

BẢO VỆ DỮ LIỆU CÁ NHÂN THEO QUY ĐỊNH PHÁP LUẬT

Nhận diện nghĩa vụ. Kiểm soát rủi ro. củng cố niềm tin.



TUÂN THỦ QUY ĐỊNH PHÁP LUẬT VỀ DỮ LIỆU CÁ NHÂN

Luật Bảo vệ dữ liệu cá nhân 91/2025/QH15 hiệu lực từ 01/01/2026.
Nghị định 330/2026/NĐ-CP xử lý vi phạm từ 19/8/2026,

Doanh nghiệp nào phải tuân thủ?

Chỉ cần **MỘT** dấu hiệu dưới đây là doanh nghiệp đang xử lý dữ liệu cá nhân và đã thuộc phạm vi Luật 91/2025/QH15.

	Có người lao động hoặc ứng viên · Hồ sơ nhân sự, bảng lương, bảo hiểm, CCCD	☐
	Có khách hàng là cá nhân · Tên, số điện thoại, email, địa chỉ giao hàng	☐
	Lắp camera hoặc chấm công sinh trắc học · Vân tay, khuôn mặt là dữ liệu nhạy cảm	☐
	Dùng đám mây, email, phần mềm hoặc AI · Đặc biệt khi máy chủ đặt ở nước ngoài	☐
	Gửi dữ liệu cho đối tác · Kế toán, ngân hàng, bảo hiểm, logistics, đại lý	☐

Ai phải làm gì?

Loại doanh nghiệp	Nghĩa vụ cốt lõi*	Hồ sơ DPIA, cập nhật hồ sơ, nhân sự bảo vệ dữ liệu
Doanh nghiệp vừa, lớn, FDI	Bắt buộc	Bắt buộc
Bất kỳ quy mô nào nếu: xử lý dữ liệu nhạy cảm, hoặc từ 100.000 người trở lên, hoặc kinh doanh dịch vụ xử lý dữ liệu	Bắt buộc	Bắt buộc, không được miễn
Doanh nghiệp nhỏ, khởi nghiệp	Bắt buộc	Được tự chọn đến 01/01/2031
Hộ kinh doanh, doanh nghiệp siêu nhỏ	Bắt buộc	Không phải thực hiện

*Nghĩa vụ cốt lõi: xin sự đồng ý, bảo đảm quyền của người có dữ liệu, biện pháp bảo vệ, thông báo vi phạm trong 72 giờ.

01/01/2026

Luật 91 và Nghị định 356 có hiệu lực

19/8/2026

Bắt đầu xử phạt theo Nghị định 330

3 tỷ đồng

Mức phạt tối đa thông thường với tổ chức (≈ 115.000 USD)

Nguồn: Luật 91/2025/QH15 Đ1, Đ8, Đ38; ND 356/2025/ND-CP Đ4, Đ41; ND 330/2026/ND-CP Đ7, Đ80. Tỷ giá 26.100 đ/USD.

Ba điều lãnh đạo cần biết

Bảo vệ dữ liệu cá nhân đã là nghĩa vụ có chế tài, và doanh nghiệp phải chứng minh được mình đã làm.

1

Dữ liệu ở khắp nơi

Hồ sơ nhân viên, khách hàng, camera, chấm công đều là dữ liệu cá nhân. Dữ liệu đã mã hóa vẫn là dữ liệu cá nhân.

Luật 91 Đ2, Đ12.1

2

Là bài toán vận hành

Luật đòi hỏi biện pháp đồng bộ về thể chế, kỹ thuật và con người, không chỉ việc của pháp chế.

Luật 91 Đ3.4

3

Phải có bằng chứng

Hồ sơ DPIA, nhật ký đồng ý, thông báo vi phạm 72 giờ. Khi tranh chấp, doanh nghiệp là bên phải chứng minh.

