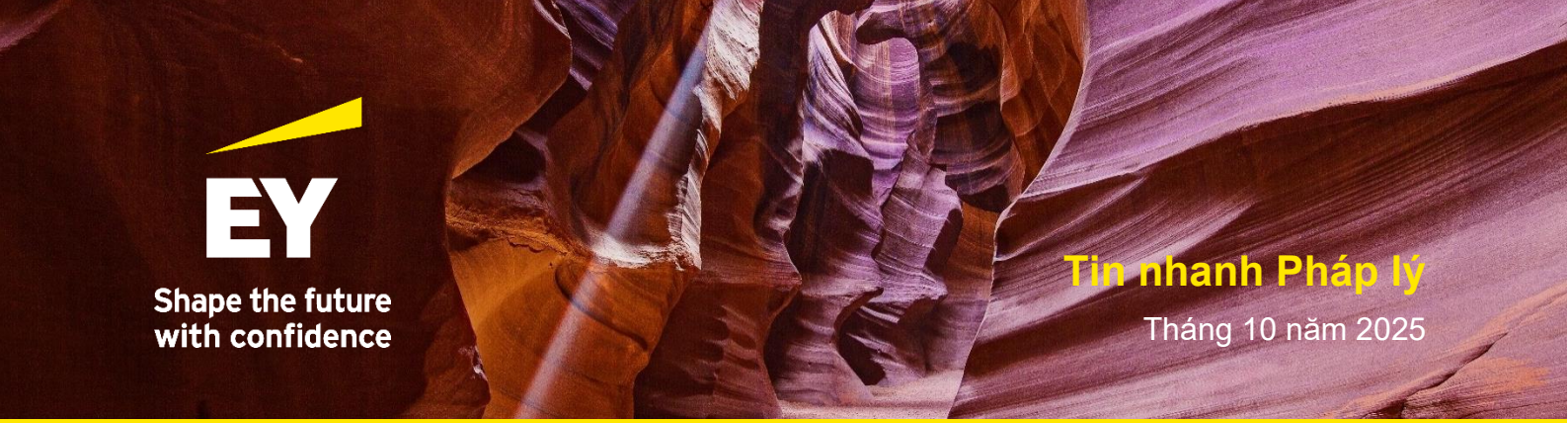


Shape the future with confidence

Tin nhanh Pháp lý

Tháng 10 năm 2025

Xem thêm các Tin nhanh khác tại đây.

Dự thảo Nghị định quy định chi tiết một số điều của Luật Bảo vệ dữ liệu cá nhân

Bản tin này đề cập các yêu cầu tuân thủ chính theo Dự thảo Nghị định quy định chi tiết một số điều của Luật Bảo vệ dữ liệu cá nhân

Sau khi Luật Bảo vệ dữ liệu cá nhân năm 2025 (Luật BVDLCN) được ban hành ngày 26 tháng 6 năm 2025, Bộ Công an đã công bố Dự thảo Nghị định quy định chi tiết một số điều của Luật BVDLCN (Dự thảo Nghị định) để lấy ý kiến. Dự thảo Nghị định này hướng đến làm rõ các yêu cầu và điều kiện bảo vệ dữ liệu cá nhân, cũng như quy trình và cơ chế thực thi theo Luật BVDLCN mới, đánh dấu một bước tiến quan trọng trong việc hình thành khung pháp lý toàn diện về bảo vệ dữ liệu cá nhân tại Việt Nam.

Một số điểm chính nổi bật trong Dự thảo Nghị định bao gồm:

- Khái niệm và phân loại dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm
- Thực hiện quyền của chủ thể dữ liệu
- Chuyển giao dữ liệu cá nhân
- Nhân sự bảo vệ dữ liệu hoặc bộ phận bảo vệ dữ liệu
- Đánh giá tác động xử lý dữ liệu cá nhân và đánh giá tác động chuyển dữ liệu xuyên biên giới
- Thông báo vi phạm quy định về bảo vệ dữ liệu cá nhân
- Dịch vụ xử lý dữ liệu cá nhân
- Bảo vệ dữ liệu cá nhân theo lĩnh vực cụ thể
- Kiểm tra hoạt động bảo vệ dữ liệu cá nhân
- Trường hợp miễn trừ

Dự kiến Nghị định sẽ được ban hành và có hiệu lực từ ngày 1 tháng 1 năm 2026. Do vậy, chúng tôi đưa ra một số khuyến nghị về kế hoạch thực hiện doanh nghiệp cần quan tâm chuẩn bị càng sớm càng tốt cho việc tuân thủ.

