

Bảng kiểm thực hành về bảo vệ dữ liệu cá nhân dành cho doanh nghiệp tại Việt Nam

Pháp luật được rà soát đến ngày 24/10/2026.

Đối tượng sử dụng hướng dẫn

Hướng dẫn này dành cho đội ngũ quản lý, pháp chế, nhân sự, tiếp thị và công nghệ thông tin đang rà soát việc xử lý dữ liệu cá nhân trong hoạt động kinh doanh thông thường tại Việt Nam. Tài liệu cung cấp điểm khởi đầu thực tiễn theo Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15 ngày 26/6/2025 và Nghị định số 356/2025/NĐ-CP ngày 31/12/2025, cùng có hiệu lực từ ngày 01/01/2026. Đây không phải cẩm nang tuân thủ riêng cho từng ngành hoặc chứng nhận tuân thủ. Nghị định 356 thay thế Nghị định số 13/2023/NĐ-CP từ ngày đó. [1-2]

Các bước dưới đây phân biệt vấn đề pháp luật quy định với biện pháp triển khai được khuyến nghị. Nghĩa vụ của doanh nghiệp phụ thuộc vào hoạt động, vai trò, dữ liệu và ngoại lệ áp dụng. Chỉ riêng việc có website tiếng Anh hoặc khách hàng ở nước ngoài chưa đủ để xác định GDPR áp dụng. Việc phân tích pháp luật nước ngoài cần được thực hiện riêng khi đáp ứng các quy tắc về phạm vi lãnh thổ hoặc căn cứ áp dụng khác của pháp luật đó.

Mục lục

- Xác định dữ liệu và hoạt động xử lý
- Xác định vai trò của doanh nghiệp và căn cứ xử lý hợp pháp
- Triển khai cơ chế đồng ý và thông tin thu thập phù hợp thực tế
- Rà soát nhà cung cấp, bên nhận và việc xử lý ở nước ngoài
- Đánh giá yêu cầu về hồ sơ đánh giá tác động và nhân sự
- Xây dựng quy trình thực hiện quyền của chủ thể dữ liệu
- Thiết lập quy trình lưu giữ, bảo vệ và xử lý sự cố
- Sử dụng bảng kiểm triển khai
- Các bước thực hành dành cho doanh nghiệp
- Căn cứ pháp luật và nguồn tham khảo

1. Xác định dữ liệu và hoạt động xử lý

Vấn đề pháp lý. Phạm vi Luật không chỉ giới hạn ở cơ sở dữ liệu khách hàng. Các định nghĩa của Luật bao gồm thu thập, phân tích, mã hóa, chỉnh sửa, xóa, công khai, chuyển giao và các hoạt động xử lý khác. Điều 3 yêu cầu xử lý trong phạm vi và mục đích cụ thể, rõ ràng, bảo đảm phù hợp về tính chính xác, lưu giữ và biện pháp bảo vệ. Điều 3-4 Nghị định 356 phân biệt dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm. [1-2]

Khuyến nghị triển khai. Nên bắt đầu từ quy trình hoạt động, không phải tên phần mềm. Rà soát tuyển dụng, tiền lương, yêu cầu của khách hàng, đầu mối nhà cung cấp, kiểm soát ra vào, bản tin và tương tác trên website. Với từng quy trình, xác định người có dữ liệu được xử lý, dữ liệu thu thập, nguồn, mục đích, hệ thống, người sử dụng và bên nhận. Làm rõ vì sao cần từng trường thông tin. Không nên bỏ qua tên và email có thể xác định cá nhân của một đầu mối công việc chỉ vì đây là quan hệ giữa các doanh nghiệp.

Cần tách việc phân loại dữ liệu khỏi đánh giá của doanh nghiệp về tầm quan trọng thương mại. Chẳng hạn, thông tin sức khỏe trong hồ sơ nhân sự cần được đánh giá về tính chất dữ liệu nhạy cảm. Công nghệ trên website cũng cần được xem xét theo dữ liệu thực sự thu thập và truyền đi. Việc có cài một plugin cụ thể không thay thế đáng tin cậy cho kiểm kê kỹ thuật.

