dữ liệu cá nhân;

(v) Phải xây dựng và ban hành chính sách nội bộ về việc bảo vệ dữ liệu cá nhân phù hợp với Nghị định này.

Các chính sách nội bộ cần đáp ứng những nội dung được yêu cầu bởi Nghị định và phải được thẩm định bởi Ủy ban bảo vệ dữ liệu cá nhân trước khi được ban hành.

Các trường hợp được phép xử lý dữ liệu mà không cần sự đồng ý của chủ thể dữ liệu

Dự thảo Nghị định cho phép bên xử lý dữ liệu được xử lý và chia sẻ dữ liệu cá nhân mà không cần sự đồng ý của chủ thể dữ liệu trong các trường hợp liên quan tới an ninh quốc gia và trật tự công cộng; các trường hợp khẩn cấp đe doa tới sức khỏe và tự do của chủ thể dữ liệu hoặc cộng đồng; phục vụ mục đích điều tra các vi phạm pháp luật; nghiên cứu và thu thập dữ liệu hoặc các trường hợp khác theo quy định của pháp luật Việt Nam và các điều ước quốc tế. Tuy nhiên, dự thảo Nghị định không nói rõ các trường hợp nêu trên liệu có bao gồm việc điều tra nội bộ của doanh nghiệp đối với người lao động hay không.

Xử lý vi phạm

Dự thảo Nghị định cũng ban hành cơ chế xử lý vi phạm về bảo vệ dữ liệu cá nhân với mức phạt hành chính từ 50.000.000 VND đến 100.000.000 VND (khoảng từ 2.000 USD đến 4.350 USD) tùy theo tính chất và mức độ của hành vi vi phạm. Bên xử lý dữ liệu còn có thể bị cấm thực hiện xử lý hoặc chuyển dữ liệu tạm thời hoặc vĩnh viễn. Đối với việc vi phạm nhiều lần, bên vi phạm có thể bị tước quyền xử lý dữ liệu và xử phạt với mức phạt lên đến 5% tổng doanh thu tại Việt Nam.

Dự thảo Nghị định hiện trao cho các cơ quan có thẩm quyền nhiều quyền quyết định trong việc áp dụng các quy định về bảo vệ dữ liệu cá nhân. Hi vọng rằng các cơ quan này sẽ sớm ban hành các văn bản hướng dẫn để cụ thể hóa việc triển khai thực hiện Nghị định trên thực tế.

Doanh nghiệp cần làm gì để chuẩn bị tốt nhất cho việc thực hiện Nghị định này?

Dự thảo Nghị định này đưa ra một nguyên tắc: tổ chức/doanh nghiệp phải tích hợp giải pháp bảo vệ dữ liệu vào từng hoạt động có liên quan đến dữ liệu cá nhân (nguyên tắc "privacy by design"). Để đạt được điều này, các tổ chức/doanh nghiệp cần phải có sự đánh giá toàn diện đối với các quy trình hoạt động kinh doanh, các hồ sơ và biểu mẫu hiện hành để có thể đáp ứng ngay khi Nghị định được ban hành và có hiệu lực. Điều này sẽ đạt được thông qua việc triển khai kế hoạch bảo vệ dữ liệu. Sau đây là một số gợi ý mà tổ chức/doanh nghiệp có thể thực hiện để khởi động kế hoạch này:

1. Xác định rõ các nguồn và vị trí lưu trữ dữ liệu, ví dụ: dữ liệu có thể được lưu trữ tại nhiều hệ thống khác nhau (tại trụ sở hay trên điện toán đám mây), ai có quyền truy cập để đánh giá rủi ro, tổn hại đối với dữ liệu. Cần lưu ý rằng, việc lưu trữ dữ liệu khách hàng tại nhiều nguồn khác nhau về bản chất không phải là một hành vi vi phạm, nhưng cần được hỗ trợ bởi một hệ thống quản lý rõ ràng và các đợt kiểm tra định kỳ để đảm bảo tuân thủ các quy định mới.
2. Kiểm tra việc thu thập các dữ liệu hiện hành có quan trọng và liên quan đến hoạt động kinh doanh không, kiểm tra quy trình xóa bỏ dữ liệu để xác định dữ liệu đã được lưu trữ có cần thiết không; nếu cần thiết thì cần kiểm tra sự cần thiết của việc mã hóa dữ liệu;
3. Cập nhật công nghệ và các chứng nhận liên quan;
4. Thiết lập và áp dụng các cơ chế phòng vệ cho toàn hệ thống để ngăn chặn các hành vi vi phạm về bảo vệ dữ liệu;
5. Kiểm tra với các bên cung cấp dịch vụ để đảm bảo việc cung cấp biện pháp bảo vệ dữ liệu cần thiết;
6. Rà soát biểu mẫu hiện hành dùng để lấy chấp thuận của chủ thể dữ liệu để đảm bảo không còn thông tin về sự im lặng hoặc không phản hồi của chủ thể dữ liệu được xem là sự đồng ý;
7. Rà soát/ban hành các chính sách và thủ tục về quyền riêng tư để đảm bảo phù hợp với quy định mới.

Vì những quy định trong dự thảo Nghị định đa phần được xây dựng dựa trên các nguyên tắc của Quy định chung về bảo mật thông tin của Liên minh Châu Âu (GDPR), những tổ chức/doanh nghiệp nào đã xây dựng các tiêu chuẩn về bảo vệ dữ liệu theo GDPR sẽ không gặp nhiều khó khăn trong việc cập nhật và tuân thủ khi các quy định của Việt Nam về dữ liệu cá nhân khi có hiệu lực.

Dự thảo của Nghị định vẫn có thể sẽ bị thay đổi sau quá trình lấy đóng góp ý kiến từ công chúng, tuy nhiên, chúng tôi nhận định rằng các góp ý sẽ không thay đổi việc Chính phủ sẽ ban hành một hành lang pháp lý nghiêm ngặt hơn về việc bảo vệ dữ liệu cá nhân trong thời gian sắp tới.

Liên hệ với chúng tôi

Hà Nội

Tầng 46, Tòa tháp Keangnam Landmark 72,
Lô E6, Đường Phạm Hùng, Phường Mễ Trì,
Quận Nam Từ Liêm, Hà Nội, Việt Nam

T: +84 (24) 3946 1600
F: +84 (24) 3946 1601
E: kpmghanoi@kpmg.com.vn

Tp. Hồ Chí Minh

Tầng 10, Tòa nhà Sun Wah,
115 Nguyễn Huệ, Phường Bến Nghé,
Quận 1, Tp. Hồ Chí Minh, Việt Nam

T: +84 (28) 3821 9266
F: +84 (28) 3821 9267
E: kpmghcmc@kpmg.com.vn

Đà Nẵng

Lô D3, Tầng 5, Tòa nhà văn phòng Indochina Riverside Towers,
74 Bạch Đằng, Phường Hải Châu I, Quận Hải Châu,
Tp. Đà Nẵng, Việt Nam

T: +84 (236) 351 9051
F: +84 (236) 351 9051
E: kpmgdanang@kpmg.com.vn

Theo dõi chúng tôi trên:

kpmg.com.vn