1. Khái niệm và phân loại dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm

- Dữ liệu cá nhân cơ bản: Khác với cách tiếp cận liệt kê tại Nghị định 13/2023/NĐ-CP (Nghị định 13), Dự thảo Nghị định định nghĩa dữ liệu cá nhân cơ bản theo phương thức loại trừ, tức là bao gồm toàn bộ dữ liệu cá nhân không thuộc danh mục dữ liệu cá nhân nhạy cảm.

- Dữ liệu cá nhân nhạy cảm: Dự thảo Nghị định đã đưa ra hướng dẫn chi tiết hơn, xác định dữ liệu cá nhân nhạy cảm yêu cầu phân quyền giới hạn truy cập, quy trình xử lý và các biện pháp bảo mật chặt chẽ. Ngoài các loại dữ liệu nhạy cảm được liệt kê tại Nghị định 13, Dự thảo Nghị định đã bổ sung cụ thể:

  (i) Quan điểm tín ngưỡng

  (ii) Danh tính điện tử của cá nhân

  (iii) Tên đăng nhập, mật khẩu truy cập của tài khoản; thông tin thẻ ngân hàng, dữ liệu về lịch sử giao dịch của tài khoản ngân hàng; thông tin tài chính, tín dụng và các thông tin khác liên quan đến hoạt động giao dịch tài chính, chứng khoán, bảo hiểm của khách hàng tại các tổ chức tín dụng, chi nhánh ngân hàng nước ngoài, tổ chức cung ứng dịch vụ trung gian thanh toán, chứng khoán, bảo hiểm, các tổ chức được phép khác

  (iv) Dữ liệu về hoạt động, lịch sử hoạt động của thuê bao viễn thông

  (v) Dữ liệu theo dõi hành vi, hoạt động sử dụng dịch vụ viễn thông, mạng xã hội, dịch vụ truyền thông trực tuyến và các dịch vụ khác trên không gian mạng

  (vi) Dữ liệu cá nhân khác do tổ chức, cá nhân xác định cần có biện pháp bảo mật chặt chẽ

  Với việc bổ sung nhóm (vi), Dự thảo Nghị định đã mở rộng khái niệm dữ liệu cá nhân nhạy cảm vượt ra ngoài các loại dữ liệu được liệt kê trong luật, đồng thời trao cho tổ chức sự linh hoạt và trách nhiệm trong việc bảo đảm an toàn cho các dữ liệu cá nhân quan trọng.

2. Thực hiện quyền của chủ thể dữ liệu

- **Quyền đồng ý**

  - Sự đồng ý rõ ràng và có thể kiểm chứng: Bên kiểm soát dữ liệu, bên kiểm soát và xử lý dữ liệu lấy sự đồng ý của chủ thể dữ liệu cá nhân đảm bảo minh chứng rõ ràng, chính xác về phương thức, thời gian, nội dung và xác thực chủ thể dữ liệu cá nhân.

  - Hình thức thể hiện sự đồng ý hợp lệ: Sự đồng ý phải đảm bảo có thể kiểm chứng được tính chính xác và có thể được thực hiện thông qua thư điện tử, trang thông tin điện tử, nền tảng, ứng dụng có thiết lập kỹ thuật xin sự đồng ý.

  - Cấm cài đặt sẵn hoặc gây hiểu nhầm: Bên kiểm soát dữ liệu, bên kiểm soát và xử lý dữ liệu không được thiết lập mặc định đồng ý hoặc tạo ra các chỉ dẫn không rõ ràng, gây hiểu lầm giữa đồng ý và không đồng ý cho chủ thể dữ liệu. Các thiết lập mặc định sẵn có phải đảm bảo nguyên tắc bảo vệ dữ liệu cá nhân, tôn trọng các quyền của chủ thể dữ liệu cá nhân.

- **Quyền rút lại sự đồng ý, hạn chế xử lý dữ liệu cá nhân, phản đối xử lý dữ liệu cá nhân, xem, chỉnh sửa hoặc yêu cầu chỉnh sửa, cung cấp, xóa dữ liệu cá nhân**

  Bên kiểm soát dữ liệu, bên kiểm soát và xử lý dữ liệu phải xây dựng quy trình, thủ tục, biểu mẫu rõ ràng để bảo đảm chủ thể dữ liệu có thể thực hiện rút lại sự đồng ý cho phép xử lý dữ liệu cá nhân, hạn chế xử lý dữ liệu cá nhân, phản đối xử lý dữ liệu cá nhân cũng như quyền xem, chỉnh sửa hoặc yêu cầu chỉnh sửa, cung cấp, xóa dữ liệu cá nhân, với thời hạn cụ thể như sau:

