INDOCHINE COUNSEL
Business Law Practitioners

Bản tin Pháp luật

NGHỊ ĐỊNH SỐ 356/2025 - LÁ CHẮN BẢO VỆ MỚI CHO DỮ LIỆU CÁ NHÂN TẠI VIỆT NAM

Tháng 1 năm 2026

Ngày 31/12/2025, Chính phủ đã chính thức ban hành Nghị định số 356/2025/NĐ-CP quy định chi tiết một số điều và biện pháp thi hành Luật Bảo vệ dữ liệu cá nhân ("**Nghị định 356**"). Nghị định 356 có hiệu lực từ ngày 01/01/2026 và thay thế Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân ("**Nghị định 13**").

Theo đó, bên cạnh Luật Bảo vệ dữ liệu cá nhân ("**Luật BVDLCN**"), Nghị định 356 được kỳ vọng sẽ trở thành lá chắn bảo vệ mới cho dữ liệu cá nhân tại Việt Nam, góp phần triển khai hiệu quả các quy định của Luật BVDLCN. Đồng thời, cả Luật BVDLCN và Nghị định 356 cùng hướng tới bảo đảm quyền con người và quyền riêng tư, ngăn chặn các hành vi xâm phạm dữ liệu cá nhân, nâng cao nhận thức, hình thành văn hóa bảo vệ dữ liệu cá nhân, cũng như xác định rõ trách nhiệm của các cơ quan, tổ chức, cá nhân trong hoạt động xử lý dữ liệu cá nhân.

Các Nội Dung Chính

- **Danh Mục Dữ Liệu Cá Nhân:** Nghị định 356 đã có những điều chỉnh đáng kể đối với danh mục dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm.

- **Sự Đồng Ý và Trách Nhiệm Xử Lý Yêu Cầu của Chủ Thể Dữ Liệu:** Nghị định 356 nghiêm cấm cơ chế *"mặc định đồng ý"* hoặc gây nhầm lẫn cho chủ thể dữ liệu. Đồng thời, các mốc thời gian phản hồi và xử lý yêu cầu của chủ thể dữ liệu đã cụ thể và chi tiết hơn so với Nghị định 13.

- **Hồ Sơ Đánh Giá Tác Động Xử Lý Dữ Liệu Cá Nhân và Chuyển Dữ Liệu Cá Nhân Xuyên Biên Giới:** Các quy định về Hồ Sơ Đánh Giá Tác Động Xử Lý Dữ Liệu Cá Nhân ("**Hồ Sơ ĐGXLDLCN**") và Hồ Sơ Đánh Giá Tác Động Chuyển Dữ Liệu Cá Nhân Xuyên Biên Giới ("**Hồ Sơ ĐGCDLXBG**") tiếp tục được ghi nhận trong Nghị định 356, với những điều chỉnh và thay đổi xuất phát từ thực tiễn khi triển khai Nghị định 13.

- **Quy Định về Chuyển Giao Dữ Liệu Cá Nhân**: Nghị định 356 làm rõ các trường hợp phải xác lập thỏa thuận

chuyển giao dữ liệu, nội dung tối thiểu của thỏa thuận, cũng như yêu cầu bảo mật bổ sung khi chuyển giao dữ liệu cá nhân nhạy cảm.

- **Yêu Cầu về Nhân Sự Bảo Vệ Dữ Liệu Cá Nhân**: Nghị định 356 quy định cụ thể về trình độ, kinh nghiệm, và yêu cầu đào tạo đối với nhân sự bảo vệ dữ liệu cá nhân, qua đó nhấn mạnh vai trò của yếu tố con người trong hệ thống tuân thủ bảo vệ dữ liệu.