Luật 91 Đ21, Đ23; NĐ 356 Đ6.2

Sự cố dữ liệu tác động đến bốn mặt của doanh nghiệp



Khách hàng & người lao động

Có quyền yêu cầu xem, sửa, xóa, hạn chế xử lý, khiếu nại, khởi kiện và đòi bồi thường (Luật 91 Đ4).



Vận hành

Kiểm tra đột xuất không báo trước; có thể bị buộc dừng xử lý dữ liệu cho đến khi nộp đủ hồ sơ (NĐ 356 Đ31; NĐ 330 Đ55).



Tài chính

Phạt tối đa 3 tỷ đồng, 5% doanh thu (chuyển dữ liệu ra nước ngoài) hoặc 10 lần khoản thu (mua bán dữ liệu), cộng bồi thường (Luật 91 Đ8).



Cơ hội kinh doanh

Hợp đồng chuyển giao dữ liệu, hợp đồng đám mây bắt buộc có điều khoản bảo vệ dữ liệu (NĐ 356 Đ7, Đ12).

+17,5 tỷ đồng
(≈ 670.000 USD)

Chi phí trung bình tăng thêm của một vụ rò rỉ khi doanh nghiệp có mức độ cao AI dùng ngoài kiểm soát (shadow AI). 1/5 tổ chức được khảo sát báo cáo sự cố liên quan đến shadow AI.

Đọc nhanh theo vai trò: CEO tr. 2–3, 10, 15 · Pháp chế tr. 5–10 · Nhân sự tr. 4, 8, 9 · CNTT tr. 7, 11–14 · Chất lượng, kiểm soát nội bộ tr. 8, 9, 12, 15

Nguồn: IBM, Cost of a Data Breach Report 2025 (quy đổi 26.100 đ/USD); Luật 91/2025/QH15; NĐ 356/2025; NĐ 330/2026.

Rủi ro trong công việc hằng ngày

Không cần hacker. Một thao tác quen thuộc cũng có thể tạo ra nghĩa vụ pháp lý.

TÌNH HUỐNG MINH HỌA



Gửi bảng lương cho đối tác

Dữ liệu: Họ tên, lương, số tài khoản, bảo hiểm

Rủi ro

Tệp Excel gửi email không bảo vệ, bị chuyển tiếp hoặc đối tác giữ quá hạn; chưa có thỏa thuận xử lý dữ liệu.

Câu hỏi cần giải quyết

Đối tác có phải bên xử lý, đã có hợp đồng chưa (Luật 91 Đ37.2)? Tệp có được bảo vệ khi chuyển giao (NĐ 356 Đ7)? Ai xóa sau khi xong việc?



Tải hồ sơ khách hàng lên công cụ AI

Dữ liệu: Hợp đồng, CCCD, lịch sử giao dịch

Rủi ro

Nền tảng ở nước ngoài có thể làm phát sinh chuyển dữ liệu xuyên biên giới; dùng ngoài mục đích đã thông báo; nhà cung cấp lưu giữ dữ liệu.

Câu hỏi cần giải quyết

Công cụ nào được phê duyệt? Dữ liệu đã khử nhận dạng chưa? Có phải lập hồ sơ chuyển dữ liệu ra nước ngoài (Luật 91 Đ20)?



Chấm công bằng vân tay, khuôn mặt

Dữ liệu: Dữ liệu sinh trắc học (nhạy cảm)

Rủi ro

Chưa thông báo đây là dữ liệu nhạy cảm; thiết bị hoặc đám mây của nhà cung cấp bị lộ; dùng sang mục đích khác.

Câu hỏi cần giải quyết

Người lao động đã biết rõ biện pháp này (Luật 91 Đ25.3)? Có bảo mật vật lý, hạn chế truy cập (Đ31.4)? Có quy trình báo sự cố trong 72 giờ (NĐ 356 Đ29)?

Rủi ro dữ liệu không chỉ bắt đầu từ một cuộc tấn công. Nó có thể xuất hiện khi doanh nghiệp thu thập quá nhiều, chia sẻ thiếu kiểm soát hoặc không biết dữ liệu đang được xử lý ở đâu.

