

[Trang chủ](#) > [Pháp luật](#) > Nghiên cứu - Trao đổi

Làm sao để bảo vệ dữ liệu cá nhân trong quan hệ lao động?

Luật sư Nguyễn Ngọc Hà (*) | 09/08/2026 11:05

Sự ra đời của Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15 và Nghị định số 356/2025/NĐ-CP không chỉ bổ sung một nghĩa vụ tuân thủ mới mà còn đặt ra yêu cầu thay đổi tư duy quản trị.



Nâng cao năng lực bảo vệ dữ liệu cá nhân sẽ góp phần nâng cao uy tín, giảm rủi ro và tăng khả năng cạnh tranh. Ảnh minh họa

Đối với cộng đồng doanh nghiệp, đặc biệt là doanh nghiệp đang đẩy mạnh chuyển đổi số, doanh nghiệp có vốn đầu tư nước ngoài (FDI), doanh nghiệp sử dụng các nền tảng quản trị nhân sự trên môi trường số, đây không đơn thuần là một quy định pháp lý mới mà là yêu cầu phải thay đổi cách thức quản trị nhân sự. Việc bảo vệ dữ liệu cá nhân không còn là trách nhiệm riêng của bộ phận pháp chế hay công nghệ thông tin mà đã trở thành một nội dung của quản trị doanh nghiệp, tác động trực tiếp đến chi phí vận hành, khả năng kiểm soát rủi ro và năng lực cạnh tranh.

Doanh nghiệp phải thay đổi cách quản trị dữ liệu nhân sự

Một trong những điểm mới đáng chú ý của Luật Bảo vệ dữ liệu cá nhân là dành Điều 25 để quy định riêng về việc xử lý dữ liệu cá nhân trong tuyển dụng và quản lý người lao động. Theo đó, doanh nghiệp chỉ được yêu cầu ứng viên cung cấp những thông tin cần thiết cho mục đích tuyển dụng; dữ liệu chỉ được sử dụng đúng mục đích đã thông báo và phải được xóa, hủy khi không còn căn cứ để tiếp tục lưu giữ.

So với trước đây, phạm vi điều chỉnh đã được mở rộng đáng kể. Nghị định số 356/2025/NĐ-CP cũng xác định dữ liệu cá nhân trong quan hệ lao động không chỉ bao gồm thông tin nhận dạng cơ bản mà còn có nhiều loại dữ liệu nhạy cảm như dữ liệu sức khỏe, dữ liệu sinh trắc học, dữ liệu định danh điện tử, dữ liệu phản ánh hoạt động trên môi trường số.

Khung pháp lý mới cũng điều chỉnh nhiều hoạt động vốn đang diễn ra phổ biến tại doanh nghiệp như sử dụng camera giám sát, phần mềm quản lý công việc, thiết bị định vị GPS, hệ thống chấm công bằng sinh trắc học hay chuyển dữ liệu nhân sự sang hệ thống quản trị của công ty mẹ ở nước ngoài.

Có thể thấy, pháp luật không hạn chế quyền quản lý của doanh nghiệp nhưng yêu cầu mọi hoạt động xử lý dữ liệu phải có căn cứ pháp lý, minh bạch về mục đích, phạm vi và thời gian lưu giữ. Đây là thay đổi lớn trong tư duy quản trị nhân sự, đòi hỏi doanh nghiệp phải coi dữ liệu cá nhân là một nội dung của quản trị rủi ro thay vì chỉ là công cụ phục vụ điều hành.

Những rủi ro doanh nghiệp cần nhận diện sớm

Mặc dù khung pháp lý đã tương đối đầy đủ, việc triển khai trên thực tế sẽ đặt ra không ít thách thức cho doanh nghiệp. Thực tiễn tư vấn cho thấy, phần lớn rủi ro hiện nay không xuất phát từ việc doanh nghiệp cố tình vi phạm mà đến từ việc chưa nhận diện đầy đủ nghĩa vụ pháp lý.

Một trong những vấn đề phổ biến là chuyển dữ liệu nhân sự xuyên biên giới. Nhiều doanh nghiệp FDI hoặc doanh nghiệp thành viên của các tập đoàn đa quốc gia sử dụng hệ thống quản trị nhân sự tập trung, trong đó dữ liệu của người lao động tại Việt Nam được đồng bộ lên máy chủ của công ty mẹ hoặc lưu trữ trên các nền tảng điện toán đám mây quốc tế.

Luật Bảo vệ dữ liệu cá nhân và Nghị định số 356/2025/NĐ-CP đã có những quy định miễn trừ nhất định đối với hoạt động quản lý nhân sự, chẳng hạn trường hợp lưu trữ dữ liệu của chính người lao động trên dịch vụ điện toán đám mây hoặc việc chuyển dữ liệu phục vụ quản lý nhân sự theo quy chế, nội quy lao động hoặc thỏa ước lao động tập thể hợp pháp. Tuy nhiên, doanh nghiệp cần xác định chính xác từng trường hợp để áp dụng đúng quy định, tránh nhầm lẫn giữa trường hợp được miễn và trường hợp vẫn phải thực hiện các nghĩa vụ theo luật.