2. Xác định vai trò của doanh nghiệp và căn cứ xử lý hợp pháp

Vấn đề pháp lý. Điều 2 phân biệt bên kiểm soát dữ liệu cá nhân, bên xử lý dữ liệu cá nhân và bên kiểm soát và xử lý dữ liệu cá nhân. Điều 9 quy định về sự đồng ý; Điều 19 xác định các trường hợp được xử lý không cần sự đồng ý, có tính đến điều kiện và biện pháp bảo đảm áp dụng. Cần đánh giá theo chính quy định pháp luật Việt Nam, không đưa một căn cứ chung về “lợi ích hợp pháp” từ hệ thống pháp luật khác vào áp dụng. [1]

Khuyến nghị triển khai. Với mỗi quy trình, ghi nhận ai quyết định mục đích, phương tiện xử lý và ai thực hiện theo chỉ dẫn. Kiểm tra căn cứ dự kiến cho việc thu thập, sử dụng và công khai dữ liệu. Tên gọi vai trò của nhà cung cấp trong hợp đồng cần được đối chiếu với hoạt động thực tế. Một tổ chức có thể có các vai trò khác nhau trong từng quy trình.

Khi dựa vào trường hợp không cần sự đồng ý theo luật, cần xác định điều khoản liên quan và giải thích vì sao tình tiết thực tế đáp ứng quy định. Lưu nhận định này trong hồ sơ nội bộ. Khi cần sự đồng ý, thiết kế quy trình thu thập để lấy và chứng minh sự đồng ý đó. Chính sách bảo vệ dữ liệu cá nhân nên mô tả hoạt động xử lý thực tế; việc đăng chính sách tự nó không tạo căn cứ hợp pháp cho mọi hoạt động của doanh nghiệp.

3. Triển khai cơ chế đồng ý và thông tin thu thập phù hợp thực tế

Vấn đề pháp lý. Điều 9 yêu cầu sự đồng ý phải tự nguyện, được đưa ra khi biết rõ thông tin, rõ ràng và kiểm chứng được; thể hiện theo từng mục đích, không coi im lặng là đồng ý. Điều này hạn chế việc bắt buộc đồng ý với các mục đích không liên quan như một điều kiện. Điều 11 quy định về sự đồng ý trước khi thu thập, trừ trường hợp luật quy định khác. Điều 6 Nghị định 356 yêu cầu chứng cứ xác định chủ thể, thời điểm và nội dung đồng ý, cấm cơ chế mặc định đồng ý và yêu cầu thông báo về dữ liệu nhạy cảm khi thuộc trường hợp áp dụng. [1-2]

Khuyến nghị triển khai. Cần phân biệt trả lời yêu cầu liên hệ với việc đưa người gửi vào danh sách tiếp thị. Lựa chọn đăng ký bản tin không bắt buộc nên được giải thích riêng với mục đích trực tiếp của biểu mẫu liên hệ. Lưu phiên bản nội dung xin ý kiến cùng hồ sơ đồng ý liên quan để doanh nghiệp chứng minh được chủ thể đã đồng ý điều gì tại thời điểm đó.

Rà soát giao diện thực tế, không chỉ các đường dẫn chính sách. Kiểm tra trường bắt buộc và tùy chọn có dễ hiểu hay không, hệ thống có ghi nhận đúng lựa chọn không. Không mô tả đường dẫn rút lại đồng ý, trang quản lý tùy chọn hoặc nút từ chối cookie nếu cơ chế đó chưa tồn tại và hoạt động được. Email xác nhận có thể hỗ trợ chứng minh đăng ký, nhưng hướng dẫn này không coi cơ chế xác nhận đăng ký hai bước là yêu cầu pháp luật bắt buộc trong mọi trường hợp.

4. Rà soát nhà cung cấp, bên nhận và việc xử lý ở nước ngoài

Vấn đề pháp lý. Hoạt động chia sẻ và các thỏa thuận xử lý dữ liệu cần được đánh giá theo Điều 17–20. Các trường hợp chuyển dữ liệu xuyên biên giới tại Điều 20 bao gồm những trường hợp lưu trữ ở nước ngoài theo quy định, chuyển dữ liệu cho tổ chức hoặc cá nhân ở nước ngoài và sử dụng nền tảng ở nước ngoài để xử lý dữ liệu thu thập tại Việt Nam. Điều này quy định yêu cầu đánh giá tác động và các ngoại lệ, trong đó có ngoại lệ cụ thể đối với việc tổ chức lưu trữ dữ liệu của chính người lao động thuộc tổ chức trên dịch vụ điện toán đám mây. Không nên tự động mở rộng ngoại lệ đó sang hoạt động xử lý dữ liệu khách hàng hoặc tiếp thị không liên quan. [1]

Khuyến nghị triển khai. Hỏi nhà cung cấp về nơi đặt dữ liệu vận hành chính, bản sao lưu và nơi thực hiện truy cập hỗ trợ. Xác định chủ thể giao kết hợp đồng và nhà thầu phụ có liên quan. Rà soát hosting, email doanh nghiệp, dịch vụ tiền lương, hệ thống quản lý khách hàng, bản đồ nhúng, công cụ phân tích và chống spam khi thực tế có sử dụng.