Nghĩa vụ theo ngành và quy mô

Luật áp dụng cho mọi tổ chức. Miễn trừ chỉ áp dụng cho 3 nghĩa vụ hồ sơ và nhân sự, không phải miễn toàn bộ.

Ngành	Hoạt động điển hình	Loại dữ liệu	Bộ phận phụ trách
Sản xuất / FDI	Tuyển dụng, chấm công, camera, bảng lương	Nhân thân, sinh trắc học, tài khoản	Nhân sự, Hành chính, CNTT
Bán lẻ / TMĐT	Khách hàng thân thiết, giao hàng, quảng cáo	Liên hệ, hành vi mua sắm, vị trí	Marketing, CSKH
Tài chính, ngân hàng, bảo hiểm	Tín dụng, thanh toán, thẩm định	Tài chính, tín dụng (nhạy cảm)	Tuân thủ, Rủi ro
Y tế	Khám chữa bệnh, bảo hiểm sức khỏe	Sức khỏe (nhạy cảm)	Hồ sơ y tế, CNTT
Giáo dục	Tuyển sinh, học bạ, camera lớp học	Dữ liệu trẻ em	Đào tạo, Hành chính
Công nghệ / Outsourcing	Vận hành hệ thống thay khách hàng	Dữ liệu của khách hàng	Pháp chế, CTO
Logistics / Du lịch	Vận chuyển, đặt phòng, thị thực	Hộ chiếu, vị trí, dữ liệu ra nước ngoài	Vận hành, Pháp chế

Dữ liệu cá nhân nhạy cảm gồm những gì?

Sức khỏe	Sinh trắc học, di truyền	Tài khoản, giao dịch ngân hàng, tín dụng
Vị trí qua dịch vụ định vị	Hình ảnh CCCD, mặt khẩu tài khoản định danh	Đời sống riêng tư, bí mật gia đình
Quan điểm chính trị, tôn giáo	Nguồn gốc chủng tộc, dân tộc	Hành vi trên mạng xã hội, dịch vụ trực tuyến

Lưu ý theo ngành
Tài chính, ngân hàng: đánh giá tuân thủ 1 năm/lần, ghi nhật ký toàn bộ hoạt động xử lý, báo sự cố dữ liệu nhạy cảm trong 72 giờ (NĐ 356 Đ8).
Trẻ em từ đủ 7 tuổi: cần sự đồng ý của cả trẻ và người đại diện khi công bố thông tin đời tư (Luật 91 Đ24).

Nguồn: Luật 91/2025/QH15 Đ1, Đ24, Đ38; NĐ 356/2025/NĐ-CP Đ4, Đ8, Đ41.

Khung pháp lý cần nắm

Ba lớp văn bản: nghĩa vụ nền tảng, yêu cầu theo hoạt động và chế tài.

1 NGHĨA VỤ NỀN TẢNG

**Luật Bảo vệ dữ liệu cá nhân
91/2025/QH15**

01/01/2026

Nguyên tắc, quyền, đồng ý, DPIA, chuyển dữ liệu ra nước ngoài, thông báo vi phạm

**Nghị định 356/2025/NĐ-CP (thay NĐ
13/2023)**

01/01/2026

Danh mục dữ liệu nhạy cảm, thời hạn xử lý yêu cầu, hồ sơ, nhân sự, dịch vụ

2 YÊU CẦU THEO HOẠT ĐỘNG

**Luật Dữ liệu 60/2024/QH15 + NĐ
165/2025/NĐ-CP**

01/7/2025

Dữ liệu cốt lõi, quan trọng; mã hóa; chuyển dữ liệu ra nước ngoài

**Luật An ninh mạng 116/2025/QH15 +
NĐ 331, 333/2026**

**01/7/2026;
19/8/2026**

Bảo vệ hệ thống thông tin theo cấp độ

NĐ 341/2026/NĐ-CP (mật mã dân sự)