- **Bảo Vệ Dữ Liệu Cá Nhân trong Những Lĩnh Vực Đặc Thù:** Các lĩnh vực như tài chính - ngân hàng, xử lý dữ liệu lớn, trí tuệ nhân tạo, vũ trụ ảo, công nghệ chuỗi khối, và điện toán đám mây được điều chỉnh bằng các yêu cầu kỹ thuật và nguyên tắc bảo vệ dữ liệu riêng biệt, phản ánh đúng đặc thù công nghệ và rủi ro phát sinh.

Bài viết này điểm qua những nội dung đáng chú ý nhất của Nghị định 356, phân tích các điểm đổi mới quan trọng, đồng thời chỉ ra những vấn đề mà cơ quan, tổ chức, cá nhân cần lưu ý, quan tâm trong quá trình bảo vệ dữ liệu cá nhân.

Danh Mục Dữ Liệu Cá Nhân

Đối với **Dữ Liệu Cá Nhân Cơ Bản**, trong bối cảnh Việt Nam đang đẩy mạnh quá trình chuyển đổi số toàn diện và đồng bộ trên nhiều lĩnh vực, hướng tới mục tiêu liên thông dữ liệu quốc gia, đồng thời bảo đảm an ninh, an toàn dữ liệu trên không gian mạng, Nghị định 356 đã có những thay đổi đáng chú ý đối với danh mục dữ liệu cá nhân cơ bản so với Nghị định 13, cụ thể như sau:

- **Số chứng minh nhân dân, số mã số thuế cá nhân, số bảo hiểm xã hội, và số thẻ bảo hiểm y tế** được loại bỏ ra khỏi danh mục dữ liệu cá nhân cơ bản, do các thông tin này đều đã được thay thế bằng số định danh cá nhân;

- **Thông tin về mối quan hệ gia đình** mở rộng thêm cho cả 02 đối tượng mới là “vợ” và “chồng”, Nghị định 13 trước đây chỉ quy định thông tin về mối quan hệ gia đình gồm “cha, mẹ” và “con cái”; và

- **Dữ liệu cá nhân phản ánh hoạt động, lịch sử hoạt động trên không gian mạng** cũng không còn được ghi nhận là dữ liệu cá nhân cơ bản trong Nghị định 356 nữa, mà chuyển thành dữ liệu cá nhân nhạy cảm.

Đối với **Dữ Liệu Cá Nhân Nhạy Cảm**, Nghị định 356 cũng đã mở rộng và cụ thể hóa hơn đối với danh mục dữ liệu cá nhân nhạy cảm, nhằm bao quát toàn diện những loại dữ liệu cần đặc biệt lưu ý trong quá trình xử lý, cũng như nâng cao nhận thức của chủ thể dữ liệu đối với dữ liệu cá nhân nhạy cảm của mình.

- **Quan điểm về tín ngưỡng** được bổ sung vào danh mục dữ liệu cá nhân nhạy cảm, bên cạnh quan điểm về chính trị và tôn giáo. Việc Nghị định 13 trước đây chưa ghi nhận quan điểm về tín ngưỡng là dữ liệu cá nhân nhạy cảm có thể được xem là một thiếu sót đáng tiếc, trong bối cảnh tôn giáo và tín ngưỡng đã được quy định riêng biệt và cụ thể tại Luật Tín ngưỡng, Tôn giáo, đặc biệt khi Việt Nam là quốc gia có sự đa dạng về tôn giáo và tín ngưỡng. Do đó, việc điều chỉnh này góp phần bảo đảm tốt hơn quyền tự do tín ngưỡng, tôn giáo của các chủ thể dữ liệu;

- **Dữ liệu vi phạm pháp luật của cá nhân** sẽ được coi là dữ liệu cá nhân nhạy cảm, trong khi trước đây chỉ dữ liệu vi phạm đến mức bị xử lý hình sự (như là tội phạm, hành vi phạm tội) mới được coi là dữ liệu cá nhân nhạy cảm;

