



DOANH NGHIỆP NHỎ VÀ NHỮNG THÁCH THỨC VỀ BẢO MẬT DỮ LIỆU - LUẬT DỮ LIỆU MỚI SẼ LÀM THAY ĐỔI CUỘC CHƠI

GÓC NHÌN PHÁP LÝ

THÁNG 3 – 2025



GIỚI THIỆU

Trong nền kinh tế số đang phát triển nhanh chóng của Việt Nam, bảo mật dữ liệu là một vấn đề quan trọng cần lưu ý. Tuy nhiên, nhiều doanh nghiệp nhỏ và vừa (“SMEs”) đang gặp khó khăn trong việc tuân thủ các quy định về bảo vệ dữ liệu do hạn chế về nguồn lực và chuyên môn.

Báo cáo Thường niên năm 2024 của Cục An toàn thông tin (AIS) thuộc Bộ Thông tin và Truyền thông (MIC) cho thấy hơn 70% các doanh nghiệp này chưa có các biện pháp bảo vệ dữ liệu toàn diện, khiến họ dễ bị tấn công trước các mối đe dọa và rủi ro pháp lý trên không gian mạng. Thông qua việc ban hành Nghị định số 13/2023/NĐ-CP về Bảo vệ dữ liệu cá nhân và Luật Dữ liệu số 60/2024/QH15, Chính phủ Việt Nam đặt mục tiêu tăng cường việc tuân thủ bảo mật dữ liệu.

Bài viết này sẽ phân tích những thách thức chính mà các SMEs đang đối mặt trong quản lý dữ liệu và sự tác động của khung pháp lý mới trong bối cảnh bảo vệ dữ liệu hiện tại.

I.

THÁCH THỨC VỀ BẢO MẬT DỮ LIỆU MÀ SMEs PHẢI ĐỐI MẶT

II.

LUẬT DỮ LIỆU MỚI CÓ THỂ GIÚP CÁC SMEs THAY ĐỔI CUỘC CHƠI NHƯ THẾ NÀO

III.

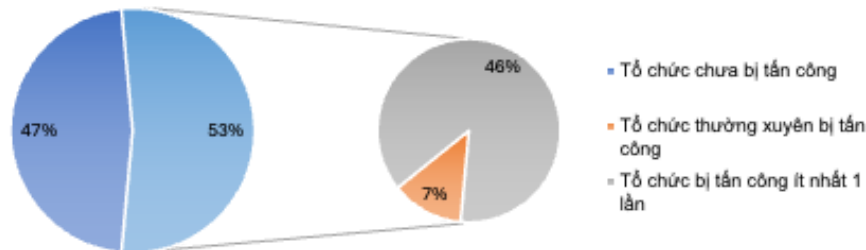
SMEs CẦN LÀM GÌ ĐỂ TUÂN THỦ LUẬT BẢO VỆ DỮ LIỆU VÀ ĐẢM BẢO HOẠT ĐỘNG CỦA DOANH NGHIỆP?

