LNT & PARTNERS

TIÊU ĐIỂM LUẬT

Cập nhật những thay đổi pháp lý quan trọng hàng tháng có ảnh hưởng đến hoạt động đầu tư và kinh doanh tại Việt Nam. Truy cập Trung tâm Tư liệu của chúng tôi để theo dõi những cập nhật pháp lý mới nhất và tin tức từ LNT & Partners.

Khung Pháp Lý Mới Về An Ninh Mạng Và Bảo Vệ Dữ Liệu Tại Việt Nam – Những Lưu Ý Quan Trọng Cho Các Tập Đoàn Đa Quốc Gia

Nguyễn Diệu Quỳnh – *Cộng sự Cấp cao*

Võ Kim Nguyên – *Cộng sự Tập sự*

1. Khung pháp lý về An ninh mạng và Bảo vệ Dữ liệu tại Việt Nam

Năm 2025, hệ thống pháp luật Việt Nam ghi dấu một bước tiến nổi bật trong việc củng cố khung pháp lý về an ninh mạng và bảo vệ dữ liệu cá nhân. Sự ra đời của Luật Dữ liệu 2024, Luật Bảo vệ Dữ liệu cá nhân 2025 ("**Luật BVDLCN 2025**"), và Luật An ninh mạng 2025 cùng với sự phát triển không ngừng của các văn bản hướng dẫn thi hành cho thấy Việt Nam đang chuyển mình sang một hệ thống pháp luật ngày một toàn diện và thống nhất hơn. Bước phát triển này cũng phản ánh xu hướng toàn cầu hóa rộng lớn hơn của Việt Nam trong việc tăng cường quản trị dữ liệu và siết chặt giám sát pháp lý.

Trong giai đoạn Luật An ninh mạng 2025 và các nghị định hướng dẫn thi hành dự kiến có hiệu lực, việc đón đầu các thay đổi pháp lý sẽ giúp doanh nghiệp thích ứng tốt hơn với bối cảnh pháp lý đang chuyển dịch tại Việt Nam, đồng thời giảm thiểu các rủi ro tiềm tàng về mặt pháp lý và vận hành. Trong bối cảnh đó, các chủ thể phải đáp ứng một khung tuân thủ đa tầng, đòi hỏi sự đánh giá thận trọng đối với các nghĩa vụ chồng lấn và các ngưỡng áp dụng liên quan.

2. Phạm vi áp dụng

Phạm vi áp dụng của khung pháp lý về dữ liệu và an ninh mạng tại Việt Nam được quy định theo hướng mở rộng ra ngoài lãnh thổ. Nhìn chung, các quy định này áp dụng đối với (i) cơ quan, tổ chức, cá nhân Việt Nam; (ii) cơ quan, tổ chức, cá nhân nước ngoài tại Việt Nam; và (iii) cơ quan, tổ chức, cá nhân nước ngoài trực tiếp tham gia hoặc có liên quan đến hoạt động bảo vệ an ninh mạng, kinh doanh sản phẩm, dịch vụ an ninh mạng; hoạt động xử lý dữ liệu cá nhân; hoạt động dữ liệu số tại Việt Nam.[1]

Theo đó, cả các chủ thể trong nước và nước ngoài, bao gồm các tập đoàn đa quốc gia, đều có thể thuộc phạm vi điều chỉnh của pháp luật về an ninh mạng và bảo vệ dữ liệu ngay cả khi không

[1] Điều 1.2 Luật An ninh mạng 2025, Điều 1.2 Luật BVDLCN 2025, Điều 2 Luật Dữ liệu 2024.

trực tiếp vận hành nền tảng số hoặc cung cấp dịch vụ mạng. Cách tiếp cận rộng và thống nhất này cho thấy rủi ro pháp lý có thể phát sinh không chỉ từ sự hiện diện thương mại tại Việt Nam mà còn từ các hoạt động xuyên biên giới, đặc biệt trong trường hợp tổ chức xử lý dữ liệu hoặc vận hành hệ thống thông tin liên quan đến người dùng hay chủ thể dữ liệu tại Việt Nam.