  - Thời hạn phản hồi: trong vòng hai ngày làm việc

- Thời hạn thực hiện:

  (i) Đối với yêu cầu rút lại sự đồng ý, hạn chế hoặc phản đối xử lý: phải hoàn thành trong vòng bảy ngày làm việc

  (ii) Đối với yêu cầu xem, chỉnh sửa hoặc yêu cầu chỉnh sửa, được cung cấp dữ liệu và xóa dữ liệu: phải hoàn thành trong vòng 10 đến 15 ngày làm việc, tùy thuộc vào việc có liên quan đến bên xử lý dữ liệu hoặc bên thứ ba hay không

- Gia hạn: Việc xử lý có thể được kéo dài thêm tối đa 10 ngày làm việc trong trường hợp yêu cầu phức tạp, với điều kiện phải thông báo cho chủ thể dữ liệu về lý do gia hạn

3. Chuyển giao dữ liệu cá nhân

- Chuyển giao dữ liệu cá nhân khi có sự đồng ý, hoặc chuyển dữ liệu để tiếp tục xử lý trong trường hợp tái cơ cấu, tổ chức lại đơn vị, doanh nghiệp, tổ chức, hoặc chuyển từ bên kiểm soát dữ liệu, bên kiểm soát và xử lý dữ liệu sang bên xử lý dữ liệu hoặc bên thứ ba để xử lý: phải có thỏa thuận bằng văn bản, trong đó nêu rõ mục đích, chủ thể dữ liệu, loại dữ liệu, thời hạn xử lý, việc xóa dữ liệu, cơ sở pháp lý và trách nhiệm của các bên.

- Chuyển giao dữ liệu cá nhân nhạy cảm: phải có biện pháp mã hóa, ẩn danh hóa và biện pháp bảo mật vật lý.

- Chuyển giao dữ liệu cá nhân có thu phí: phải có sự đồng ý rõ ràng, giới hạn trong mục đích chuyển giao, xác định rõ vai trò của các bên và có thỏa thuận trước khi chuyển dữ liệu.

- Chuyển dữ liệu nội bộ trong cùng một tổ chức: phải xây dựng chính sách và phòng chống việc chia sẻ trái phép.

- Giao dịch dữ liệu: Dữ liệu phải được khử nhận dạng trước khi giao dịch trên sàn dữ liệu.

4. Nhân sự bảo vệ dữ liệu (DPO) hoặc bộ phận bảo vệ dữ liệu (DPD)

Theo quy định của Luật BVDLCN, doanh nghiệp có nghĩa vụ: (i) bổ nhiệm nội bộ DPO hoặc thành lập nội bộ DPD và/ hoặc (ii) thuê tổ chức, cá nhân bên ngoài cung cấp dịch vụ bảo vệ dữ liệu cá nhân.

Dự thảo Nghị định hướng dẫn cụ thể hơn về việc chỉ định DPO/DPD như sau:

- Điều kiện năng lực đối với DPO nội bộ: (i) Trình độ đại học, (ii) có ít nhất ba năm kinh nghiệm công tác liên quan đến một trong các lĩnh vực pháp chế, xử lý dữ liệu cá nhân, an ninh mạng, an ninh dữ liệu, quản trị rủi ro, quản lý tuân thủ, (iii) có chứng nhận hoàn thành khóa học bồi dưỡng kiến thức, kỹ năng cơ bản về bảo vệ dữ liệu cá nhân do tổ chức đủ năng lực đào tạo tại Việt Nam cấp, (iv) đạt yêu cầu tại chương trình đánh giá chuyên môn về bảo vệ dữ liệu cá nhân do A05 tổ chức, (v) am hiểu quy định pháp luật về bảo vệ dữ liệu cá nhân và hoạt động xử lý dữ liệu cá nhân của cơ quan, tổ chức, và (vi) không có tiền án trong lĩnh vực dữ liệu, công nghệ thông tin, mạng viễn thông

- Điều kiện năng lực đối với DPD nội bộ: Nhân sự trong DPD phải đáp ứng đủ các điều kiện năng lực như DPO nội bộ.

- Điều kiện năng lực đối với cá nhân cung cấp dịch vụ bảo vệ dữ liệu cá nhân: tương tự DPO, ngoại trừ yêu cầu có ít nhất năm năm kinh nghiệm liên quan

- Điều kiện năng lực đối với tổ chức cung cấp dịch vụ bảo vệ dữ liệu cá nhân: (i) hoạt động trong lĩnh vực công nghệ, pháp lý hoặc tư vấn, (ii) có ít nhất ba nhân sự đáp ứng tiêu chuẩn của cá nhân cung cấp dịch vụ bảo vệ dữ liệu cá nhân; (iii) đã cung cấp các sản phẩm, dịch vụ liên quan đến bảo mật, an ninh mạng, công nghệ thông tin, đánh giá tiêu chuẩn, tư vấn về bảo vệ dữ liệu cá nhân. Tổ chức cung cấp dịch vụ phải chuẩn bị hồ sơ năng lực chứng minh khả năng bảo vệ dữ liệu cá nhân.