- **Dữ liệu trong lĩnh vực ngân hàng** như tên đăng nhập, mật khẩu truy cập của tài khoản ngân hàng; thông tin thẻ ngân hàng, dữ liệu về lịch sử giao dịch của tài khoản ngân hàng; thông tin về hoạt động, lịch sử giao dịch trong lĩnh vực chứng khoán, bảo hiểm tại các công ty chứng khoán, công ty bảo hiểm của khách hàng cũng được coi là dữ liệu cá nhân nhạy cảm. Có thể thấy rằng dữ liệu cá nhân nhạy cảm trong lĩnh vực ngân hàng đã được mở rộng, không chỉ gói gọn trong các thông tin giao dịch tại các ngân hàng như trước đây; và

- **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** được bổ sung vào danh mục dữ liệu cá nhân nhạy cảm. Việc thay đổi này của Nghị định 356 là hết sức cần thiết khi mà hành vi xâm phạm dữ liệu cá nhân diễn ra ngày càng phổ biến trên không gian mạng.

Một điểm cần hết sức lưu ý trong quy định về danh mục dữ liệu cá nhân, cụ thể là chỉ có số định danh cá nhân được ghi nhận là dữ liệu cá nhân cơ bản, còn thông tin tên đăng nhập và mật khẩu để truy cập tài khoản định danh điện tử của cá nhân, cũng như hình ảnh thẻ căn cước, thẻ căn cước công dân, chứng minh nhân dân sẽ là dữ liệu cá nhân nhạy cảm.

Sự phân định cụ thể này xuất phát từ thực tế rằng các thông tin và hình ảnh nêu trên, nếu bị xâm phạm, có thể gây ảnh hưởng trực tiếp và nghiêm trọng đến quyền và lợi ích hợp pháp của cơ quan, tổ chức và cá nhân. Chẳng hạn, hành vi truy cập trái phép vào tài khoản định danh điện tử, việc sử dụng hình ảnh chứng minh nhân dân / căn cước công dân để vay tiền qua các ứng dụng, đăng ký thuê bao trả sau, đăng ký mã số thuế không có thật, hoặc thực hiện các hành vi trái pháp luật khác. Bên cạnh đó, mã QR trên thẻ căn cước công dân chứa nhiều thông tin cá nhân, có thể bị tội phạm công nghệ cao lợi dụng nhằm trục lợi.

Chính vì vậy, Nghị định 356 cũng nhấn mạnh rằng các cơ quan, tổ chức phải thiết lập quy định phân quyền giới hạn truy cập, quy trình xử lý, và các biện pháp bảo mật trong quá trình xử lý dữ liệu cá nhân nhạy cảm.

Sự Đồng Ý và Trách Nhiệm Xử Lý Yêu Cầu của Chủ Thể Dữ Liệu

Sự đồng ý của chủ thể dữ liệu luôn là yêu cầu then chốt trong hoạt động xử lý dữ liệu cá nhân. Tuy nhiên, theo Luật BVDLCN, vẫn tồn tại một số trường hợp ngoại lệ mà cơ quan, tổ chức được phép xử lý dữ liệu cá nhân mà không cần sự đồng ý của chủ thể dữ liệu. Một trường hợp đáng chú ý là việc xử lý dữ liệu cá nhân nhằm thực hiện thỏa thuận của chủ thể dữ liệu với cơ quan, tổ chức, cá nhân có liên quan theo quy định của pháp luật, chẳng hạn như nhằm mục đích thực hiện hợp đồng lao động giữa người sử dụng lao động và người lao động. Mặc dù Nghị định 356 hiện chưa có hướng dẫn chi tiết hơn đối với quy định này của Luật BVDLCN, đây vẫn là một nội dung mà các cơ quan, tổ chức có thể cân nhắc và xem xét áp dụng trong thực tiễn hoạt động của mình.

Đáng chú ý, Nghị định 356 đã quy định rõ hơn trách nhiệm của Bên kiểm soát dữ liệu và Bên kiểm soát và xử lý dữ liệu cá nhân liên quan đến việc thu thập, quản lý và chứng minh sự đồng ý của chủ thể dữ liệu. Theo đó, các chủ thể này có

trách nhiệm phải lưu trữ sự đồng ý của chủ thể dữ liệu và không được phép thiết lập phương thức *"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.