3. Các Nghĩa vụ Tuân thủ Chính về An ninh mạng và Bảo vệ Dữ liệu

Lưu trữ dữ liệu tại Việt Nam và Thành lập hiện diện thương mại tại Việt Nam

Lưu trữ dữ liệu tại Việt Nam là nghĩa vụ yêu cầu các doanh nghiệp trong nước và ngoài nước cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng tại Việt Nam có hoạt động thu thập, khai thác, phân tích, xử lý dữ liệu về thông tin cá nhân, dữ liệu về mối quan hệ của người sử dụng dịch vụ, dữ liệu do người sử dụng dịch vụ tại Việt Nam tạo ra phải lưu trữ các dữ liệu này tại Việt Nam.[2]

Các loại dữ liệu cụ thể phải được lưu trữ tại Việt Nam hiện được điều chỉnh bởi Nghị định 53/2022/NĐ-CP và có hiệu lực đến hết ngày 30 tháng 6 năm 2026. Mặc dù chưa được chính thức thông qua, Dự thảo Nghị định hướng dẫn thi hành Luật An ninh mạng 2025 hiện đang đề xuất xác định các loại dữ liệu này như sau:[3]

(i) Dữ liệu về thông tin cá nhân của người sử dụng dịch vụ tại Việt Nam;

(ii) Dữ liệu do người sử dụng dịch vụ tại Việt Nam tạo ra: Tên tài khoản sử dụng dịch vụ, thời gian sử dụng dịch vụ, thông tin thẻ tín dụng, địa chỉ thư điện tử, địa chỉ mạng (IP) đăng nhập, đăng xuất gần nhất, số điện thoại đăng ký được gắn với tài khoản hoặc dữ liệu;

(iii) Dữ liệu về mối quan hệ của người sử dụng dịch vụ tại Việt Nam: bạn bè, nhóm mà người sử dụng kết nối hoặc tương tác.

Ngoài ra, doanh nghiệp nước ngoài có hoạt động kinh doanh trong một số lĩnh vực nhất định, như dịch vụ viễn thông, lưu trữ, chia sẻ dữ liệu trên không gian mạng, thương mại điện tử, trò chơi điện tử trên mạng, ứng dụng trực tuyến, v.v. có thể thuộc trường hợp phải đặt chi nhánh hoặc văn phòng đại diện tại Việt Nam. Tuy nhiên, yêu cầu này không được áp dụng trong mọi trường hợp mà chỉ phát sinh khi doanh nghiệp không tuân thủ các nghĩa vụ về an ninh mạng sau khi đã nhận được yêu cầu chính thức từ cơ quan có thẩm quyền.[4] Các yêu cầu này có thể tạo ra những tác động đáng kể về mặt vận hành đối với các tập đoàn đa quốc gia, đặc biệt trong trường hợp hạ tầng dữ liệu toàn cầu của họ phụ thuộc vào hệ thống lưu trữ tập trung hoặc các nền tảng điện toán đám mây đặt ngoài lãnh thổ Việt Nam.

Tuân thủ quy định về chuyển dữ liệu xuyên biên giới

Các nghĩa vụ tuân thủ liên quan đến chuyển dữ liệu xuyên biên giới được điều chỉnh đồng thời bởi Luật BVDLCN 2025 và Luật Dữ liệu 2024. Trong khi Luật BVDLCN điều chỉnh đối với dữ liệu cá nhân, thì Luật Dữ liệu 2024 có phạm vi áp dụng rộng hơn đối với toàn bộ dữ liệu số, bao gồm dữ

[2] Điều 25.3 Luật An ninh mạng 2025
[3] Điều 28.1 và 28.2 Dự thảo Nghị định hướng dẫn chi tiết Luật An ninh mạng 2025, Dự thảo 3
[4] Điều 25.3 Luật An ninh mạng 2025, Điều 28 Dự thảo Nghị định hướng dẫn chi tiết Luật An ninh mạng 2025, Dự thảo 3

liệu dùng chung, dữ liệu doanh nghiệp, và đặc biệt là các loại dữ liệu được phân loại là "dữ liệu quan trọng" và "dữ liệu cốt lõi".[5]

Theo Luật BVDLCN 2025, doanh nghiệp phải lập và gửi hồ sơ đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới cho cơ quan có thẩm quyền trong vòng 60 ngày kể từ ngày đầu tiên chuyển dữ liệu xuyên biên giới.[6] Đáng chú ý, Luật BVDLCN 2025 cũng quy định một số trường hợp được miễn trừ áp dụng, bao gồm việc chuyển dữ liệu của người lao động được lưu trữ trên hệ thống điện toán đám mây và trường hợp chủ thể dữ liệu cá nhân tự chuyển dữ liệu cá nhân của mình xuyên biên giới. Đối với các trường hợp này, các chủ thể không phải thực hiện đánh giá tác động đối với hoạt động chuyển dữ liệu.[7] Yêu cầu về hồ sơ, biểu mẫu và thủ tục cho quy trình này được thực hiện theo Nghị định 356/2025/NĐ-CP và các Phụ lục đính kèm.