Trách nhiệm của DPO và DPD là xây dựng và triển khai chính sách, quy trình và biện pháp kỹ thuật nhằm bảo đảm tuân thủ pháp luật về bảo vệ dữ liệu cá nhân; thực hiện quyền của chủ thể dữ liệu; đánh giá thực trạng tuân thủ và ứng phó với vi phạm hoặc hoạt động chuyển dữ liệu xuyên biên giới. Họ cũng phải triển khai đào tạo, thực hiện đánh giá tác động, và tư vấn cho tổ chức về các quyết định liên quan đến bảo vệ dữ liệu cá nhân. Trong khi đó, trách nhiệm của cá nhân, tổ chức cung cấp dịch vụ bảo vệ dữ liệu cá nhân chỉ giới hạn trong phạm vi dịch vụ đã thỏa thuận.

5. Đánh giá tác động xử lý dữ liệu cá nhân (DPIA) và đánh giá tác động chuyển dữ liệu xuyên biên giới (CTIA)

Dự thảo Nghị định bổ sung một trường hợp miễn trừ đáng chú ý đối với CTIA, cụ thể là: "Hoạt động chuyển dữ liệu cá nhân xuyên biên giới để quản lý nhân sự xuyên biên giới theo quy tắc, quy chế lao động và thỏa ước lao động tập thể theo quy định của pháp luật". Quy định này cho thấy sự giảm bớt gánh nặng tuân thủ đối với các công ty đa quốc gia thực hiện quản lý dữ liệu nhân sự ở nhiều quốc gia.

Ngược lại, yêu cầu về hồ sơ DPIA và CTIA lại nghiêm ngặt hơn đáng kể so với quy định tại Nghị định 13. Hồ sơ CTIA và DPIA phải bao gồm sơ đồ luồng dữ liệu; phương án bảo đảm an toàn dữ liệu cá nhân (sau khi chuyển đối với CTIA), các biện pháp và tiêu chuẩn bảo vệ dữ liệu cá nhân áp dụng; sơ đồ hệ thống và mô tả hệ thống lưu trữ, xử lý dữ liệu (sau khi chuyển đối với CTIA); quy trình về việc bên tiếp nhận dữ liệu chuyển giao, cung cấp dữ liệu cá nhân cho bên thứ ba (đối với CTIA); kết quả tự đánh giá tuân thủ và tài liệu chứng minh bảo đảm quyền của chủ thể dữ liệu; đánh giá mức độ bảo vệ dữ liệu của bên nhận (đối với CTIA).

Các trường hợp và thời hạn cập nhật hồ sơ DPIA và CTIA cũng được làm rõ trong Dự thảo Nghị định:

- Cập nhật định kỳ sáu tháng một lần khi: (i) phát sinh mục đích chuyển hoặc xử lý dữ liệu mới; hoặc (ii) thay đổi về bên kiểm soát dữ liệu, bên kiểm soát và xử lý dữ liệu, bên xử lý dữ liệu, bên thứ ba.
- Cập nhật ngay trong vòng 60 ngày nếu: tổ chức bị tổ chức lại, chấm dứt hoạt động, giải thể hoặc phá sản; có thay đổi về tổ chức, cá nhân cung cấp dịch vụ bảo vệ dữ liệu cá nhân; hoặc phát sinh ngành nghề, dịch vụ mới hoặc thay đổi ngành nghề, dịch vụ liên quan đến dữ liệu cá nhân đã được đăng ký trong hồ sơ DPIA, CTIA.

6. Thông báo vi phạm quy định về bảo vệ dữ liệu cá nhân

Đối với dữ liệu vị trí và dữ liệu sinh trắc học, ngoài việc phải thông báo cho A05, bên kiểm soát dữ liệu hoặc bên kiểm soát và xử lý dữ liệu còn có nghĩa vụ (i) thông báo cho các chủ thể dữ liệu bị ảnh hưởng trong thời hạn 72 giờ kể từ thời điểm phát hiện vi phạm, hoặc (ii) trường hợp vì lý do kỹ thuật hoặc khẩn cấp khiến không thể thông báo cho tất cả các chủ thể bị ảnh hưởng trong thời hạn 72 giờ, phải thông báo công khai bằng phương tiện điện tử và gửi thông báo cá nhân hóa ngay khi điều kiện kỹ thuật cho phép. Hồ sơ vi phạm phải được lưu tối thiểu năm năm.