01/9/2026

Khi kinh doanh, sử dụng sản phẩm mã hóa

**Luật Trí tuệ nhân tạo 134/2025/QH15
+ NĐ 142/2026 + QĐ 33/2026/QĐ-TTg**

**01/3/2026;
15/8/2026**

Phân loại rủi ro, minh bạch, danh mục hệ thống AI rủi ro cao

**Luật Giao dịch điện tử 20/2023; Luật
Bảo vệ quyền lợi người tiêu dùng
19/2023; pháp luật lao động, chuyên
ngành**

—

Theo hoạt động cụ thể

3 CHẾ TÀI

**Luật 91 Đ8 + NĐ 330/2026/NĐ-CP (xử
phạt an ninh mạng và bảo vệ dữ liệu
cá nhân)**

19/8/2026

Mức phạt cụ thể từng hành vi, biện pháp khắc phục

Điểm giao thoa: đã lập hồ sơ DPIA và hồ sơ chuyển dữ liệu ra nước ngoài theo Luật 91 thì không phải lập thêm đánh giá rủi ro theo pháp luật về dữ liệu, kể cả với dữ liệu cốt lõi, quan trọng là dữ liệu cá nhân (Luật 91 Đ5.4; NĐ 356 Đ42.3).

Nguồn: Văn bản gốc theo số hiệu; hiệu lực đối chiếu điều khoản hiệu lực của từng văn bản.

Ai chịu trách nhiệm, dữ liệu đi đâu?

Xác định đúng vai trò là bước đầu tiên, vì nghĩa vụ đi theo vai trò.

Vai trò	Định nghĩa ngắn	Ví dụ
Bên kiểm soát	Quyết định mục đích và phương tiện xử lý	Doanh nghiệp thuê công ty khác tính lương
Bên xử lý	Xử lý theo yêu cầu của bên kiểm soát, thông qua hợp đồng	Công ty dịch vụ tính lương, nhà cung cấp đám mây
Bên kiểm soát và xử lý	Vừa quyết định, vừa trực tiếp xử lý	Doanh nghiệp tự tuyển dụng, tự quản lý nhân sự
Bên thứ ba	Bên khác tham gia xử lý theo quy định	Đơn vị kiểm toán, công ty bảo hiểm

Vòng đời dữ liệu: ai nhận, xử lý ở đâu?



Biểu tượng cam: chẳng có thể phát sinh chuyển dữ liệu ra nước ngoài

Ba trường hợp được coi là chuyển dữ liệu xuyên biên giới

- a) Chuyển dữ liệu đang lưu tại Việt Nam ra hệ thống lưu trữ ở nước ngoài
- b) Chuyển dữ liệu cho tổ chức, cá nhân ở nước ngoài
- c) Dùng nền tảng ở nước ngoài để xử lý dữ liệu thu thập tại Việt Nam

Hai điểm hay nhầm: (1) Mã hóa không làm dữ liệu hết là dữ liệu cá nhân. (2) Chỉ dữ liệu đã khử nhận dạng, không thể xác định lại một người cụ thể, mới không còn là dữ liệu cá nhân.

Nguồn: Luật 91/2025/QH15 Đ2, Đ12.1, Đ20.1.

Căn cứ xử lý và quyền cá nhân

Mỗi hoạt động xử lý cần có căn cứ, và mỗi yêu cầu của người có dữ liệu cần được xử lý đúng hạn.

Việc cần thực hiện	Bảng chứng cần có	Căn cứ
Xác định mục đích cụ thể cho từng hoạt động; chỉ thu thập dữ liệu cần thiết	Danh mục hoạt động xử lý (khuyến nghị)	Luật 91 Đ3.2
Xin đồng ý theo từng mục đích; không đặt sẵn mặc định đồng ý; im lặng không phải là đồng ý; nói rõ khi là dữ liệu nhạy cảm	Nhật ký đồng ý kiểm chứng được: ai, lúc nào, nội dung gì	Luật 91 Đ9; NĐ 356 Đ6
Khi xử lý không cần đồng ý, phải có cơ chế giám sát	Phân tích căn cứ; quy trình; đánh giá định kỳ	Luật 91 Đ19
Tiếp nhận và xử lý yêu cầu của người có dữ liệu	Quy trình, biểu mẫu, sổ theo dõi thời hạn	NĐ 356 Đ5
Lưu trữ đúng thời hạn; xóa hồ sơ ứng viên không trúng tuyển; xóa dữ liệu người lao động khi nghỉ việc (trừ khi có thỏa thuận hoặc luật quy định khác)	Chính sách lưu trữ; biên bản xóa, hủy	Luật 91 Đ14, Đ25