Trong khi đó, dữ liệu được phân loại là dữ liệu quan trọng hoặc dữ liệu cốt lõi theo Luật Dữ liệu 2024 sẽ chịu sự điều chỉnh của một cơ chế pháp lý riêng. Khi thực hiện chuyển dữ liệu xuyên biên giới đối với các loại dữ liệu này, tổ chức, cá nhân có liên quan phải thực hiện đánh giá tác động của việc chuyển dữ liệu, tập trung vào tính hợp pháp của hoạt động chuyển dữ liệu, các rủi ro tiềm ẩn (như rò rỉ dữ liệu và ảnh hưởng đến an ninh quốc gia), cũng như nghĩa vụ của bên nhận dữ liệu. Hồ sơ, biểu mẫu, và trình tự, thủ tục thực hiện được quy định tại Nghị định 165/2025/NĐ-CP và các Phụ lục đính kèm. Lưu ý, trong trường hợp dữ liệu đồng thời được xác định là dữ liệu cá nhân và dữ liệu cốt lõi hoặc dữ liệu quan trọng, thì không cần thực hiện đánh giá tác động theo Luật BVDLCN 2025.[8]

Cơ chế quản lý hai tầng này đòi hỏi các tập đoàn đa quốc gia phải rà soát lại các luồng dữ liệu nội bộ trong tập đoàn cũng như cấu trúc quản trị dữ liệu toàn cầu, đặc biệt trong trường hợp các hệ thống khu vực hoặc toàn cầu được thiết kế mà không có sự phân tách theo từng khu vực tài phán cụ thể.

4. Cơ chế thực thi và chế tài đối với hành vi không tuân thủ

Báo cáo và thông báo sự cố

Khi xảy ra vi phạm dữ liệu hoặc sự cố an ninh mạng, doanh nghiệp có nghĩa vụ thực hiện việc báo cáo và thông báo tới cơ quan nhà nước có thẩm quyền theo quy định. Tùy thuộc vào tính chất và mức độ nghiêm trọng của sự cố, các nghĩa vụ tương ứng sẽ được áp dụng.

Chẳng hạn, đối với hành vi vi phạm dữ liệu cá nhân, bên xử lý dữ liệu cá nhân có nghĩa vụ thông báo cho bên kiểm soát dữ liệu cá nhân hoặc bên kiểm soát và xử lý dữ liệu cá nhân ngay khi phát hiện vi phạm. Trường hợp hành vi vi phạm có nguy cơ gây ảnh hưởng đến quốc phòng, an ninh quốc gia, trật tự, an toàn xã hội hoặc xâm phạm đến tính mạng, sức khỏe, danh dự, nhân phẩm hoặc tài sản của chủ thể dữ liệu, bên phát hiện hành vi vi phạm phải thực hiện thông báo tới cơ quan nhà nước có thẩm quyền.[9] Luật An ninh mạng 2025 cũng yêu cầu chủ quản hệ thống thông tin thực hiện báo cáo sự cố cho cơ quan nhà nước có thẩm quyền trong thời hạn theo quy định.[10]

Chỉ định nhân sự bảo vệ dữ liệu cá nhân

[5] Điều 1.1 Luật BVDLCN 2025, Điều 1, Điều 3 Luật Dữ liệu 2024
[6] Điều 20.5 Luật BVDLCN 2025
[7] Điều 20.6 Luật BVDLCN 2025
[8] Điều 12 Nghị định 165/2025/NĐ-CP
[9] Điều 23 Luật BVDLCN 2025
[10] Điều 40 Luật An ninh mạng 2025