7. Dịch vụ xử lý dữ liệu cá nhân

Trước sự gia tăng mạnh mẽ của các hoạt động liên quan đến dữ liệu cá nhân, nhà làm luật đã siết chặt giám sát bằng cách phân dịch vụ xử lý dữ liệu cá nhân vào ngành, nghề kinh doanh có điều kiện, phải đáp ứng yêu cầu về nhân sự, xin cấp giấy chứng nhận đủ điều kiện kinh doanh từ A05, và tuân thủ các nghĩa vụ trong quá trình hoạt động.

Dịch vụ xử lý dữ liệu cá nhân bao gồm:

- Cung cấp và vận hành hệ thống, phần mềm tự động để để thay mặt bên kiểm soát, bên kiểm soát và xử lý dữ liệu tiến hành xử lý dữ liệu cá nhân
- Chấm điểm, xếp hạng hoặc đánh giá mức độ tín nhiệm của chủ thể dữ liệu
- Thu thập, xử lý dữ liệu cá nhân trực tuyến từ trang web, ứng dụng và mạng xã hội

- Thu thập, xử lý dữ liệu cá nhân qua trang web, ứng dụng, phần mềm và mạng xã hội để khảo sát, nghiên cứu thị trường
- Thu thập, xử lý dữ liệu cá nhân qua trang web, ứng dụng, phần mềm chăm sóc sức khỏe, theo dõi sức khỏe, dịch vụ y tế
- Thu thập, xử lý dữ liệu cá nhân qua ứng dụng, phần mềm giáo dục có yếu tố giám sát như điểm danh, ghi hình, chấm điểm hành vi, nhận diện cảm xúc
- Phân tích và khai thác dữ liệu cá nhân, gồm: sử dụng các công cụ phân tích để tìm kiếm thông tin, xu hướng và mẫu từ dữ liệu cá nhân; áp dụng các phương pháp khai thác dữ liệu để trích xuất giá trị từ dữ liệu cá nhân, dự đoán hành vi người dùng hoặc tối ưu hóa dịch vụ
- Mã hóa dữ liệu cá nhân trong quá trình truyền tải và lưu trữ
- Xử lý dữ liệu cá nhân tự động dựa trên công nghệ dữ liệu lớn, trí tuệ nhân tạo, chuỗi khối, vũ trụ ảo
- Nền tảng ứng dụng cung cấp dữ liệu vị trí cá nhân

8. Bảo vệ dữ liệu cá nhân theo lĩnh vực cụ thể

Dự thảo Nghị định đưa ra định nghĩa về dữ liệu lớn, trí tuệ nhân tạo, công nghệ chuỗi khối, vũ trụ ảo, đồng thời làm rõ nghĩa vụ bảo vệ dữ liệu cá nhân theo từng lĩnh vực chuyên ngành theo quy định của Luật BVDLCN.

- **Đối với hoạt động tài chính, ngân hàng, hoạt động thông tin tín dụng**
  - Tuân thủ các tiêu chuẩn quốc tế và tiêu chuẩn Việt Nam về bảo vệ dữ liệu và an ninh mạng
  - Thực hiện đánh giá tuân thủ hằng năm
  - Ghi lại nhật ký toàn bộ hoạt động xử lý dữ liệu cá nhân
  - Khi xin sự đồng ý, phải nêu rõ mục đích xử lý dữ liệu, nguồn thu thập dữ liệu và các bên thu thập, chia sẻ, thời gian lưu trữ, cũng như cách thức rút lại sự đồng ý và xóa dữ liệu
  - Thông báo cho các chủ thể dữ liệu bị ảnh hưởng trong vòng 72 giờ nếu xảy ra vi phạm liên quan đến thông tin ngân hàng, tài chính hoặc tín dụng
- **Đối với dữ liệu lớn (xử lý dữ liệu cá nhân trên quy mô lớn, liên tục, tích hợp từ nhiều nguồn khác nhau, có khả năng phân tích hành vi, dự đoán xu hướng hoặc phân loại người dùng)**
  - Áp dụng mã hóa, ẩn danh, giả danh dữ liệu và phân quyền truy cập
  - Giám sát việc truy cập, tiến hành đánh giá an ninh mạng định kỳ và đào tạo nhân sự
  - Ràng buộc bên thứ ba tuân thủ quy định
  - Thông báo cho chủ thể dữ liệu về cách thức dữ liệu được sử dụng
- **Đối với trí tuệ nhân tạo và vũ trụ ảo**
  - Thông báo cho chủ thể dữ liệu về việc xử lý tự động, giải thích ảnh hưởng của thuật toán và đưa ra các lựa chọn để chủ thể dữ liệu có quyền không tham gia
  - Thiết lập hệ thống an minh mạng vững chắc, thiết lập phương án dự phòng chiến lược, xây dựng cơ chế bảo vệ dữ liệu cá nhân theo tiêu chuẩn quốc tế cao nhất và cảnh báo sớm các nguy cơ an ninh mạng, thiết lập cơ chế kiểm soát, ngăn chặn việc lợi dụng trí tuệ nhân tạo, vũ trụ ảo vào các hoạt động xâm phạm an ninh quốc gia, trật tự an toàn xã hội, đánh giá tuân thủ hằng năm, đánh giá tác động bảo vệ dữ liệu cá nhân trước khi triển khai