Thời hạn xử lý yêu cầu của người có dữ liệu

Mọi yêu cầu: phản hồi trong 02 ngày làm việc, sau đó thực hiện trong thời hạn dưới đây

Loại yêu cầu	Doanh nghiệp tự làm	Khi cần bên xử lý thực hiện	Gia hạn tối đa 1 lần
Rút đồng ý, hạn chế, phản đối	15 ngày	20 ngày	15 ngày
Xem, chỉnh sửa, cung cấp	10 ngày	15 ngày	10 ngày
Xóa dữ liệu	20 ngày	30 ngày	20 ngày

Nguồn: Luật 91/2025/QH15; NĐ 356/2025/NĐ-CP Đ5, Đ6. Không có/không chứng minh được sự đồng ý: phạt 30–50 triệu đồng (NĐ 330 Đ43).

Hồ sơ, nhân sự và nhà cung cấp

Nghĩa vụ hồ sơ có điều kiện. Cần biết khi nào phải làm, ai làm và nộp ở đâu.

Nghĩa vụ	Áp dụng khi	Yêu cầu chính
Hồ sơ đánh giá tác động xử lý dữ liệu (DPIA)	Doanh nghiệp là bên kiểm soát; bên xử lý lập theo thỏa thuận	Nộp 01 bản chính trong 60 ngày từ ngày bắt đầu xử lý; cập nhật 6 tháng khi có thay đổi, 10 ngày khi tổ chức lại (Luật 91 Đ21–22; NĐ 356 Đ19–20)
Hồ sơ chuyển dữ liệu ra nước ngoài (DTIA)	Thuộc 1 trong 3 trường hợp ở trang 7	Nộp trong 60 ngày từ lần chuyển đầu tiên, kèm hợp đồng, sơ đồ luồng dữ liệu, đánh giá bên nhận (NĐ 356 Đ18)
Không phải lập DTIA	Các trường hợp loại trừ	Lưu dữ liệu người lao động trên đám mây; quản lý nhân sự xuyên biên giới theo quy chế lao động; ký hợp đồng, vận chuyển, thanh toán, khách sạn, thị thực (Luật 91 Đ20.6; NĐ 356 Đ17.3)
Nhân sự, bộ phận bảo vệ dữ liệu	Mọi tổ chức, trừ trường hợp miễn ở trang 2	Chỉ định bằng văn bản; cao đẳng trở lên, ít nhất 2 năm kinh nghiệm, đã được đào tạo; có thể thuê dịch vụ (NĐ 356 Đ13, Đ15–16)
Hợp đồng chuyển giao dữ liệu	Khi chuyển dữ liệu cho bên khác	7 nội dung: mục đích, loại dữ liệu, thời hạn và xóa, cơ sở pháp lý, trách nhiệm bảo vệ, quyền của người có dữ liệu, phối hợp khi vi phạm (NĐ 356 Đ7.1)
Hợp đồng dịch vụ đám mây	Khi dùng đám mây xử lý dữ liệu cá nhân	Ghi rõ luồng xử lý, vai trò, biện pháp bảo mật; dữ liệu phải được mã hóa khi lưu và khi truyền (NĐ 356 Đ12)
Giấy chứng nhận dịch vụ xử lý dữ liệu	Khi doanh nghiệp cung cấp dịch vụ xử lý thay khách hàng	Do Bộ Công an cấp; 9 loại dịch vụ, gồm vận hành hệ thống thay khách hàng và mã hóa dữ liệu cá nhân (NĐ 356 Đ21–25)

Chuyển tiếp: sự đồng ý và hồ sơ đã nộp theo NĐ 13/2023 trước 01/01/2026 tiếp tục được sử dụng; khi cập nhật thì làm theo quy định mới (Luật 91 Đ39).