Đối với bảo vệ dữ liệu cá nhân, tổ chức là bên kiểm soát dữ liệu hoặc bên xử lý dữ liệu có nghĩa vụ chỉ định nhân sự hoặc bộ phận chuyên trách đáp ứng điều kiện về năng lực để phụ trách công tác bảo vệ dữ liệu cá nhân, bao gồm nhưng không giới hạn ở việc tiếp nhận và báo cáo các hành vi vi phạm quy định về bảo vệ dữ liệu cá nhân, tổ chức triển khai các kế hoạch ứng cứu khẩn cấp đối với sự cố bảo vệ dữ liệu cá nhân.[11]

Mặc dù Luật An ninh mạng 2025 không quy định rõ về việc phải chỉ định bộ phận chuyên trách đối với các sự cố an ninh mạng, dự thảo văn bản hướng dẫn thi hành cho thấy các tổ chức, đặc biệt là các đơn vị vận hành hệ thống thông tin quan trọng quốc gia, nên thành lập bộ phận chuyên trách về an ninh mạng với chuyên môn và tính độc lập phù hợp.[12] Tương tự, các tổ chức xử lý dữ liệu cốt lõi hoặc dữ liệu quan trọng cũng phải bảo đảm có các chức năng chuyên trách về giám sát rủi ro, đánh giá, đào tạo và ứng phó sự cố.[13]

Trên cơ sở các yêu cầu này, doanh nghiệp cần cân nhắc kỹ lưỡng việc phân công nhân sự hoặc bộ phận có đủ năng lực phụ trách công tác bảo vệ dữ liệu và tuân thủ an ninh mạng nhằm bảo đảm tuân thủ hiệu quả các quy định pháp luật có liên quan.

Lưu trữ nhật ký hệ thống và lưu giữ chứng cứ

Doanh nghiệp trong nước và nước ngoài khi cung cấp dịch vụ trên mạng viễn thông, mạng Internet, và các dịch vụ gia tăng trên không gian mạng phải lưu nhật ký hệ thống phục vụ cho việc xác minh, điều tra và xử lý các hành vi vi phạm pháp luật an ninh ninh mạng.[14] Việc lưu nhật ký phải bao gồm các thông tin kỹ thuật quan trọng (ví dụ: thông tin tài khoản người dùng, hoạt động đăng nhập/đăng xuất, địa chỉ IP và nhật ký xử lý dữ liệu) và phải được lưu giữ trong một thời hạn nhất định nhằm bảo đảm khả năng truy xuất và tuân thủ quy định pháp luật.[15]

Đối với hệ thống thông tin quan trọng về an ninh quốc gia, một số yêu cầu bổ sung được áp dụng, bao gồm lưu trữ nhật ký hệ thống theo hình thức tập trung, sao lưu dữ liệu định kỳ, cũng như ghi nhận các hoạt động của hệ thống, lỗi phát sinh và các sự cố an ninh mạng.[16] Tương tự, theo Nghị định 165/2025/NĐ-CP, các tổ chức quản lý dữ liệu cốt lõi hoặc dữ liệu quan trọng phải duy trì nhật ký, đồng thời triển khai kế hoạch dự phòng và tiến hành diễn tập ứng phó sự cố định kỳ.[17]

Bên cạnh nghĩa vụ lưu nhật ký hệ thống, các tổ chức phải tuân thủ nghĩa vụ lưu giữ các tài liệu quan trọng chứng minh việc tuân thủ quy định về bảo vệ dữ liệu và an ninh mạng. Các tài liệu này bao gồm báo cáo đánh giá tác động bảo vệ dữ liệu cá nhân và báo cáo đánh giá tác động chuyển dữ liệu cá nhân xuyên biên giới theo quy định tại Nghị định 356/2025/NĐ-CP[18], cũng như báo cáo đánh giá rủi ro đối với hoạt độnng xử lý dữ liệu cốt lõi, dữ liệu quan trọng theo Nghị định 165/2025/NĐ-CP[19]. Các hồ sơ, tài liệu hỗ trợ như nhật ký xử lý dữ liệu cốt lõi và dữ liệu quan trọng, nhật ký truy cập của nhân sự quản trị, tài liệu liên quan đến diễn tập ứng phó sự cố, cũng như nhật