hệ thống, đặc biệt nếu có khả năng ảnh hưởng nghiêm trọng đến quyền chủ thể dữ liệu cá nhân

- Cơ quan có thẩm quyền có quyền yêu cầu hủy thuật toán trí tuệ nhân tạo trong trường hợp vi phạm về bảo vệ dữ liệu cá nhân.

- **Đối với điện toán đám mây**
  - Hợp đồng với nhà cung cấp dịch vụ điện toán đám mây phải quy định rõ việc tuân thủ pháp luật Việt Nam về bảo vệ dữ liệu, vai trò và trách nhiệm của các bên, luồng xử lý dữ liệu, biện pháp bảo mật, thông báo thay đổi, thời hạn lưu trữ, việc xóa dữ liệu và bảo đảm quyền của chủ thể dữ liệu.
  - Nhà cung cấp dịch vụ điện toán đám mây phải tuân thủ pháp luật Việt Nam về bảo vệ dữ liệu, đề nghị các nhà thầu phụ tuân thủ và áp dụng biện pháp kỹ thuật, tổ chức phù hợp với quy mô và mức độ xử lý dữ liệu.
  - Dữ liệu cá nhân phải được mã hóa ở trạng thái nghỉ và truyền, kèm theo phân quyền truy cập nghiêm ngặt.
- **Đối với công nghệ chuỗi khối**
  - Không lưu trữ trực tiếp dữ liệu cá nhân trên chuỗi khối; chỉ lưu trữ khi dữ liệu cá nhân đã được mã hóa hoặc lưu trữ giá trị băm của dữ liệu cá nhân
  - Chỉ áp dụng các thuật toán mã hóa, thuật toán băm đảm bảo an toàn
  - Thực hiện đánh giá tuân thủ quy định về bảo vệ dữ liệu hằng năm
  - Thực hiện đánh giá tác động bảo vệ dữ liệu trước khi triển khai công nghệ, đặc biệt nếu có khả năng ảnh hưởng nghiêm trọng đến quyền chủ thể dữ liệu cá nhân

9. Kiểm tra hoạt động bảo vệ dữ liệu cá nhân

Việc kiểm tra hoạt động bảo vệ dữ liệu cá nhân được tiến hành thường xuyên, định kỳ hoặc đột xuất, căn cứ vào hành vi vi phạm pháp luật hoặc thực hiện công tác quản lý nhà nước. Mọi tổ chức, cá nhân có hoạt động xử lý dữ liệu cá nhân, cung cấp dịch vụ xử lý dữ liệu, thực hiện DPIA, CTIA hoặc chứng nhận đủ điều kiện năng lực bảo vệ dữ liệu cá nhân đều có thể thuộc đối tượng kiểm tra. Nội dung kiểm tra bao gồm hiện trạng tuân thủ công tác bảo vệ dữ liệu, hoạt động DPIA, CTIA và hoạt động chứng nhận đủ điều kiện năng lực công nghệ và pháp lý về bảo vệ dữ liệu. A05 sẽ thông báo cho đối tượng kiểm tra trước 15 ngày làm việc, và kết quả kiểm tra được bảo mật.