Tên thương hiệu nước ngoài chưa trả lời được mọi vấn đề chuyển dữ liệu; tương tự, nhà cung cấp xuất hóa đơn trong nước không chứng minh toàn bộ xử lý diễn ra tại Việt Nam. Cần ghi nhận luồng dữ liệu thực tế và đánh giá yêu cầu áp dụng. Hợp đồng nhà cung cấp nên điều chỉnh chỉ dẫn xử lý, mục đích được phép, bảo vệ dữ liệu, bên nhận tiếp theo, hỗ trợ thực hiện quyền, báo cáo và chuyển xử lý sự cố, xóa hoặc hoàn trả khi phù hợp. Đánh giá yêu cầu áp dụng đối với thỏa thuận chuyển giao theo Điều 7 Nghị định 356. [2]

5. Đánh giá yêu cầu về hồ sơ đánh giá tác động và nhân sự

Vấn đề pháp lý. Điều 20–22 điều chỉnh đánh giá tác động chuyển dữ liệu xuyên biên giới, đánh giá tác động xử lý và việc cập nhật. Điều 21 phân biệt nghĩa vụ của bên kiểm soát với bên xử lý. Điều 38–39 của Luật và Điều 41 Nghị định 356 quy định ngoại lệ, chuyển tiếp cụ thể. Việc miễn hoặc cho phép lựa chọn không thực hiện một số yêu cầu đối với doanh nghiệp nhỏ, khởi nghiệp hoặc siêu nhỏ nhất định không phải miễn chung nghĩa vụ theo pháp luật bảo vệ dữ liệu cá nhân. Việc xử lý dữ liệu nhạy cảm, cung cấp dịch vụ xử lý dữ liệu hoặc đặt quy mô luật định có thể ảnh hưởng điều kiện áp dụng. [1–2]

Khuyến nghị triển khai. Xác định có phải lập hồ sơ đánh giá tác động hay không, ai lập và duy trì, sự kiện bắt đầu tính thời hạn và thời hạn nộp áp dụng, cách theo dõi thay đổi. Kiểm tra cơ sở áp dụng miễn trừ hoặc cơ chế lựa chọn dựa trên hoạt động và tiêu chí quy mô thực tế. Không nên cho rằng số lao động ít là đủ điều kiện.

Rà soát yêu cầu áp dụng đối với nhân sự hoặc bộ phận phụ trách và năng lực cần thiết của bên cung cấp dịch vụ bên ngoài. Duy trì trách nhiệm giải trình rõ ràng trong doanh nghiệp ngay cả khi thuê ngoài. Nếu đã có hồ sơ hoặc sự đồng ý từ trước, cần xem xét Điều 39, thay vì mặc định phải làm lại toàn bộ hoặc mọi thỏa thuận trước đây đều được tiếp tục mà không thay đổi. [1]

Thay đổi thủ tục sắp có hiệu lực. Nghị định số 392/2026/NĐ-CP được ban hành ngày 20/10/2026 và có hiệu lực ngày 15/11/2026. Điều 42–47 sửa đổi một số thủ tục tại Nghị định 356. Các sửa đổi này không được áp dụng như yêu cầu đang có hiệu lực trong hướng dẫn; cần kiểm tra lại thủ tục nộp và đánh giá hồ sơ trước khi sử dụng tài liệu từ ngày đó. [3]