[11] Điều 13.2 Nghị định 356/2025/NĐ-CP, Điều 14.1.d,e Nghị định 356/2025/NĐ-CP

[12] Điều 4.2 và 4.3 Dự thảo Nghị định hướng dẫn chi tiết Luật An ninh mạng 2025

[13] Điều 13 Nghị định 165/2025/NĐ-CP

[14] Điều 25.2.b Luật An ninh mạng 2025

[15] Điều 25.6.b,c Dự thảo Nghị định hướng dẫn chi tiết Luật An ninh mạng 2025

[16] Mục 4.dd Phụ lục 2, Điều 33.2 Dự thảo Nghị định hướng dẫn chi tiết Luật An ninh mạng 2025

[17] Điều 19.8 Nghị định 165/2025/NĐ-CP

[18] Điều 18, 19 Nghị định 365/2025/NĐ-CP

[19] Điều 17 Nghị định 165/2025/NĐ-CP

ký sao lưu và khôi phục dữ liệu cũng cần được lưu giữ nhằm phục vụ cho hoạt động thanh tra, kiểm tra và điều tra của cơ quan nhà nước có thẩm quyền.[20]

Chế tài và xử phạt đối với hành vi vi phạm

Thực tiễn thực thi gần đây cho thấy các hành vi vi phạm được xử lý theo khuôn khổ pháp luật hiện hành. Các vi phạm hành chính hiện chủ yếu được điều chỉnh bởi Nghị định 15/2020/NĐ-CP, văn bản này vẫn đang được áp dụng trên thực tế, trong khi các hành vi có dấu hiệu tội phạm sẽ chịu sự điều chỉnh của Bộ luật Hình sự 2015. Theo Nghị định 15/2020/NĐ-CP, các hình thức xử phạt chính bao gồm cảnh cáo và phạt tiền.

Dự thảo Nghị định quy định xử phạt vi phạm hành chính trong lĩnh vực an ninh mạng và bảo vệ dữ liệu cá nhân trên cơ sở Luật BVDLCN 2025 và Luật An ninh mạng 2025 đề xuất một cơ chế xử phạt theo hướng tinh gọn hơn, trong đó phạt tiền là hình thức xử phạt chủ yếu, phản ánh xu hướng tăng cường tính nghiêm khắc và khả năng răn đe trong hoạt động thực thi pháp luật. Dự thảo cũng đưa ra các chế tài cụ thể, bao gồm mức phạt dựa trên doanh thu lên đến 5% tổng doanh thu hằng năm đối với một số hành vi vi phạm liên quan đến chuyển dữ liệu xuyên biên giới. Đối với hành vi mua bán dữ liệu cá nhân, mức phạt có thể lên đến 10 lần khoản lợi bất hợp pháp thu được từ hành vi vi phạm đó.[21]

Đối với các tập đoàn đa quốc gia, cơ chế xử phạt dựa trên doanh thu có thể làm gia tăng đáng kể mức độ rủi ro tài chính, đặc biệt trong bối cảnh các hoạt động xử lý và chuyển dữ liệu xuyên biên giới thường được thực hiện trên quy mô lớn. Do đó, việc chú trọng tuân thủ các nghĩa vụ pháp lý có liên quan là cần thiết nhằm giảm thiểu các rủi ro pháp lý và tài chính tiềm ẩn.

5. Một số lưu ý quan trọng cho các tập đoàn đa quốc gia

Để bảo đảm tuân thủ trong giai đoạn chờ ban hành các văn bản hướng dẫn thi hành, các tập đoàn đa quốc gia nên ưu tiên triển khai các biện pháp kiểm soát đã được quy định rõ trong các văn bản luật và ít có khả năng thay đổi đáng kể, đặc biệt tập trung vào các luồng dữ liệu xuyên biên giới, hoạt động chuyển dữ liệu nội bộ trong tập đoàn và việc nội địa hóa các khuôn khổ quản trị dữ liệu toàn cầu, nhất là đối với các lĩnh vực có mức độ rủi ro pháp lý trực tiếp.

(i) **Quản trị và phân loại dữ liệu**

Xác định và phân loại dữ liệu dựa trên các tiêu chí chung, bao gồm phân loại theo loại dữ liệu (ví dụ: dữ liệu cá nhân, đặc biệt là dữ liệu cá nhân nhạy cảm như dữ liệu về tình trạng sức khỏe) và theo mức độ quan trọng về mặt pháp lý (ví dụ: khả năng được xác định là dữ liệu cốt lõi hoặc dữ liệu quan trọng).

