IL

VIỆN NGHIÊN CỨU PHÁP LUẬT
và Phát triển Giáo dục — ILED

ẤN PHẨM CHUYÊN ĐỀ · Q2/2026

Cẩm nang Tuân thủ Luật Trí tuệ Nhân tạo 2026

Hướng dẫn dành cho Doanh nghiệp vừa và nhỏ Việt Nam

Phát hành:	Quý II năm 2026
Phiên bản:	1.0
Cập nhật theo:	Luật Trí tuệ Nhân tạo 134/2025/QH15 và Nghị định 142/2026/NĐ-CP
Phụ trách nội dung:	LG. Trương Hữu Hiệp - Phó Viện trưởng Luật học, ILED

Mục lục

Phần VIII - Phụ lục

PHẦN I

Tổng quan

1. Bối cảnh pháp lý

Việt Nam đã ban hành **Luật Trí tuệ Nhân tạo số 134/2025/QH15** tại kỳ họp Quốc hội năm 2025, đánh dấu lần đầu tiên có một đạo luật chuyên ngành về AI. Luật quy định khung pháp lý chung về quyền và nghĩa vụ của các bên liên quan đến hệ thống AI, phân loại rủi ro, cơ chế đánh giá phù hợp và quản lý nhà nước về AI tại Việt Nam.

Tiếp đó, ngày **30/04/2026**, Chính phủ ban hành **Nghị định số 142/2026/NĐ-CP** quy định chi tiết và biện pháp thi hành Luật Trí tuệ Nhân tạo. Nghị định gồm 8 chương, 46 điều và 17 mẫu phụ lục, có hiệu lực thi hành từ **01/05/2026** - chỉ một ngày sau ngày ký.

> **LƯU Ý**
>
> Tốc độ thi hành rất gấp. Doanh nghiệp đang sử dụng hoặc cung cấp hệ thống AI tại Việt Nam phải tuân thủ ngay lập tức các quy định về phân loại rủi ro, hồ sơ kỹ thuật, đánh giá phù hợp và thông báo qua Cổng thông tin điện tử một cửa AI.

Mối quan hệ với các văn bản pháp luật khác

Luật AI và Nghị định 142/2026 không tồn tại độc lập. Doanh nghiệp dùng AI vẫn phải tuân thủ:

- **Nghị định 13/2023/NĐ-CP** về Bảo vệ Dữ liệu Cá nhân - khi AI xử lý dữ liệu cá nhân của khách hàng, nhân viên, đối tác.
- **Luật An ninh mạng 2018** - khi AI vận hành trên hạ tầng số quan trọng hoặc xử lý dữ liệu nhạy cảm.
- **Pháp luật chuyên ngành**: tài chính - ngân hàng (Luật Các tổ chức tín dụng), y tế (Luật Khám bệnh, Chữa bệnh), giáo dục, lao động.

Khoản 7 Điều 12 NĐ 142/2026 cho phép sử dụng **Hồ sơ DPIA theo NĐ 13/2023** để thay thế hoặc tích hợp làm thành phần của Hồ sơ phân loại rủi ro AI - giảm chi phí tuân thủ đáng kể cho doanh nghiệp đã có DPIA.

2. Doanh nghiệp nào bị ảnh hưởng

Phạm vi điều chỉnh của Luật AI rất rộng. Hãy tự kiểm tra xem doanh nghiệp anh chị có thuộc đối tượng tuân thủ không:

4 vai trò pháp lý theo Luật AI

Vai trò	Định nghĩa	Ví dụ
Nhà phát triển	Tổ chức, cá nhân nghiên cứu, thiết kế, huấn luyện hệ thống AI	Công ty AI tự xây dựng mô hình, startup AI tiếng Việt
Nhà cung cấp	Tổ chức, cá nhân đưa hệ thống AI ra thị trường, cung cấp cho người sử dụng	SaaS bán phần mềm AI, đại lý phân phối AI nước ngoài tại VN
Bên triển khai	Tổ chức, cá nhân triển khai, vận hành hệ thống AI để cung cấp dịch vụ hoặc thực hiện hoạt động kinh doanh	Doanh nghiệp dùng chatbot AI cho website TMĐT, ngân hàng dùng AI chấm điểm tín dụng
Người sử dụng	Cá nhân, tổ chức sử dụng hệ thống AI cho công việc hàng ngày, không tham gia phát triển hoặc triển khai	Nhân viên dùng ChatGPT viết nội dung, kế toán dùng Copilot xử lý số liệu