Nguồn: Luật 91/2025/QH15; NĐ 356/2025/NĐ-CP.

Chế tài khi không tuân thủ

Mức phạt tối đa không phải là mức sẽ bị phạt. Hậu quả vận hành thường đến trước tiền phạt.

3 tỷ đồng

≈ 115.000 USD
Mức tối đa cho các vi phạm thông thường

5% doanh thu

năm trước liền kề
Vi phạm quy định chuyển dữ liệu ra nước ngoài

10 lần

khoản thu có được
Mua bán dữ liệu cá nhân

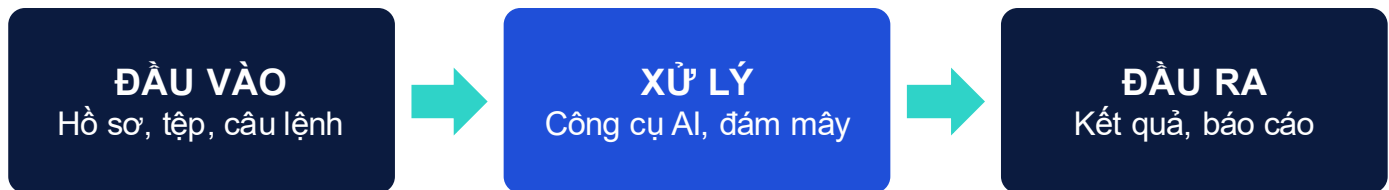
Hành vi vi phạm (tổ chức)	Mức phạt	Căn cứ ND 330
Xử lý khi chưa có sự đồng ý; mặc định đồng ý; không lưu nhật ký đồng ý	30–50 triệu	Đ43.1
Coi im lặng là đồng ý; tiếp tục xử lý sau khi bị yêu cầu ngừng	50–70 triệu	Đ43.2
Không lập, không nộp hồ sơ DPIA trong 60 ngày (có thể bị buộc dừng xử lý dữ liệu đến khi nộp đủ)	20–30 triệu	Đ55.1, Đ55.3
Báo cơ quan chuyên trách chậm hơn 72 giờ khi có vi phạm gây hại	40–60 triệu	Đ54.3
Không chỉ định, hoặc chỉ định nhân sự bảo vệ dữ liệu không đủ điều kiện	20–30 triệu	Đ57.2
Lắp phần mềm theo dõi, camera không thông báo người lao động; không xóa dữ liệu khi nghỉ việc	50–70 triệu	Đ61.2
Dùng đám mây nhưng không mã hóa dữ liệu khách hàng khi lưu và khi truyền	50–70 triệu	Đ69.2
Dữ liệu sinh trắc học không bảo mật vật lý, không hạn chế truy cập, không báo trong 72 giờ	50–70 triệu	Đ70.1
Chuyển dữ liệu ra nước ngoài không lập hồ sơ, dẫn đến lộ dữ liệu từ 10.000 người trở lên	1–5% doanh thu tại Việt Nam	Đ56.3; đình chỉ chuyển 6–12 tháng

Mức trần áp dụng cho tổ chức; cá nhân chịu tối đa 1/2 (Luật 91 Đ8; ND 330 Đ7). Ngoài tiền phạt: buộc xóa dữ liệu thu thập trái phép, nộp lại khoản thu, bồi thường thiệt hại, có thể bị truy cứu trách nhiệm hình sự.

Nghĩa vụ cụ thể phụ thuộc vào hoạt động xử lý, vai trò, loại dữ liệu và điều kiện áp dụng. Doanh nghiệp cần xác định phạm vi trước khi lựa chọn hồ sơ và giải pháp.