THÁCH THỨC VỀ BẢO MẬT DỮ LIỆU MÀ CÁC DOANH NGHIỆP NHỎ PHẢI ĐỐI MẶT

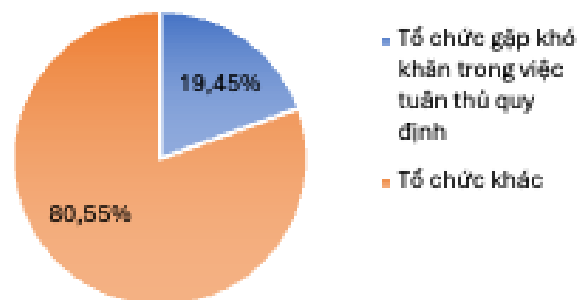
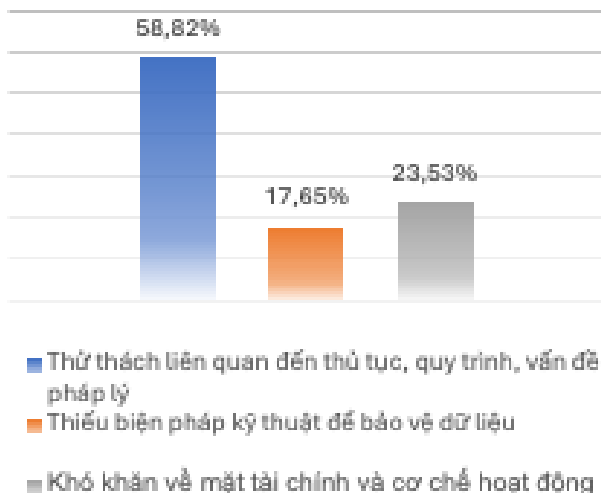
SMEs tại Việt Nam thường thiếu nguồn lực để đáp ứng yêu cầu về bảo mật dữ liệu. Dưới đây là một số những thách thức chính được nêu trong các báo cáo chính thống:

1. Chưa trang bị đầy đủ kiến thức về Luật Bảo vệ dữ liệu

Báo cáo tổng kết An ninh mạng 2024 đối với các cơ quan và doanh nghiệp cho thấy 46.15% các tổ chức này từng bị tấn công mạng ít nhất một lần trong năm qua, trong đó, 6.77% thường xuyên bị tấn công. Tổng số vụ tấn công mạng trong năm 2024 ước tính lên tới 659,000 vụ và có tới 14.59% cơ quan, doanh nghiệp cho biết đã bị tấn công bằng mã độc ransomware trong năm qua, gây ảnh hưởng nghiêm trọng đến tài chính và uy tín của họ.



Mặc dù phải đối mặt với những rủi ro trên, chỉ 56.53% tổ chức có nhân sự chuyên trách về bảo vệ dữ liệu cá nhân, trong khi 43.47% tổ chức còn lại hoặc không có nhân sự chuyên trách hoặc phải phụ thuộc vào nguồn nhân lực bán thời gian. Hơn nữa, 19.45% các cơ quan, doanh nghiệp gặp khó khăn trong việc tuân thủ quy định do tính phức tạp của các thủ tục pháp lý. Một lượng lớn các tổ chức cũng chưa có đủ chuyên môn kỹ thuật để triển khai các biện pháp bảo mật cơ bản, chẳng hạn như mã hoá và lưu trữ dữ liệu an toàn. Trong các vấn đề được nêu ra, vướng mắc lớn nhất là về thủ tục, quy trình, pháp lý, chiếm đến 58.82% và thiếu các biện pháp kỹ thuật để bảo vệ dữ liệu chiếm 17.65%. Báo cáo cho thấy sự phức tạp từ thủ tục pháp lý là thách thức chính, từ đó làm nổi bật nhu cầu cấp thiết về hướng dẫn thực hiện cụ thể rõ ràng và các biện pháp an ninh mạng mạnh mẽ hơn.



I.

THÁCH THỨC VỀ BẢO MẬT DỮ LIỆU MÀ CÁC SMES PHẢI ĐỐI MẶT

2. Hạn chế về mặt tài chính

Việc tuân thủ các quy định về bảo mật dữ liệu cá nhân đòi hỏi khoản đầu tư đáng kể vào hạ tầng an ninh mạng, bao gồm phần mềm bảo mật, phần cứng và các biện pháp lưu trữ an toàn. Tuy nhiên, các doanh nghiệp vừa và nhỏ thường gặp khó khăn trong việc phân bổ nguồn lực cho các khoản đầu tư này. Tại Hội nghị Thường trực Chính phủ ngày 27/02/2025 – nơi các chiến lược đột phá cho các SMEs được thảo luận, chỉ khoảng 30 – 35% các doanh nghiệp này báo cáo rằng họ có thể tiếp cận các khoản vay ưu đãi dành cho đầu tư an ninh mạng. Điều này cho thấy hạn chế về mặt tài chính là một rào cản lớn trong việc tuân thủ quy định. Ngoài ra, doanh nghiệp được kỳ vọng sẽ dành ít nhất 10% ngân sách cho an ninh mạng, công nghệ thông tin và các hoạt động vận hành – yêu cầu mà nhiều doanh nghiệp nhỏ và vừa không thể đáp ứng. Chi phí tuân thủ không chỉ giới hạn trong cơ sở hạ tầng mà còn bao gồm các công cụ bảo mật, đào tạo nhân sự và tư vấn pháp lý, gây áp lực lên nguồn tài chính hạn chế.