Bạn có dùng AI không? - Decision tree

Nếu doanh nghiệp đang sử dụng **bất kỳ** một trong những thứ sau, anh chị đã thuộc phạm vi điều chỉnh:

- Chatbot trên website / Zalo / Messenger / Telegram
- Công cụ AI viết nội dung (ChatGPT, Claude, Gemini, Copilot)
- AI sàng lọc CV, phân tích ứng viên
- AI gợi ý sản phẩm / cá nhân hoá trên website TMĐT
- AI nhận diện khuôn mặt cho hệ thống chấm công / kiểm soát ra vào
- Hệ thống chấm điểm tín dụng, đánh giá rủi ro tự động
- AI dịch tự động cho dịch vụ khách hàng
- AI phân tích cảm xúc khách hàng từ data review
- AI tối ưu giá / quản lý kho thông minh
- AI dự đoán doanh số / phân tích báo cáo tài chính

> **TIN TỐT**
>
> Việc tuân thủ **không khó như tưởng tượng**. Phần lớn các trường hợp dùng AI thuộc mức rủi ro **không đáng kể** hoặc **trung bình** - chỉ cần lập hồ sơ đơn giản, không phải đánh giá phức tạp.

PHẦN II

Phân loại rủi ro AI

3. Bốn mức rủi ro

Theo Điều 9 Nghị định 142/2026/NĐ-CP, mọi hệ thống AI được phân loại theo 4 mức rủi ro:

Mức rủi ro	Đặc điểm	Ví dụ	Yêu cầu tuân thủ
Không đáng kể	Không tương tác trực tiếp người dùng cuối, không tạo nội dung công khai, không quyết định ảnh hưởng quan trọng	AI lọc spam email, AI gợi ý từ tiếp theo khi gõ, AI tối ưu vận hành nội bộ	Hầu như không cần làm gì. Khuyến nghị lưu nội bộ thông tin về hệ thống.
Trung bình	Tương tác với khách hàng / đối tác, tạo nội dung công khai, hỗ trợ ra quyết định không quan trọng	Chatbot CSKH, AI tạo nội dung marketing, AI gợi ý sản phẩm TMĐT, AI dịch tự động	Lập hồ sơ phân loại rủi ro (Điều 12) + thông báo trên Cổng AI + lưu trữ suốt vòng đời
Cao	Có thể ảnh hưởng đáng kể đến quyền và lợi ích hợp pháp, tài sản, sức khỏe, an toàn của cá nhân hoặc xã hội	AI sàng lọc CV / tuyển dụng, chấm điểm tín dụng, đánh giá rủi ro bảo hiểm, AI nhận diện khuôn mặt, AI hỗ trợ chẩn đoán y tế	Hồ sơ đầy đủ + đánh giá phù hợp + giám sát con người + báo cáo sự cố + đăng ký Cổng AI
Không chấp nhận được	Hệ thống vi phạm hiến pháp, quyền con người, an ninh quốc gia, đạo đức xã hội	AI phân loại điểm xã hội (social scoring), AI thao túng tâm lý có chủ đích, AI nhận dạng cảm xúc trong tuyển dụng / giáo dục	**Bị cấm** phát triển, cung cấp, triển khai và sử dụng tại Việt Nam

Danh mục AI rủi ro cao bắt buộc

Theo phụ lục Luật AI, các nhóm sau mặc định thuộc rủi ro cao và phải đánh giá phù hợp bắt buộc trước khi đưa vào sử dụng:

- AI trong hệ thống cơ sở hạ tầng quan trọng (giao thông, năng lượng, viễn thông, cấp nước)
- AI trong giáo dục - đào tạo (đánh giá, phân loại học sinh)
- AI trong tuyển dụng - quản lý nhân sự (sàng lọc, đánh giá hiệu suất)
- AI trong dịch vụ thiết yếu (tài chính - ngân hàng, bảo hiểm, y tế)
- AI thực thi pháp luật (đánh giá tái phạm, dự đoán tội phạm)
- AI trong tư pháp và quá trình dân chủ

- AI nhận dạng sinh trắc học từ xa (real-time biometric ID)

4. Checklist tự phân loại 12 câu

Trả lời **"Có"** hay **"Không"** cho 12 câu hỏi sau. Đếm số "Có" để xác định mức rủi ro sơ bộ.