10. Trường hợp miễn trừ

Quy định miễn trừ về nghĩa vụ thực hiện DPIA, cập nhật DPIA và CTIA, cũng như bổ nhiệm DPO, DPD sẽ không áp dụng đối với tổ chức nhỏ, tổ chức khởi nghiệp, hộ kinh doanh và tổ chức siêu nhỏ khi các tổ chức này:

- Kinh doanh dịch vụ xử lý dữ liệu cá nhân
- Trực tiếp xử lý dữ liệu cá nhân nhạy cảm
- Xử lý dữ liệu cá nhân kể từ thời điểm có quy mô đạt từ 100,000 chủ thể dữ liệu (đối với tổ chức nhỏ, tổ chức khởi nghiệp) hoặc 500,000 chủ thể dữ liệu (đối với hộ kinh doanh và tổ chức siêu nhỏ)

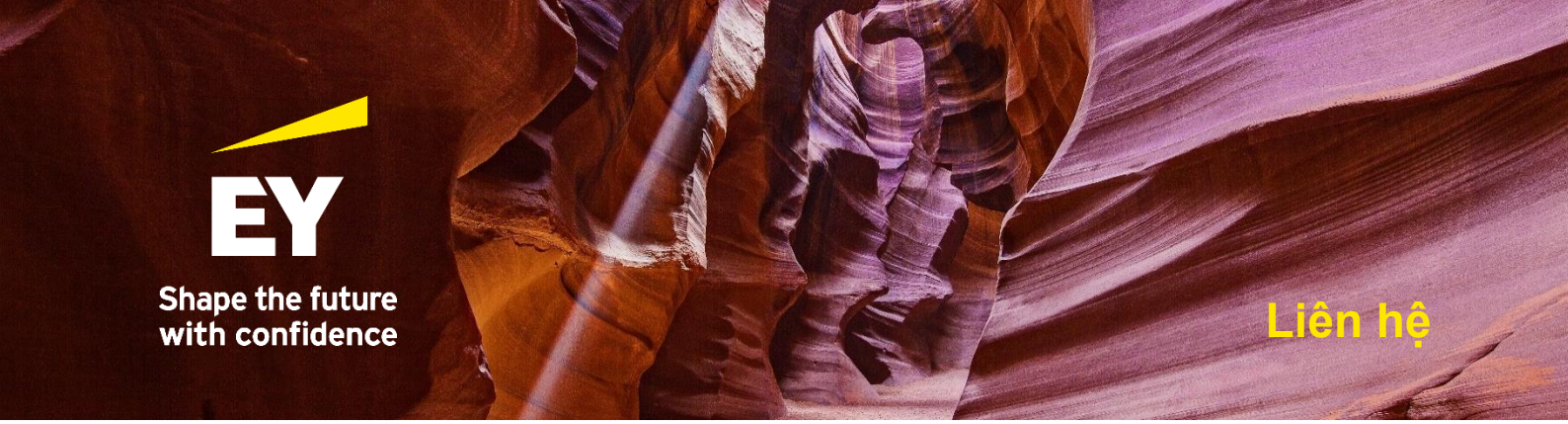
Kế hoạch thực hiện

Dự thảo Nghị định đưa ra những thay đổi quan trọng, mở rộng và làm rõ hơn các nghĩa vụ của tổ chức trong việc xử lý dữ liệu cá nhân, dự kiến có hiệu lực từ ngày 1 tháng 1 năm 2026 cùng với Luật BVDLCN. Những cập nhật này thể hiện sự siết chặt trong quản lý pháp lý và nhấn mạnh yêu cầu các tổ chức cần nhanh chóng hành động để tuân thủ khung pháp lý bảo vệ dữ liệu được tăng cường tại Việt Nam. Một số nhóm hành động liên quan được khuyến nghị nhằm bảo đảm tuân thủ và chuẩn bị cho việc kiểm tra của A05.

- **Tăng cường khung bảo vệ dữ liệu cá nhân:** Tổ chức phải rà soát và sửa đổi khung bảo vệ dữ liệu cá nhân hiện tại để phù hợp với phân loại mới về dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm, các hoạt động xử lý dữ liệu theo chuyên ngành và biện pháp bảo vệ tương ứng. Tổ chức cần thiết lập quy trình rõ ràng để thu thập và quản lý sự đồng ý của chủ thể dữ liệu, đảm bảo sự đồng ý phải được ghi nhận và có thể kiểm chứng, với thời hạn phản hồi cụ thể đối với các yêu cầu của chủ thể dữ liệu.

- **Nhân sự:** Ngoại trừ một số trường hợp đặc biệt, các tổ chức bắt buộc phải bổ nhiệm DPO, DPD đáp ứng đầy đủ tiêu chuẩn chuyên môn. Việc bổ nhiệm cần được thực hiện bằng văn bản, trong đó nêu rõ trách nhiệm pháp lý của DPO, DPD. Đồng thời, tổ chức cũng cần triển khai các khóa đào tạo và nâng cao nhận thức cho nhân viên tham gia xử lý dữ liệu cá nhân nhằm bảo đảm họ nắm vững các yêu cầu mới theo Luật BVDLCN và Dự thảo Nghị định.