Mặc cho Chính phủ đã có những chính sách hỗ trợ, việc tiếp cận vẫn còn hạn chế. Chỉ có 25% các SMEs hưởng được lợi ích từ các gói tín dụng hỗ trợ chuyển đổi số và bảo mật dữ liệu. Điều này nhấn mạnh những thách thức về mặt tài chính mà các doanh nghiệp này phải đối mặt trong việc đáp ứng các yêu cầu về bảo mật dữ liệu, buộc họ phải tự gánh chịu các chi phí mà không có sự hỗ trợ phù hợp từ bên ngoài.



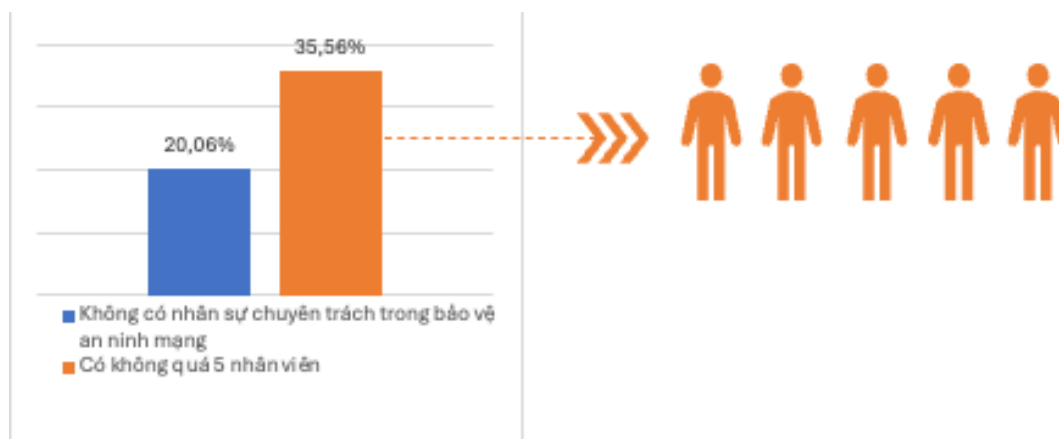
THÁCH THỨC VỀ BẢO MẬT DỮ LIỆU MÀ CÁC SMES PHẢI ĐỐI MẶT

3. Thiếu Hệ thống Quản lý Dữ liệu hoàn thiện, nguồn lực và chuyên môn còn hạn chế.

Một thách thức thường thấy ở các SMEs tại Việt Nam là thiếu Hệ thống Quản lý Dữ liệu hoàn thiện. Nhiều doanh nghiệp vẫn còn phải phụ thuộc vào các phương pháp truyền thống như bảng tính hay hồ sơ bản giấy, dễ dẫn đến sự kém hiệu quả, sai sót, trùng lặp dữ liệu và tăng nguy cơ mất dữ liệu. Việc thiếu hệ thống dữ liệu tích hợp còn hạn chế khả năng xử lý khối lượng dữ liệu lớn một cách hiệu quả, cản trở quá trình ra quyết định chiến lược và phân tích khách hàng. Lưu trữ không có tổ chức, định dạng không nhất quán và hệ thống bảo mật yếu kém khiến doanh nghiệp dễ bị tấn công mạng và vi phạm quy định pháp luật.