Bên cạnh đó, nhằm bảo đảm quyền và lợi ích hợp pháp của chủ thể dữ liệu, Nghị định 356 đã quy định cụ thể và chi tiết hơn các mốc thời gian, thời hạn liên quan đến trách nhiệm tiếp nhận và xử lý yêu cầu của chủ thể dữ liệu, thay cho quy định còn mang tính khái quát về thời hạn 72 giờ tại Nghị định 13.

Theo đó, Bên kiểm soát dữ liệu và Bên kiểm soát và xử lý dữ liệu cá nhân có trách nhiệm xây dựng quy trình, thủ tục và biểu mẫu rõ ràng để thực hiện các yêu cầu của chủ thể dữ liệu, đồng thời tuân thủ các thời hạn phản hồi và thời hạn xử lý tương ứng đối với từng loại yêu cầu, cụ thể như sau:

TT	Yêu cầu của chủ thể dữ liệu	Thời hạn phản hồi yêu cầu	Thời hạn xử lý, thực hiện yêu cầu
1	Yêu cầu rút lại sự đồng ý / hạn chế xử lý / phản đối xử lý dữ liệu	02 ngày làm việc	15 ngày (nếu liên quan Bên xử lý / Bên thứ ba là 20 ngày)
2	Yêu cầu xem / chỉnh sửa / cung cấp dữ liệu cá nhân		10 ngày (nếu liên quan Bên xử lý / Bên thứ ba là 15 ngày)
3	Yêu cầu xóa dữ liệu cá nhân		20 ngày (nếu liên quan Bên xử lý / Bên thứ ba là 30 ngày)
4	Yêu cầu thực hiện các biện pháp, giải pháp bảo vệ dữ liệu cá nhân		15 ngày

Mặc dù đã có quy định cụ thể về thời hạn xử lý, chủ thể dữ liệu cũng cần hết sức lưu ý, để áp dụng được các thời hạn nêu trên, chủ thể dữ liệu phải thực hiện đúng các thủ tục theo như thỏa thuận và quy định của Bên kiểm soát dữ liệu, hay Bên kiểm soát và xử lý dữ liệu. Trường hợp chủ thể dữ liệu không thực hiện đúng các thủ tục này, việc phản hồi và xử lý có thể sẽ kéo dài và ảnh hưởng đến quyền và lợi ích hợp pháp của chủ thể dữ liệu.

Ngoài ra, Nghị định 356 cũng có cơ chế gia hạn thời hạn xử lý yêu cầu là 01 lần tùy theo tính chất, mức độ phức tạp của yêu cầu, kèm nghĩa vụ giải trình tính cần thiết/hợp lý của việc gia hạn này.

Hồ Sơ Đánh Giá Tác Động Xử Lý Dữ Liệu Cá Nhân và Chuyển Dữ Liệu Cá Nhân Xuyên Biên Giới

Một trong những nội dung được các cơ quan, tổ chức đặc biệt quan tâm khi Nghị định 356 có hiệu lực là các quy định liên quan đến nghĩa vụ và trách nhiệm lập Hồ Sơ ĐGXLDLCN và Hồ Sơ ĐGCDLXBG.

Theo Luật BVDLCN, trường hợp hồ sơ của cơ quan, tổ chức đã được Cơ quan chuyên trách bảo vệ dữ liệu cá nhân tiếp nhận theo quy định tại Nghị định 13 trước ngày 01/01/2026 thì các hồ sơ này tiếp tục có giá trị sử dụng và không phải lập lại hồ sơ mới. Tuy nhiên, trong trường hợp cơ quan, tổ chức có cập nhật, điều chỉnh nội dung các hồ sơ đã nộp, hoặc

chưa thực hiện nghĩa vụ lập hồ sơ theo Nghị định 13 trước đây, thì kể từ ngày 01/01/2026, việc lập hồ sơ phải được thực hiện theo trình tự, thủ tục và biểu mẫu quy định tại Luật BVDLCN và Nghị định 356.