Sử dụng AI và đám mây có kiểm soát

AI không bị cấm. Điều cần làm là biết dữ liệu nào đi vào, xử lý ở đâu và kết quả được dùng ra sao.



- 1 Công cụ được phê duyệt**
 Công cụ nào được dùng? Máy chủ ở đâu? Có phải lập hồ sơ chuyển dữ liệu ra nước ngoài? *Luật 91 Đ20.1*
- 2 Dữ liệu đầu vào**
 Hạn chế dữ liệu nhạy cảm; khử nhận dạng hoặc ẩn danh trước khi đưa vào. *Luật 91 Đ30.1; NĐ 356 Đ9.3*
- 3 Nhà cung cấp, nhà thầu phụ**
 Có lưu nội dung nhập vào không? Có dùng để huấn luyện? Nhật ký lưu ở đâu? *NĐ 356 Đ12*
- 4 Kết quả đầu ra**
 Kết quả AI suy ra nếu xác định được một người thì vẫn là dữ liệu cá nhân. Xử lý tự động phải thông báo, giải thích, cho quyền không tham gia. *NĐ 356 Đ10*
- 5 Lưu và xóa**
 Nội dung nhập vào, lịch sử, tệp tải lên được xóa khi nào? *Luật 91 Đ14*

Theo luật mới về AI và đám mây

Hệ thống AI, đám mây phải có biện pháp bảo mật, xác thực và phân quyền truy cập (Luật 91 Đ30.3). Dữ liệu cá nhân trên đám mây phải mã hóa khi lưu và khi truyền (NĐ 356 Đ12.4). Bên triển khai AI kế thừa phân loại rủi ro của nhà cung cấp và phải phân loại lại nếu sửa đổi làm phát sinh rủi ro mới (Luật 134/2025 Đ10.2); hệ thống thuộc danh mục rủi ro cao có lộ trình riêng (QĐ 33/2026/QĐ-TTg).

Nguồn: Luật 91/2025/QH15; NĐ 356/2025/NĐ-CP; Luật 134/2025/QH15; QĐ 33/2026/QĐ-TTg.

Ba trụ cột bảo vệ dữ liệu

Không trụ cột nào tự đứng một mình. Thiếu một trụ cột, hai trụ cột còn lại mất hiệu quả.

 QUY TRÌNH	 CON NGƯỜI	 CÔNG NGHỆ
Danh mục hoạt động xử lý, căn cứ xử lý KHUYẾN NGHỊ	Chỉ định nhân sự, bộ phận bảo vệ dữ liệu (Luật 91 Đ33.2) BẮT BUỘC	Phân quyền truy cập dữ liệu nhạy cảm (NĐ 356 Đ4.2) BẮT BUỘC
Chính sách, thông báo, quy trình xin đồng ý (Luật 91 Đ9) BẮT BUỘC	Phân công trách nhiệm từng bộ phận KHUYẾN NGHỊ	Xác thực đa yếu tố khi xử lý dữ liệu lớn (NĐ 356 Đ9.3) BẮT BUỘC KHI ÁP DỤNG
Quy trình thực hiện quyền (NĐ 356 Đ5) BẮT BUỘC	Đào tạo định kỳ (NĐ 356 Đ9.2, Đ14) BẮT BUỘC KHI ÁP DỤNG	Mã hóa và quản lý khóa (NĐ 356 Đ7.2, Đ12.4) BẮT BUỘC KHI ÁP DỤNG
Hợp đồng với nhà cung cấp (NĐ 356 Đ7, Đ12) BẮT BUỘC	Thỏa thuận bảo mật KHUYẾN NGHỊ	Nhật ký, giám sát truy cập (NĐ 356 Đ8.1, Đ9.3) BẮT BUỘC KHI ÁP DỤNG
Ứng phó sự cố, báo trong 72 giờ (Luật 91 Đ23; NĐ 356 Đ28) BẮT BUỘC	Chống nhân sự nội bộ chia sẻ trái phép dữ liệu cho bên thứ ba (NĐ 356 Đ7.4) BẮT BUỘC	Sao lưu, khôi phục; xóa an toàn (Luật 91 Đ14.3) BẮT BUỘC

Ô màu cam: Nghị định 356 yêu cầu có biện pháp chống nhân sự nội bộ chia sẻ trái phép dữ liệu. Đây là điểm mà quy trình và con người cần thêm lớp kiểm soát ngay trên tệp dữ liệu.