Hạn chế về nguồn lực cũng ngăn cản nhiều doanh nghiệp nhỏ và vừa đầu tư vào hệ thống quản lý dữ liệu tiên tiến hoặc tuyển dụng nhân sự công nghệ thông tin và an ninh mạng có chuyên môn. Báo cáo tổng kết An ninh mạng năm 2024 cho thấy 20.06% đơn vị chưa có đơn vị chuyên trách về an ninh mạng, trong khi có 35.56% cơ quan, doanh nghiệp chỉ bố trí được không quá 05 (năm) người phụ trách về an ninh mạng, một con số rất nhỏ so với mức cần thiết để đối phó với các mối đe dọa trên không gian mạng.

Để giải quyết những thách thức này, cần có các hướng dẫn pháp lý rõ ràng hơn, hỗ trợ tài chính và tăng cường đầu tư vào hạ tầng an ninh mạng để giúp các SMEs tuân thủ các quy định mới về bảo mật dữ liệu và có thể đối mặt với các rủi ro trên nền tảng số.



Nhằm đảm bảo an ninh mạng, các tổ chức phải áp dụng mô hình Trung tâm điều hành an ninh 24/7 bao gồm 03 (ba) ca làm việc và 04 (bốn) đội trực. Mỗi tổ chức cần ít nhất 08 (tám) đến 10 (mười) vị trí chuyên trách. Việc thiếu nhân lực ảnh hưởng đến việc quản lý rủi ro và giảm hiệu quả các biện pháp ứng phó và khắc phục sự cố. Điều này khiến các tổ chức dễ bị tấn công mạng hơn cũng như bị thiệt hại nghiêm trọng về mặt tài chính và uy tín. Do đó, việc các doanh nghiệp không chú trọng trong việc bảo mật dữ liệu; giao phó cho các nhân viên không có chuyên môn trong việc bảo mật dữ liệu; thiếu hiểu biết cùng với việc không đào tạo nhân sự phù hợp dễ dẫn đến việc xử lý sai dữ liệu khách hàng. Nếu không có chương trình đào tạo bài bản hoặc không có chuyên môn, các biện pháp bảo vệ dữ liệu thường bị bỏ qua, khiến doanh nghiệp dễ đối mặt với việc rò rỉ thông tin và không tuân thủ quy định của pháp luật.



II. LUẬT DỮ LIỆU MỚI CÓ THỂ GIÚP CÁC SMES THAY ĐỔI CUỘC CHƠI NHƯ THẾ NÀO

Các quy định mới về bảo vệ dữ liệu, bao gồm Nghị định 13/2023/NĐ-CP về Bảo vệ dữ liệu cá nhân và Luật Dữ liệu số 60/2024/QH15, không chỉ đưa ra các yêu cầu nghiêm ngặt hơn mà còn tạo ra nhiều cơ hội cho các SMEs thay đổi cách quản lý và bảo vệ dữ liệu.

- Tăng cường bảo mật và giảm thiểu rủi ro rò rỉ dữ liệu;
- Mở rộng cơ hội kinh doanh quốc tế;
- Hỗ trợ từ Chính phủ và Hiệp hội Doanh nghiệp trong việc tuân thủ bảo vệ dữ liệu cho các SMEs.