6. Xây dựng quy trình thực hiện quyền của chủ thể dữ liệu

Vấn đề pháp lý. Điều 4 xác định các quyền của chủ thể dữ liệu. Điều 5 Nghị định 356 yêu cầu quy trình rõ ràng và quy định các thời hạn phản hồi, thực hiện khác nhau đối với từng yêu cầu. Chẳng hạn, yêu cầu rút lại đồng ý, hạn chế hoặc phản đối xử lý đáp ứng điều kiện có thời hạn phản hồi là hai ngày làm việc và thời hạn thực hiện thông thường là 15 ngày, có tính đến các điều kiện, bao gồm trường hợp liên quan bên xử lý hoặc bên thứ ba và việc gia hạn được phép. Không thể thay quy định này bằng một thời hạn duy nhất áp dụng chung một cách an toàn. [1-2]

Khuyến nghị triển khai. Thiết lập đầu mối được theo dõi thường xuyên, sổ tiếp nhận, quy trình kiểm tra danh tính tương xứng với yêu cầu và cơ chế chuyển cấp xử lý. Ghi nhận loại yêu cầu, thời điểm tiếp nhận, xác minh, đánh giá pháp lý, thời hạn áp dụng, bộ phận chịu trách nhiệm và kết quả. Không nên thường xuyên thu toàn bộ bản sao giấy tờ định danh nếu phương thức ít xâm phạm hơn có thể xác minh được danh tính.

Thử quy trình bằng tình huống thực tế: một người từng đăng ký bản tin yêu cầu rút lại đồng ý tiếp thị và xóa dữ liệu. Bộ phận phụ trách cần phân biệt đừng gửi bản tin trong tương lai với việc xác định hồ sơ khác có lý do lưu giữ hợp pháp hay không. Theo Điều 10, rút lại đồng ý không làm mất hiệu lực hồi tố của việc xử lý trước đó. Phản hồi cần giải thích kết quả thực tế và giới hạn hợp pháp, không hứa xóa ngay trên mọi hệ thống. [1]

7. Thiết lập quy trình lưu giữ, bảo vệ và xử lý sự cố

Vấn đề pháp lý. Điều 3 gắn việc lưu giữ với thời gian phù hợp mục đích xử lý, trừ trường hợp pháp luật quy định khác. Điều 23 yêu cầu thông báo những vi phạm có khả năng gây tổn hại theo trường hợp được quy định chậm nhất 72 giờ kể từ khi phát hiện; đồng thời yêu cầu bên xử lý thông báo kịp thời cho bên kiểm soát có liên quan. Không nên giản lược thành khẳng định mọi sự kiện kỹ thuật đều có cùng nghĩa vụ báo cáo. [1]

Khuyến nghị triển khai. Ban hành lịch lưu giữ theo loại hồ sơ, nêu lý do, mốc bắt đầu tính, người chịu trách nhiệm và cách xóa. Phân biệt nghĩa vụ lưu hồ sơ theo luật với mong muốn lưu thông tin vì lý do kinh doanh. Xử lý bản sao lưu và yêu cầu tạm ngừng xóa để phục vụ vấn đề pháp lý theo cách hệ thống thực sự thực hiện được.

Lựa chọn biện pháp kiểm soát tương ứng với rủi ro: phân quyền truy cập, quản lý tài khoản, bảo vệ thiết bị, chia sẻ an toàn và phương án khôi phục là các nội dung hữu ích để rà soát. Tránh cam kết công khai về an toàn tuyệt đối. Đối với sự cố, quy định thời gian báo cáo, chuyển xử lý nội bộ đủ ngắn để đánh giá và thực hiện thông báo ra bên ngoài khi cần trong thời hạn áp dụng. Lưu lại thời điểm phát hiện, dữ liệu bị ảnh hưởng, hậu quả có thể xảy ra, biện pháp kiểm soát và quyết định báo cáo.

8. Bảng kiểm triển khai

Các tài liệu chứng minh được đề xuất dưới đây là công cụ thực hành; không phải tất cả đều là tài liệu có tên gọi bắt buộc theo pháp luật. Mỗi mục nên được hoàn tất, xác định không áp dụng kèm lý do hoặc phân công người phụ trách khắc phục.