Nguồn: Luật 91/2025/QH15; NĐ 356/2025/NĐ-CP. “Bắt buộc khi áp dụng”: khi doanh nghiệp thuộc trường hợp điều khoản quy định.

Lộ trình nền tảng 90 ngày

Bắt đầu từ việc biết mình có dữ liệu gì, rồi mới đến hồ sơ và công cụ.



NGÀY 1–30
Nhận diện

Việc ưu tiên: Kiểm kê dữ liệu; vẽ luồng dữ liệu; xác định vai trò, căn cứ, nghĩa vụ; rà soát hồ sơ đã nộp

Phụ trách: DPO, Pháp chế, Nhân sự, CNTT

Đầu ra: Bản đồ dữ liệu; danh sách khoảng trống theo mức ưu tiên



NGÀY 31–60
Thiết lập

Việc ưu tiên: Hoàn thiện DPIA, hồ sơ chuyển dữ liệu ra nước ngoài, hợp đồng nhà cung cấp, quy trình đồng ý và quyền; cấu hình biện pháp bảo vệ

Phụ trách: Pháp chế, CNTT, Mua hàng

Đầu ra: Bộ hồ sơ áp dụng; các kiểm soát đã triển khai



NGÀY 61–90
Kiểm chứng

Việc ưu tiên: Kiểm thử; diễn tập sự cố 72 giờ; đào tạo; xử lý tồn tại

Phụ trách: DPO, CNTT, toàn bộ quản lý

Đầu ra: Kết quả kiểm thử; kế hoạch duy trì và đánh giá định kỳ

Lưu ý: lộ trình là khuyến nghị cách tổ chức công việc, không thay thế hay gia hạn thời hạn pháp luật. Nếu hồ sơ bắt buộc chưa nộp đúng hạn (ví dụ DPIA trong 60 ngày), cần xử lý ngay trong giai đoạn 1 và tham vấn pháp lý.

Nguồn: Khuyến nghị quản trị của AISA; thời hạn hồ sơ theo Luật 91/2025/QH15 Đ20, Đ21.

Doanh nghiệp đã nhận diện đủ khoảng trống bảo vệ dữ liệu?

Làm khảo sát khoảng 10 phút để rà soát bước đầu về quản trị, hồ sơ và biện pháp kỹ thuật. Kết quả giúp xác định việc cần ưu tiên và chuẩn bị cho buổi trao đổi chuyên môn.



Quét QR để làm khảo sát
aisa.vn/assessment/pdp

Sau khảo sát: trao đổi cùng AISA về nhu cầu bảo vệ dữ liệu và xem demo DCS trên môi trường của AISA, với dữ liệu giả lập.

Khảo sát dựa trên thông tin tự khai, không thay thế đánh giá pháp lý hoặc kiểm tra hệ thống.



AISA · AI | Security | Automation

Đơn vị phát triển giải pháp DCS – bảo mật lấy dữ liệu làm trung tâm (Data-Centric Security) tại Việt Nam.

Hotline: +84 905 885 539 **Email:** info@aisa.vn **Web:** aisa.vn

Địa chỉ: Tầng 16, Saigon Tower, 29 Lê Duẩn, Sài Gòn, TP. Hồ Chí Minh

Tài liệu tổng hợp quy định pháp luật Việt Nam hiện hành đến 15/10/2026 nhằm mục đích tham khảo, không phải ý kiến pháp lý. Doanh nghiệp nên tham vấn chuyên gia pháp lý cho trường hợp cụ thể.