LUẬT DỮ LIỆU MỚI CÓ THỂ GIÚP CÁC SMES THAY ĐỔI CUỘC CHƠI NHƯ THẾ NÀO

1. Tăng cường bảo mật và giảm thiểu rủi ro rò rỉ dữ liệu

Việc triển khai các biện pháp bảo vệ dữ liệu cá nhân theo Luật Dữ liệu mới cho phép các SMEs giảm thiểu rủi ro an ninh và bảo vệ thông tin khách hàng. Ứng dụng công nghệ bảo mật tiên tiến ngăn chặn tấn công mạng, rò rỉ dữ liệu và lạm dụng thông tin cá nhân, đảm bảo hoạt động kinh doanh liên tục và tuân thủ quy định pháp luật. Luật Dữ liệu ban hành mức xử phạt nghiêm khắc, bao gồm phạt tiền lên đến 5% doanh thu hàng năm, như được nêu trong Dự thảo Nghị định về xử phạt hành chính đối với vi phạm an toàn thông tin mạng. Việc tuân thủ các quy định này không chỉ giảm thiểu rủi ro về mặt tài chính và pháp lý mà còn bảo vệ danh tiếng thương hiệu, củng cố niềm tin khách hàng. Hơn nữa, việc tuân thủ quy định pháp luật cũng khuyến khích các SMEs áp dụng công nghệ bảo mật tiên tiến, tăng cường khả năng phòng thủ trước các cuộc tấn công mạng và nâng cao hiệu quả hoạt động lâu dài.



2. Mở rộng cơ hội kinh doanh quốc tế

Một trong những tác động tích cực của Luật Dữ liệu mới là tạo điều kiện thuận lợi cho các doanh nghiệp vừa và nhỏ tiếp cận thị trường quốc tế dễ dàng hơn. Việc tuân thủ quy định về bảo mật dữ liệu củng cố niềm tin từ khách hàng trong nước và nâng cao khả năng hợp tác của các doanh nghiệp với đối tác quốc tế - đặc biệt tại các khu vực như Liên minh châu Âu, nơi cần phải tuân thủ Quy định bảo vệ dữ liệu chung. Các quy định tương tự tại các quốc gia khác cũng nhấn mạnh tầm quan trọng của việc bảo vệ dữ liệu trong hoạt động kinh doanh toàn cầu. Việc đáp ứng các tiêu chuẩn bảo vệ dữ liệu quốc tế giúp doanh nghiệp tham gia vào các hiệp định thương mại thuận lợi hơn, mở rộng cơ hội thị trường, từ đó tăng nguồn doanh thu. Trong bối cảnh toàn cầu hoá và thương mại điện tử phát triển nhanh chóng, việc tuân thủ quy định không chỉ là yêu cầu pháp lý mà còn là lợi thế cạnh tranh, giúp các SMEs thành công trong giao dịch xuyên biên giới. Bằng cách ưu tiên bảo mật dữ liệu, các doanh nghiệp này có thể giảm thiểu rủi ro pháp lý, nâng cao danh tiếng thương hiệu, xây dựng niềm tin với khách hàng và đối tác. Chiến lược tuân thủ quy định như vậy không chỉ làm tăng tính cạnh tranh mà còn thúc đẩy đổi mới sáng tạo và phát triển bền vững trong nền kinh tế số toàn cầu.

LUẬT DỮ LIỆU MỚI CÓ THỂ GIÚP CÁC DOANH NGHIỆP NHỎ THAY ĐỔI CUỘC CHƠI NHƯ THẾ NÀO

3. Hỗ trợ từ Chính phủ và Hiệp hội Doanh nghiệp trong việc tuân thủ bảo vệ dữ liệu cho SMEs

Nhằm giúp các SMEs trong việc tuân thủ các quy định bảo vệ dữ liệu mới, Chính phủ và các hiệp hội doanh nghiệp đã tổ chức các chương trình hỗ trợ nhằm đảm bảo việc tuân thủ quy định và nâng cao biện pháp bảo mật dữ liệu.

- **Chương trình đào tạo miễn phí**

Chính phủ và hiệp hội doanh nghiệp tổ chức các chương trình đào tạo miễn phí nhằm trang bị cho các doanh nghiệp vừa và nhỏ những kỹ năng và kiến thức quan trọng để bảo vệ dữ liệu. Các khoá học này tập trung vào những chủ đề chính như mã hoá dữ liệu, quản lý truy cập và các phương pháp an ninh mạng tốt nhất, giúp các doanh nghiệp này giảm thiểu rủi ro và tăng cường khả năng bảo mật dữ liệu.