Nội dung rà soát	Tài liệu, chứng cứ cần chuẩn bị	Tính chất
Mục đích và dữ liệu	Danh mục quy trình, trường thông tin cần thiết, phân loại dữ liệu cơ bản/nhạy cảm	Triển khai Điều 2-3 của Luật và Điều 3-4 Nghị định 356

Nội dung rà soát	Tài liệu, chứng cứ cần chuẩn bị	Tính chất
Vai trò và căn cứ xử lý	Đánh giá vai trò và phân tích sự đồng ý hoặc ngoại lệ luật định	Đánh giá pháp lý theo Điều 2, 9 và 19
Thu thập và sự đồng ý	Nội dung thông tin khi thu thập, kiểm tra giao diện và chứng cứ về sự đồng ý khi cần	Yêu cầu pháp luật; hình thức phụ thuộc quy trình
Nhà cung cấp và bên nhận	Sơ đồ luồng dữ liệu thực tế, trả lời của nhà cung cấp và thỏa thuận liên quan	Đánh giá pháp lý cùng tài liệu chứng minh được khuyến nghị
Xử lý ở nước ngoài	Kết quả xác minh vị trí lưu trữ, truy cập; đánh giá tác động áp dụng hoặc hồ sơ về ngoại lệ	Đánh giá pháp lý theo Điều 20
Hồ sơ đánh giá tác động và nhân sự	Quyết định về phạm vi áp dụng, hồ sơ hiện hành, sổ cập nhật và người chịu trách nhiệm	Yêu cầu pháp luật áp dụng; không có miễn trừ chung cho mọi doanh nghiệp nhỏ và vừa
Yêu cầu thực hiện quyền	Đầu mối được theo dõi, sổ yêu cầu và bảng thời hạn theo từng loại	Triển khai Điều 4 của Luật và Điều 5 Nghị định 356
Lưu giữ và bảo vệ	Lịch theo loại hồ sơ, rà soát quyền truy cập và chứng cứ xóa	Nguyên tắc pháp luật được hỗ trợ bằng biện pháp vận hành
Sự cố	Quy trình báo cáo, chuyển xử lý, ghi nhận phát hiện và đánh giá nghĩa vụ báo cáo	Điều 23 cùng các biện pháp chuẩn bị được khuyến nghị

9. Các bước thực hành dành cho doanh nghiệp

Lựa chọn một quy trình có mức độ rủi ro đáng kể và rà soát trọn vẹn từ thu thập đến xóa dữ liệu trước khi viết lại toàn bộ tài liệu. Dựa trên kết quả để thống nhất thông báo, quy trình xin đồng ý, hợp đồng nhà cung cấp và hướng dẫn nội bộ. Mở rộng sang quy trình khác với cùng tiêu chuẩn chứng minh.

Xác định ngày rà soát của cấp quản lý và theo dõi thay đổi quan trọng, bao gồm phần mềm mới, bên nhận ở nước ngoài khác hoặc cách sử dụng mới đối với dữ liệu hiện có. Kiểm tra lại pháp luật trước khi dựa vào ngoại lệ hoặc nộp hồ sơ đánh giá tác động. Quy trình đã được thực hiện và có người phụ trách rõ ràng tạo nền tảng tuân thủ hữu ích hơn một chính sách mô tả các biện pháp doanh nghiệp chưa áp dụng.

10. Căn cứ pháp luật và nguồn tham khảo

Tất cả nguồn được truy cập ngày **24/10/2026**. Tên gọi, mô tả văn bản bằng tiếng Anh trong bản gốc nhằm giải thích và không được giới thiệu là bản dịch chính thức.

1. **Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15 ngày 26/6/2025**, có hiệu lực ngày 01/01/2026; **văn bản tiếng Việt đã ký**. Các quy định liên quan: Điều 2-4, 9-11, 17-23 và 38-39.
2. **Nghị định số 356/2025/NĐ-CP ngày 31/12/2025, bản đăng Công báo chính thức**, có hiệu lực ngày 01/01/2026. Các quy định liên quan: Điều 3-7, 13-16, 41-42 và thủ tục, biểu mẫu đánh giá tác động áp dụng. Điều 42 quy định Nghị định 13/2023 hết hiệu lực từ ngày 01/01/2026.
3. **Nghị định số 392/2026/NĐ-CP ngày 20/10/2026**, Điều 42-48; **văn bản ký**, đặc biệt trang 31-34. Có hiệu lực ngày 15/11/2026; đã ban hành nhưng chưa có hiệu lực tại ngày chốt nghiên cứu.

Nội dung này cung cấp thông tin pháp lý chung trên cơ sở các nguồn được rà soát đến ngày 24/10/2026, không phải ý kiến tư vấn pháp lý cho một vụ việc cụ thể. Việc áp dụng pháp luật Việt Nam phụ thuộc vào các tình tiết và hoàn cảnh liên quan.