- **Thủ tục hành chính:** Các yêu cầu nghiêm ngặt mới về DPIA và CTIA đòi hỏi hồ sơ, tài liệu đầy đủ và chi tiết. Tổ chức nên rà soát các hoạt động xử lý dữ liệu hiện tại và các luồng chuyển dữ liệu xuyên biên giới để xác định các hoạt động cần ưu tiên chú trọng. Đồng thời, cần xây dựng và triển khai khung DPIA và CTIA chặt chẽ, bao gồm sơ đồ luồng dữ liệu và kế hoạch bảo mật chi tiết, cùng với việc phân công rõ trách nhiệm cho nhân sự trong việc giám sát và ghi nhận các thay đổi.



Văn phòng Tp. Hồ Chí Minh

Robert King | Lãnh đạo Dịch vụ Thuế, EY Việt Nam, Lào, Campuchia
Công ty Cổ phần Tư vấn EY Việt Nam
robert.m.king@vn.ey.com

Thân Xuân Thịnh | Luật sư thành viên
Công ty Luật TNHH EY Việt Nam
thinh.xuan.than@vn.ey.com

Robert Tran | Phó Tổng Giám đốc
Công ty TNHH Dịch vụ An toàn thông tin EY Việt Nam
robert.tran@vn.ey.com

Trần Thị Cẩm Thạch | Luật sư Cấp cao
Công ty Luật TNHH EY Việt Nam
thach.cam.tran@vn.ey.com

Văn phòng Hà Nội

Nguyễn Hoàng Anh Linh | Luật sư Chủ nhiệm Cấp cao
Công ty Luật TNHH EY Việt Nam
linh.hoang.anh.nguyen@vn.ey.com

Nguyễn Hồng Lê | Luật sư
Công ty Luật TNHH EY Việt Nam
le.hong.nguyen@vn.ey.com

Khối Doanh nghiệp Nhật Bản (JBS)

Takahisa Onose | Lãnh đạo JBS, EY Việt Nam, Lào, Campuchia
Công ty TNHH Ernst & Young Việt Nam
takahisa.onose@vn.ey.com

Takaaki Nishikawa | Giám đốc
Công ty TNHH Ernst & Young Việt Nam
takaaki.nishikawa@vn.ey.com

Yuka Otomi | Phó Giám đốc
Công ty TNHH Ernst & Young Việt Nam
yuka.otomi@vn.ey.com

Khối Doanh nghiệp Hàn Quốc (KBS)

Phan Thanh Bình | Lãnh đạo KBS, EY Việt Nam, Lào, Campuchia
Công ty Cổ phần Tư vấn EY Việt Nam
binh.thanh.phan@vn.ey.com

Kyung Hoon Han | Giám đốc
Công ty TNHH Ernst & Young Việt Nam
kyung.hoon.han@vn.ey.com

Khối Doanh nghiệp nói tiếng Trung (CBS)

Lê Đức Trường | Lãnh đạo CBS, EY Việt Nam, Lào, Campuchia
Công ty TNHH Ernst & Young Việt Nam
truong.duc.le@vn.ey.com

Owen Tsao | Giám đốc
Công ty TNHH Ernst & Young Việt Nam
owen.tsao@vn.ey.com

Lương Kiết Trinh | Chủ nhiệm
Công ty TNHH Ernst & Young Việt Nam
trinh.kiet.luong@vn.ey.com

EY | Xây dựng một thế giới làm việc tốt đẹp hơn

EY đang xây dựng một thế giới làm việc tốt đẹp hơn bằng cách tạo ra giá trị mới cho khách hàng, con người, xã hội và hành tinh, đồng thời tạo dựng sự tín nhiệm trên các thị trường vốn.

Đội ngũ chuyên gia của EY, được hỗ trợ bởi dữ liệu, AI và công nghệ tiên tiến, giúp khách hàng tự tin kiến tạo tương lai và tìm ra câu trả lời cho các vấn đề cấp bách nhất của hôm nay và ngày mai.

Đội ngũ chuyên gia EY cung cấp đầy đủ các dịch vụ đảm bảo, tư vấn, thuế, chiến lược và giao dịch tài chính. Với hiểu biết sâu sắc về từng khu vực kinh tế, mạng lưới chuyên gia đa ngành được kết nối toàn cầu và các lãnh đạo đa năng trong hệ sinh thái, đội ngũ của EY có thể cung cấp dịch vụ tại hơn 150 quốc gia và các vùng lãnh thổ.

Toàn lực để tự tin kiến tạo tương lai.

APAC No. 16141001
ED None

ey.com/vi_vn