Về tổng thể, Nghị định 356 đã có những thay đổi căn bản cả về hình thức và nội dung của các loại hồ sơ nêu trên, theo hướng tích hợp, điều chỉnh và bổ sung các yêu cầu mang tính kỹ thuật. Đồng thời, Nghị định 356 không còn quy định cụ thể Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (A05) là cơ quan đầu mối tiếp nhận và xử lý các vấn đề liên quan đến bảo vệ dữ liệu cá nhân, mà chỉ ghi nhận chung là Cơ quan chuyên trách bảo vệ dữ liệu cá nhân.

Bên cạnh đó, nếu như Nghị định 13 trước đây chưa quy định rõ trách nhiệm của Cơ quan chuyên trách bảo vệ dữ liệu cá nhân trong việc đánh giá và phản hồi kết quả đối với các hồ sơ đánh giá tác động, thì Nghị định 356 đã quy định cụ thể nội dung này. Theo đó, Cơ quan chuyên trách bảo vệ dữ liệu cá nhân có trách nhiệm đánh giá và thông báo kết quả hồ sơ đạt yêu cầu hoặc không đạt yêu cầu trong thời hạn 15 ngày kể từ ngày tiếp nhận hồ sơ hợp lệ.

Một điểm đáng chú ý khác của Nghị định 356 mà các cơ quan, tổ chức cần lưu ý nhằm áp dụng hiệu quả và tránh phát sinh các chi phí tuân thủ không cần thiết là việc Nghị định 356 này đã quy định cụ thể các trường hợp không phải lập Hồ Sơ ĐGCDLXBG. Trong đó, có thể kể đến một số trường hợp tiêu biểu như:

- Chuyển dữ liệu cá nhân xuyên biên giới phục vụ quản lý nhân sự xuyên biên giới theo quy định nội bộ, quy chế lao động và thỏa ước lao động tập thể phù hợp với pháp luật; hoặc
- Cung cấp dữ liệu cá nhân xuyên biên giới nhằm ký kết hợp đồng hoặc thực hiện các thủ tục liên quan đến vận chuyển xuyên biên giới, hậu cần, chuyển tiền, thanh toán, đặt phòng khách sạn, xin thị thực hoặc xin học bổng.

Đối với các trường hợp này, cơ quan, tổ chức không phải thực hiện Hồ Sơ ĐGCDLXBG theo quy định của Nghị định 356.

Quy Định về Chuyển Giao Dữ Liệu Cá Nhân

Luật BVDLCN đã quy định tổng cộng 07 trường hợp chuyển giao dữ liệu cá nhân và giao Chính phủ quy định chi tiết trách nhiệm, nghĩa vụ tương ứng. Trên cơ sở đó, Nghị định 356 quy định rằng, đối với 03 trường hợp chuyển giao dữ liệu cá nhân dưới đây, tổ chức, cá nhân phải xác lập thỏa thuận chuyển giao dữ liệu cá nhân, trong đó tối thiểu phải bao gồm các nội dung sau: mục đích; loại dữ liệu; thời hạn; cơ sở pháp lý; trách nhiệm bảo vệ; trách nhiệm thực hiện quyền chủ thể; cơ chế phối hợp khi xảy ra vi phạm.

- Chuyển giao dữ liệu cá nhân khi có sự đồng ý của chủ thể dữ liệu cá nhân;
- Chuyển giao dữ liệu cá nhân để tiếp tục xử lý dữ liệu cá nhân trong trường hợp chia, tách, sáp nhập cơ quan, tổ chức, đơn vị hành chính, v.v.; và
- Bên kiểm soát dữ liệu cá nhân, Bên kiểm soát và xử lý dữ liệu cá nhân chuyển giao dữ liệu cá nhân cho Bên xử lý dữ liệu cá nhân, Bên thứ ba để xử lý dữ liệu cá nhân theo quy định.