(ii) **Tuân thủ chuyển dữ liệu xuyên biên giới**

- Chuẩn bị hồ sơ đánh giá chuyển dữ liệu cá nhân xuyên biên giới.
- Xác định liệu dữ liệu có thể thuộc phạm vi dữ liệu cốt lõi/dữ liệu quan trọng hay không (kéo theo các yêu cầu nghiêm ngặt hơn).

[20] Điều 17, 19 Nghị định 165/2025/NĐ-CP; Điều 31, 33, Mục 4.b và Mục 4.dd Phụ lục 2 Dự thảo Nghị định hướng dẫn chi tiết Luật An ninh mạng 2025

[21] Điều 6, Dự thảo Nghị định quy định xử phạt vi phạm hành chính trong lĩnh vực an ninh mạng và bảo vệ dữ liệu cá nhân

- Điều chỉnh các thỏa thuận nội bộ trong tập đoàn phù hợp với yêu cầu của pháp luật Việt Nam.

(iii) **Đảm bảo cơ sở pháp lý và xây dựng cơ chế xin sự đồng ý**

- Đảm bảo cơ chế xin sự đồng ý của chủ thể dữ liệu cá nhân hợp pháp, đặc biệt đối với các dữ liệu cá nhân nhạy cảm (như dữ liệu về tình trạng sức khỏe)

- Rà soát và cập nhật thông báo bảo mật và chính sách nội bộ.

(iv) **Sẵn sàng phát hiện và báo cáo sự cố:** Thiết lập quy trình nội bộ, xác định ngưỡng báo cáo, chính sách leo thang xử lý sự cố và thẩm quyền ra quyết định.

(v) **Lưu nhật ký, giám sát và lưu giữ chứng cứ:** Triển khai hệ thống ghi nhật ký có khả năng theo dõi truy cập người dùng và hoạt động hệ thống, lưu giữ nhật ký đầy đủ và bảo đảm dấu vết kiểm toán sẵn sàng phục vụ thanh tra, kiểm tra.

(vi) **Quản trị trị nội bộ và phân công trách nhiệm:** Chỉ định nhân sự phụ trách bảo vệ dữ liệu (Nhận sự bảo vệ dữ liệu cá nhân hoặc chức danh tương đương) và xác định rõ trách nhiệm giữa các bộ phận CNTT, Pháp chế và Tuân thủ.

Đồng thời, doanh nghiệp cũng cần lưu ý các thay đổi pháp lý quan trọng, đặc biệt là việc mở rộng phạm vi các hành vi bị nghiêm cấm trên không gian mạng nhằm ứng phó với các rủi ro công nghệ mới phát sinh. Đáng lưu ý, pháp luật đã quy định rõ việc cấm sử dụng trí tuệ nhân tạo để giả mạo hoặc mạo danh cá nhân. Khuôn khổ pháp lý cũng tăng cường các biện pháp bảo vệ trước các nguy cơ trên môi trường mạng, bao gồm cơ chế bảo vệ trẻ em chặt chẽ hơn, đồng thời mở rộng phạm vi nội dung bị cấm để bao gồm cả thông tin sai lệch và các hành vi trình bày sai sự thật. Trong bối cảnh đó, doanh nghiệp cần dự liệu khả năng cơ quan quản lý sẽ tăng cường giám sát và kiểm tra trong thời gian tới.

Trong bối cảnh khuôn khổ pháp lý của Việt Nam tiếp tục được hoàn thiện, việc xây dựng cơ chế tuân thủ chủ động và hoàn thiện sẽ trở thành một yếu tố tạo lợi thế cạnh tranh quan trọng đối với các doanh nghiệp hoạt động tại thị trường Việt Nam. Trên thực tế, các tập đoàn đa quốc gia nên cân nhắc liệu mô hình quản trị dữ liệu toàn cầu hiện tại có cần được điều chỉnh để phù hợp với các yêu cầu pháp lý đang ngày càng phát triển tại Việt Nam hay không. Việc tham gia và theo dõi sát sao các thay đổi về mặt chính sách và pháp luật không chỉ giúp doanh nghiệp cập nhật kịp thời xu hướng quản lý nhà nước mà còn tạo cơ hội đóng góp ý kiến vào quá trình xây dựng chính sách, qua đó bảo đảm các góc nhìn thực tiễn từ hoạt động kinh doanh được xem xét trong quá trình ban hành các văn bản pháp luật mới.