- **Hỗ trợ và hướng dẫn về mặt kỹ thuật**

Các tổ chức như Liên đoàn Thương mại và Công nghiệp Việt Nam (VCCI) và Hiệp hội Thương mại điện tử Việt Nam (VECOM) cung cấp hỗ trợ kỹ thuật thông qua tài liệu hướng dẫn, công cụ và hướng dẫn chi tiết về cách triển khai các biện pháp bảo vệ dữ liệu. Những tài nguyên này giúp các doanh nghiệp vừa và nhỏ tuân thủ quy định pháp luật dễ dàng và áp dụng các giải pháp bảo mật thực tiễn mà không cần chuyên môn sâu về công nghệ.

- **Xây dựng hệ thống tuân thủ vững chắc**

Sự hợp tác giữa Chính phủ và Hiệp hội doanh nghiệp tạo ra một hệ thống hỗ trợ toàn diện giúp các doanh nghiệp vừa và nhỏ tự tin đáp ứng nghĩa vụ tuân thủ quy định pháp luật. Bằng cách tận dụng các nguồn tài nguyên, chương trình đào tạo và hỗ trợ kỹ thuật, các doanh nghiệp này có thể củng cố niềm tin của khách hàng, phát triển việc vận hành hệ thống bảo vệ và tạo nền tảng vững chắc cho sự phát triển bền vững của doanh nghiệp trong nền kinh tế toàn cầu ngày càng phát triển dựa trên dữ liệu.



CÁC SMES CẦN LÀM GÌ ĐỂ TUÂN THỦ LUẬT BẢO VỆ DỮ LIỆU VÀ ĐẢM BẢO HOẠT ĐỘNG CỦA DOANH NGHIỆP?



Nhằm tuân thủ một cách hiệu quả các quy định về bảo vệ dữ liệu, các SMEs cần phải xây dựng chiến lược bảo vệ dữ liệu toàn diện, bao gồm các biện pháp pháp lý, kỹ thuật và quy trình. Dưới đây là những hoạt động chính mà các SMEs cần phải làm để đảm bảo việc tuân thủ và tăng cường khả năng bảo mật dữ liệu:

Ban hành chính sách bảo vệ dữ liệu rõ ràng	- Các SMEs cần xây dựng và thiết lập chính sách bảo vệ dữ liệu, quy định chi tiết về quy trình thu thập, xử lý, lưu trữ và chia sẻ thông tin cá nhân. - Đảm bảo chính sách phù hợp với Nghị định 13/2023/NĐ-CP về Bảo vệ dữ liệu cá nhân và Luật Dữ liệu số 60/2024/QH15 để tránh vi phạm pháp luật. - Chỉ định nhân sự phụ trách bảo mật dữ liệu hoặc chỉ định người giám sát việc thực thi chính sách và tuân thủ quy định pháp luật.
Đào tạo và nâng cao nhận thức cho nhân viên	- Tổ chức đào tạo định kỳ cho nhân viên về các quy định bảo mật thông tin, giao thức an ninh và những mối đe dọa tiềm ẩn trên không gian mạng. - Đào tạo theo vai trò để nhân sự hiểu được trách nhiệm của họ trong việc xử lý dữ liệu. - Kiểm soát nghiêm ngặt, chỉ cho phép nhân sự có thẩm quyền tiếp cận dữ liệu quan trọng.
Đầu tư vào Công nghệ Bảo mật	- Triển khai các phần mềm mã hoá, tường lửa, và biện pháp lưu trữ an toàn để bảo vệ các thông tin nhạy cảm trước các mối đe dọa trên nền tảng số. - Áp dụng xác thực đa yếu tố (MFA) và hệ thống phát hiện xâm nhập (IDS) để ngăn chặn truy cập trái phép. - Đánh giá rủi ro an ninh mạng thường xuyên để phát hiện lỗ hổng và đưa ra biện pháp xử lý kịp thời.