Trường hợp dữ liệu được chuyển giao là dữ liệu cá nhân nhạy cảm, bên cạnh việc xác lập thỏa thuận, phải có biện pháp bảo mật vật lý đối với thiết bị lưu trữ và truyền tải, biện pháp mã hóa, ẩn danh dữ liệu cá nhân và các biện pháp bảo mật khác.

Đối với trường hợp chia sẻ dữ liệu cá nhân nội bộ, giữa các bộ phận trong cùng một cơ quan, tổ chức để xử lý dữ liệu cá nhân, Nghị định 356 không yêu cầu cơ quan, tổ chức phải xác lập thỏa thuận như trong 03 trường hợp nêu trên, nhưng thay vào đó, các cơ quan, tổ chức phải xây dựng quy trình kiểm soát việc chia sẻ, sử dụng dữ liệu cá nhân đúng quy định.

Trường hợp giao dịch trên sàn dữ liệu, dữ liệu cá nhân phải được khử nhận dạng trước khi giao dịch. Đối với quy định này, chúng ta vẫn phải chờ đợi thêm những hướng dẫn, quy định chi tiết hơn về khử nhận dạng dữ liệu cá nhân.

Cần lưu ý rằng, trường hợp cơ quan, tổ chức, cá nhân thực hiện cung cấp dữ liệu cá nhân dựa trên từng yêu cầu cụ thể của chủ thể dữ liệu thì không được coi là chuyển giao dữ liệu và không phải thực hiện theo các quy định nêu trên. Quy định này có thể xuất phát từ thực tế là chủ thể dữ liệu mong muốn thực hiện các quyền của chủ thế dữ liệu đối với chính dữ liệu cá nhân của mình, theo đó chủ thể dữ liệu muốn kiểm tra, giám sát quá trình xử lý dữ liệu cá nhân của mình đang diễn ra như thế nào, cũng như những dữ liệu cá nhân nào của mình đang được thu thập và xử lý.

Yêu Cầu về Nhân Sự Bảo Vệ Dữ Liệu Cá Nhân

Nghị định 356 quy định nhân sự bảo vệ dữ liệu cá nhân được cơ quan, tổ chức chỉ định phải đáp ứng đủ các điều kiện năng lực như sau:

- Có trình độ cao đẳng trở lên;
- Có ít nhất 02 năm kinh nghiệm công tác (kể từ thời điểm tốt nghiệp) liên quan đến một trong các lĩnh vực về pháp chế, công nghệ thông tin, an ninh mạng, an ninh dữ liệu, quản trị rủi ro, kiểm soát tuân thủ, quản lý nhân sự, tổ chức cán bộ; và
- Đã được đào tạo, bồi dưỡng kiến thức pháp luật và kỹ năng chuyên môn về bảo vệ dữ liệu cá nhân.

Quy định này của Nghị định 356 trao cho các cơ quan, tổ chức quyền chủ động trong việc tuyển dụng và chỉ định nhân sự bảo vệ dữ liệu cá nhân, đồng thời giao trách nhiệm đào tạo, bồi dưỡng kiến thức và kỹ năng về bảo vệ dữ liệu cá nhân cho các chủ thể này. Cách tiếp cận này tạo ra sự linh hoạt và thuận tiện hơn cho cơ quan, tổ chức trong quá trình tuân thủ. Tuy nhiên, việc chưa thiết lập cơ chế kiểm tra, đánh giá và hậu kiểm đối với các nhân sự, cơ quan và tổ chức nêu trên cũng có thể phát sinh những rủi ro nhất định đối với quyền và lợi ích của chủ thể dữ liệu trong thực tiễn.