Một rủi ro khác là sử dụng dữ liệu vượt quá mục đích thu thập ban đầu. Chẳng hạn, kết quả khám sức khỏe định kỳ được thu thập nhằm đáp ứng yêu cầu của pháp luật lao động, nhưng sau đó lại được sử dụng để đánh giá năng lực hoặc cơ hội thăng tiến của người lao động. Việc mở rộng mục đích sử dụng như vậy có thể không còn phù hợp với nguyên tắc xử lý dữ liệu theo Luật Bảo vệ dữ liệu cá nhân.

Bên cạnh đó, nhiều doanh nghiệp hiện vẫn chưa thiết lập cơ chế để người lao động thực hiện các quyền của chủ thể dữ liệu như quyền được biết, quyền truy cập, chỉnh sửa, xóa dữ liệu hoặc phản đối việc xử lý dữ liệu. Thiếu quy trình nội bộ và đầu mối tiếp nhận yêu cầu có thể khiến doanh nghiệp vi phạm thời hạn xử lý theo quy định của pháp luật.

Sau khi quan hệ lao động chấm dứt, doanh nghiệp cũng phải đối mặt với bài toán cân bằng giữa nghĩa vụ xóa dữ liệu và nhu cầu lưu giữ hồ sơ để giải quyết tranh chấp, nghĩa vụ thuế, bảo hiểm xã hội hoặc các

yêu cầu của pháp luật chuyên ngành. Vì vậy, việc xây dựng chính sách lưu trữ dữ liệu theo từng nhóm hồ sơ và từng căn cứ pháp lý sẽ giúp doanh nghiệp hạn chế đáng kể rủi ro.

Chủ động tuân thủ để nâng cao năng lực cạnh tranh

Bên cạnh việc đặt ra các nghĩa vụ mới, Luật Bảo vệ dữ liệu cá nhân cũng quy định chế tài khá nghiêm khắc. Theo Điều 8, tổ chức có hành vi vi phạm có thể bị xử phạt đến 10 lần khoản thu bất hợp pháp đối với hành vi mua, bán dữ liệu cá nhân; 5% doanh thu năm liền kề đối với vi phạm về chuyển dữ liệu xuyên biên giới và 3 tỷ đồng đối với nhiều hành vi vi phạm khác. Ngoài việc xử phạt hành chính, doanh nghiệp còn có thể phải bồi thường thiệt hại nếu việc xử lý dữ liệu trái pháp luật gây ảnh hưởng đến quyền và lợi ích hợp pháp của người lao động.

Trong bối cảnh đó, doanh nghiệp cần chuyển từ tư duy "khắc phục khi có vi phạm" sang chủ động xây dựng hệ thống quản trị dữ liệu cá nhân.

Trước hết, doanh nghiệp nên tiến hành rà soát toàn bộ dữ liệu đang thu thập và xử lý, lập bản đồ dữ liệu (data mapping), xác định rõ mục đích sử dụng, thời hạn lưu giữ và căn cứ pháp lý đối với từng nhóm dữ liệu. Đây là nền tảng để doanh nghiệp kiểm soát rủi ro và đáp ứng yêu cầu của cơ quan quản lý khi cần thiết.

Tiếp theo, cần rà soát, sửa đổi các tài liệu nội bộ như hợp đồng lao động, nội quy lao động, quy chế quản lý dữ liệu, quy trình tuyển dụng và các biểu mẫu thu thập thông tin để bảo đảm phù hợp với Luật Bảo vệ dữ liệu cá nhân và Nghị định số 356/2025/NĐ-CP.

Doanh nghiệp cũng cần xây dựng cơ chế phối hợp giữa bộ phận nhân sự, pháp chế và công nghệ thông tin; bổ nhiệm nhân sự hoặc bộ phận phụ trách bảo vệ dữ liệu đáp ứng điều kiện theo quy định; đồng thời tổ chức đào tạo định kỳ nhằm nâng cao nhận thức của người lao động về bảo vệ dữ liệu cá nhân.

Quan trọng hơn, doanh nghiệp nên xem việc tuân thủ không chỉ là yêu cầu pháp lý mà còn là một yếu tố của quản trị hiện đại. Trong bối cảnh các nhà đầu tư, đối tác và khách hàng ngày càng coi trọng tiêu chuẩn quản trị doanh nghiệp, năng lực bảo vệ dữ liệu cá nhân sẽ góp phần nâng cao uy tín, giảm rủi ro và tăng khả năng cạnh tranh.

() Luật sư cấp cao, Văn phòng Luật sư NHQuang & Cộng sự*

 Chia sẻ Facebook

 Theo dõi trên Google News

 Chia sẻ Zalo



-  Bảo vệ dữ liệu
- Quan hệ lao động
- Quản trị nhân sự
- Doanh nghiệp
- Dữ liệu cá nhân
- Quản trị rủi ro
- Dữ liệu nhân sự

BÀI LIÊN QUAN