CÁC DOANH NGHIỆP VỪA VÀ NHỎ CẦN LÀM GÌ ĐỂ TUÂN THỦ LUẬT BẢO VỆ DỮ LIỆU VÀ ĐẢM BẢO HOẠT ĐỘNG CỦA DOANH NGHIỆP?

Tuân thủ các cập nhật pháp lý và phối hợp với cơ quan chức năng	• Theo dõi các cập nhật từ các cơ quan chức năng có liên quan. • Các doanh nghiệp vừa và nhỏ nên kết nối với các hiệp hội doanh nghiệp như VCCI và VECOM để cập nhật các hướng dẫn về việc tuân thủ và các phương pháp tối ưu nhất. • Phối hợp với các cơ quan chức năng để kiểm tra định kỳ và dùng hỗ trợ pháp lý khi cần.
Xây dựng kế hoạch ứng phó sự cố và kiểm toán bảo mật	• Xây dựng kế hoạch ứng phó sự cố nhằm nhanh chóng phát hiện và hạn chế rủi ro khi bị tấn công trên nền tảng số. • Tiến hành kiểm toán bảo mật và kiểm tra việc xâm nhập thường xuyên để đảm bảo hệ thống an toàn. • Xây dựng chính sách lưu trữ và huỷ dữ liệu để quản lý dữ liệu theo đúng quy trình an toàn.
Tận dụng các chương trình hỗ trợ từ Chính phủ và ngành công nghiệp	• Tận dụng các sáng kiến an ninh mạng do Chính phủ hỗ trợ như chương trình đào tạo và hỗ trợ tài chính cho chuyển đổi số. • Đăng ký các khoản vay ưu đãi hoặc quỹ hỗ trợ các SMEs từ hiệp hội doanh nghiệp trong việc xây dựng cơ sở hạ tầng an ninh mạng.

Bằng cách chủ động triển khai các biện pháp này, các SMEs có thể tuân thủ quy định của pháp luật Việt Nam trong việc bảo vệ an toàn dữ liệu, giảm thiểu rủi ro và xây dựng uy tín với khách hàng cũng như đối tác. Một hệ thống bảo vệ dữ liệu vững chắc không chỉ bảo vệ hoạt động doanh nghiệp mà còn tạo cơ hội cho việc mở rộng thị trường quốc tế.





Nội dung trong tài liệu này không cấu thành tư vấn pháp lý và cũng không phản ánh ý kiến của chúng tôi hoặc bất kỳ chuyên gia tư vấn nào của chúng tôi. Mặc dù chúng tôi cố gắng cung cấp thông tin chính xác và cập nhật nhất một cách có thể, chúng tôi không thể đảm bảo rằng những thông tin này còn chính xác lúc người đọc nhận được hoặc sẽ duy trì tính chính xác này trong tương lai. Bất cứ ai cũng không nên quyết định hành động dựa trên những thông tin trong tài liệu này nếu không có sự tư vấn pháp lý phù hợp từ các chuyên gia sau khi xem xét từng tình huống cụ thể. Bạn nên liên hệ với luật sư của Q&A để được tư vấn cho các vấn đề pháp lý cụ thể.

Nếu có bất kỳ thắc mắc nào, xin vui lòng liên hệ:



Nguyễn Thanh Hải

Luật sư thành viên

T: +84 94 651 8259

E: hainguyen@quoclaw.vn



Nguyễn Quang Tiên Yên

Cộng sự

T: +84 82 523 0998

E: yennguyen@quoclaw.vn

CÔNG TY LUẬT TNHH QUỐC VÀ CỘNG SỰ

Tầng 1, Số 1 Trần Khánh Dư, Phường Tân Định, Quận 1, Thành phố Hồ Chí Minh.

www.quoclaw.vn

T: +84 985 036 774

QA | QUOC &
ASSOCIATES