Bảo Vệ Dữ Liệu Cá Nhân trong Những Lĩnh Vực Đặc Thù

Bên cạnh các quy định chung về bảo vệ dữ liệu cá nhân, Nghị định 356 dành nhiều quy định để điều chỉnh hoạt động bảo vệ dữ liệu cá nhân trong một số lĩnh vực đặc thù, theo đó yêu cầu các bên liên quan phải áp dụng các biện pháp thận

trọng và nghiêm ngặt hơn.

- **Trong hoạt động tài chính, ngân hàng, hoạt động thông tin tín dụng**: Nghị định 356 yêu cầu áp dụng tiêu chuẩn, quy chuẩn kỹ thuật bảo vệ dữ liệu cá nhân; quy chuẩn kỹ thuật khử nhận dạng dữ liệu cá nhân, ẩn danh dữ liệu cá nhân được ban hành và áp dụng tại Việt Nam.

- **Trong xử lý dữ liệu lớn**: Các cơ quan, tổ chức, cá nhân được yêu cầu phải sử dụng phương thức xác thực mạnh, yêu cầu tối thiểu xác thực đa yếu tố (mật khẩu, mã PIN kết hợp với mật khẩu dùng một lần, thiết bị ký số hoặc yếu tố sinh trắc học), phân quyền truy cập để đảm bảo chỉ những người có quyền mới có thể truy cập dữ liệu cá nhân.

- **Trong hệ thống trí tuệ nhân tạo, vũ trụ ảo**: Nghị định 356 yêu cầu chủ thể dữ liệu cá nhân phải có quyền chỉnh sửa, ẩn danh, xóa hồ sơ nhận dạng, kể cả khi nền tảng lưu trữ lịch sử hành vi.

- **Trong công nghệ chuỗi khối**: Nghị định 356 yêu cầu không lưu trữ trực tiếp dữ liệu cá nhân trên chuỗi khối, chỉ lưu trữ khi dữ liệu cá nhân đã được khử nhận dạng hoặc lưu trữ giá trị băm của dữ liệu cá nhân. Pháp luật về bảo vệ dữ liệu cá nhân hiện nay ghi nhận 02 thuật ngữ đáng chú ý là: **"khử nhận dạng"** và **"mã hóa"**. Điểm khác biệt cơ bản là dữ liệu cá nhân sau khi được mã hóa vẫn được coi là dữ liệu cá nhân và tiếp tục chịu sự điều chỉnh của các quy định pháp luật liên quan, trong khi dữ liệu cá nhân sau khi được khử nhận dạng sẽ không còn được xem là dữ liệu cá nhân.

- **Trong điện toán đám mây**: Dữ liệu cá nhân phải được mã hóa ở trạng thái nghỉ và truyền, kèm theo phân quyền truy cập nghiêm ngặt. Khác với công nghệ chuỗi khối ở trên, dữ liệu cá nhân trong điện toán đám mây phải được mã hóa, tức là được chuyển đổi sang dạng không thể nhận biết nếu không có được giải mã; và dữ liệu cá nhân sau khi được mã hóa vẫn được coi là dữ liệu cá nhân.

Sự khác biệt trong các yêu cầu áp dụng đối với dữ liệu cá nhân trong điện toán đám mây và công nghệ chuỗi khối có thể xuất phát từ đặc thù thiết kế của từng công nghệ. Cụ thể, điện toán đám mây được thiết kế để quản lý dữ liệu cá nhân trong môi trường có kiểm soát, do đó pháp luật tập trung vào các yêu cầu về bảo mật dữ liệu. Trong khi đó, công nghệ chuỗi khối được thiết kế để lưu trữ dữ liệu theo cơ chế bất biến và phi tập trung, vì vậy đòi hỏi phải loại bỏ yếu tố nhận dạng, xác định cá nhân ngay từ giai đoạn đầu.