LIÊN HỆ

Để biết thêm thông tin, vui lòng liên hệ với các Luật sư Thành viên của chúng tôi:

Ông **Bùi Ngọc Hồng**

Sáp nhập & Mua lại, Đầu tư nước ngoài, Tuân thủ Pháp luật, Lao động, Giải quyết tranh chấp

Hong.Bui@LNTpartners.com

Ông **Trần Thái Bình**

Quản trị doanh nghiệp, Lao động, Đầu tư nước ngoài, Giải quyết tranh chấp, Bất động sản, Sáp nhập & Mua lại, Thuế

Binh.Tran@LNTpartners.com

Bà **Hoàng Nguyễn Hạ Quyên**

Sáp nhập & Mua lại, Tuân thủ Pháp luật, Lao động, Phá sản & Tái cấu trúc

Quyen.Hoang@LNTpartners.com

Ông **Lê Nết**

Tài chính & Ngân hàng, Bất động sản, Giải quyết tranh chấp, Sáp nhập & Mua lại, Thuế

Net.Le@LNTpartners.com

Ông **Nguyễn Anh Tuấn**

Chống độc quyền/Cạnh tranh, Sáp nhập & Mua lại, Lao động, Tuân thủ Pháp luật, Đầu tư nước ngoài

Tuan.Nguyen@LNTpartners.com

Ông **Nguyễn Xuân Thủy**

Sáp nhập & Mua lại, Đầu tư nước ngoài, Lao động, Thuế

Thuy.Nguyen@LNTpartners.com

Bà **Vũ Thanh Minh**

Thuế, Đầu tư nước ngoài, Tài chính & Ngân hàng, Quản trị doanh nghiệp, Sáp nhập & Mua lại

Minh.Vu@LNTpartners.com

Ông **Nguyễn Công Phú**

Giải quyết tranh chấp

Phu.Nguyen@LNTpartners.com

Bà **Lương Trung Vân Nhi**

Giải quyết tranh chấp, Lao động

VanNhi.Luong@LNTpartners.com

Bà **Nguyễn Thị Điệp**

Giải quyết tranh chấp, Tài chính & Ngân hàng, Lao động, Thuế, Sở hữu trí tuệ, Tuân thủ Pháp luật

Diep.Nguyen@LNTpartners.com

Ông **Ngô Thanh Hải**

Tài chính & Ngân hàng, Quản trị doanh nghiệp, Giải quyết tranh chấp, Bất động sản

Hai.Ngo@LNTpartners.com

Bà **Vũ Thị Thịnh**

Đầu Tư Nước Ngoài, Sáp nhập & Mua lại, Tuân Thủ Pháp Luật, Giải quyết tranh chấp, Cơ sở hạ tầng, Năng Lượng & Tài Nguyên

ThiThinh.Vu@LNTpartners.com

Để biết thêm thông tin, vui lòng liên hệ:

Tp. Hồ Chí Minh (trụ sở chính)

Tầng 12A, Tòa tháp Saigon Marina IFC,
Số 2 Tôn Đức Thắng, Phường Sài Gòn

+84 28 3821 2357

Hà Nội

Tầng 12, Tòa nhà Pacific Place,
83B Lý Thường Kiệt, Phường Cửa Nam

+84 24 3824 8522

Về chúng tôi

LNT & PARTNERS ("LNT") là một công ty luật độc lập tại Việt Nam, cung cấp dịch vụ pháp lý toàn diện với thế mạnh trong các lĩnh vực doanh nghiệp và M&A, cạnh tranh, dược phẩm, bất động sản, hạ tầng, tài chính, cũng như các vụ tranh tụng và trọng tài phức tạp. Chúng tôi tự hào là một trong những hãng luật hàng đầu tại Việt Nam, đồng hành cùng nhiều khách hàng trong nước và quốc tế, bao gồm các tập đoàn thuộc danh sách Fortune Global 500 và nhiều công ty niêm yết uy tín tại Việt Nam.

Nếu bạn cần thêm thông tin liên quan đến bất kỳ bản tin pháp lý nào, đừng ngần ngại liên hệ trực tiếp với các tác giả.