Kết Luận

Dữ liệu cá nhân là vấn đề liên quan chặt chẽ tới quyền con người, quyền công dân, an toàn, an ninh mạng, an ninh thông tin, an ninh dữ liệu, công nghệ thông tin và cách mạng công nghiệp lần thứ tư, chính phủ điện tử, chính phủ số, và kinh tế số. Nghị định 356 được kỳ vọng sẽ tiếp tục hoàn thiện hành lang pháp lý cho công tác bảo vệ dữ liệu cá nhân.

Tuy nhiên, Nghị định 356 hiện mới hướng dẫn một số điều của Luật BVDLCN. Do đó, để nâng cao hiệu quả triển khai và thi hành, cũng như phát huy đầy đủ giá trị và ý nghĩa thực tiễn của Luật BVDLCN, trong thời gian tới, chúng ta có cơ sở để kỳ vọng và cùng chờ đợi thêm các văn bản hướng dẫn khác trong lĩnh vực bảo vệ dữ liệu cá nhân này.

Giới thiệu về Indochine Counsel

Được thành lập vào tháng 10 năm 2006, Indochine Counsel là một hãng luật thương mại hàng đầu tại Việt Nam. Với vị thế thuận lợi, chúng tôi hỗ trợ các nhà đầu tư quốc tế và các doanh nghiệp nước ngoài trong việc chinh phục môi trường pháp lý tại một trong những quốc gia năng động và thú vị nhất châu Á. Chúng tôi cũng tự hào cung cấp các dịch vụ pháp lý cho các nhà đầu tư trong nước đang tìm kiếm cơ hội vươn ra thế giới. Với đội ngũ hơn 45 luật sư và nhân viên làm việc tại hai văn phòng tại Thành phố Hồ Chí Minh và Hà Nội, Indochine Counsel cung cấp dịch vụ pháp lý chuyên nghiệp trong nhiều lĩnh vực khác nhau, đồng hành cùng khách hàng trong suốt hành trình phát triển doanh nghiệp. Chúng tôi là đối tác đáng tin cậy tại Việt Nam, mang đến giải pháp pháp lý toàn diện cho cả thị trường trong nước và quốc tế.

Indochine Counsel cung cấp các dịch vụ pháp lý toàn diện trong nhiều lĩnh vực khác nhau bao gồm:

- Chống Độc quyền & Cạnh tranh
- Tài chính & Ngân hàng
- Doanh nghiệp & Thương mại
- Năng lượng, Tài nguyên & Cơ sở hạ tầng
- Sở hữu Trí tuệ
- Đầu tư Nước ngoài
- Lao động & Việc làm
- Tranh tụng & Giải quyết Tranh chấp
- Mua bán & Sáp nhập
- Bất Động sản & Xây dựng
- Chứng khoán & Thị trường Vốn
- Công nghệ, Truyền thông & Viễn thông

Liên hệ

Để biết thêm thông tin hoặc cần hỗ trợ, vui lòng liên hệ với chúng tôi:

Đặng Thế Đức
Luật sư Điều hành
E duc.dang@indochinecounsel.com

Thái Gia Hân
Luật sư Cao cấp | Trưởng Bộ phận Sở hữu Trí tuệ, Công nghệ & Truyền thông
E han.thai@indochinecounsel.com

Nguyễn Lê Toàn Phước
Trợ lý Luật sư
E phuoc.nguyen@indochinecounsel.com

Văn phòng Tp. Hồ Chí Minh

Phòng 305, Tầng 3, Tòa nhà Centec
72-74 Nguyễn Thị Minh Khai, Phường Xuân Hòa
Thành phố Hồ Chí Minh, Việt Nam

T +84 28 3823 9640
F +84 28 3823 9641
E info@indochinecounsel.com

Văn phòng Hà Nội

Phòng 705, Tầng 7, Tòa nhà CMC
Phố Duy Tân, Phường Cầu Giấy
Hà Nội, Việt Nam

T +84 24 3795 5261
F +84 24 3795 5262
E hanoi@indochinecounsel.com

Liên hệ với chúng tôi tại
Indochinecounsel.com

Linkedin Facebook YouTube