- ☐ **1.** Hệ thống AI có tương tác trực tiếp với khách hàng / người ngoài tổ chức không?
- ☐ **2.** Hệ thống có tạo ra nội dung công khai (văn bản, hình ảnh, âm thanh) cho người ngoài thấy không?
- ☐ **3.** Hệ thống có hỗ trợ hoặc tự động ra quyết định ảnh hưởng đến tuyển dụng, lương, đánh giá nhân viên không?
- ☐ **4.** Hệ thống có hỗ trợ hoặc tự động ra quyết định về cấp tín dụng, bảo hiểm, dịch vụ tài chính cho khách hàng không?
- ☐ **5.** Hệ thống có xử lý dữ liệu cá nhân của trên 1.000 người hoặc dữ liệu cá nhân nhạy cảm (sức khỏe, sinh trắc, tôn giáo) không?
- ☐ **6.** Hệ thống có hỗ trợ chẩn đoán hoặc điều trị y tế không?
- ☐ **7.** Hệ thống có nhận diện khuôn mặt, sinh trắc học không?
- ☐ **8.** Hệ thống có vận hành trong hạ tầng giao thông, năng lượng, viễn thông không?
- ☐ **9.** Hệ thống có sử dụng dữ liệu của trẻ em dưới 18 tuổi không?
- ☐ **10.** Hệ thống có khả năng gây thiệt hại tài chính đáng kể (trên 100 triệu VND) cho 1 cá nhân nếu lỗi không?
- ☐ **11.** Hệ thống có thể bị lợi dụng để thao túng quyết định, tâm lý người dùng không?
- ☐ **12.** Hệ thống có dùng để đánh giá / phân loại điểm xã hội của người dân không?

Cách tính kết quả

Số câu "Có"	Mức rủi ro sơ bộ	Hành động
0	Không đáng kể	Không bắt buộc làm hồ sơ
1 - 2 (chỉ câu 1, 2)	Trung bình	Lập hồ sơ phân loại rủi ro
3 trở lên (bất kỳ câu 3-10)	Cao	Hồ sơ đầy đủ + đánh giá phù hợp + HITL
Có câu 11 hoặc 12	Không chấp nhận được	Dừng triển khai ngay

KHUYẾN NGHỊ

Sau khi tự phân loại, hãy **đối chiếu với Công cụ phân loại rủi ro tự động** trên Cổng thông tin một cửa AI của Bộ KH&CN (sắp vận hành). Kết quả từ Công cụ này có giá trị pháp lý là một tài liệu điện tử hợp lệ trong hồ sơ.

PHẦN III

Hồ sơ phân loại rủi ro

5. Cấu trúc hồ sơ và bảo vệ bí mật

Theo Điều 12 Nghị định 142/2026/NĐ-CP, đối với hệ thống AI **rủi ro cao và trung bình**, nhà cung cấp phải lập và lưu trữ hồ sơ phân loại rủi ro suốt thời gian hệ thống hoạt động.

4 nội dung bắt buộc

1. Nhận diện hệ thống	Tên hệ thống, phiên bản, mã định danh nội bộ hoặc mã định danh do cơ quan có thẩm quyền cấp; tên, địa chỉ và thông tin liên hệ của nhà cung cấp.
2. Mô tả hệ thống	Mục đích sử dụng, chức năng chính, kiến trúc hệ thống ở mức chức năng - nghiệp vụ, phạm vi triển khai, nhóm người sử dụng và người bị ảnh hưởng.
3. Thông tin về dữ liệu	Mô tả khái quát loại dữ liệu đầu vào chủ yếu được sử dụng để vận hành hệ thống.
4. Quản lý rủi ro	Tóm tắt các biện pháp quản lý rủi ro, bảo đảm an toàn và tính minh bạch của hệ thống.

> **TIN TỐT - BẢO VỆ BÍ MẬT KINH DOANH**
>
> Hồ sơ **không bắt buộc tiết lộ** mã nguồn, bộ tham số mô hình, thuật toán chi tiết, dữ liệu huấn luyện thô hoặc các thông tin thuộc bí mật nhà nước, bí mật kinh doanh, bí mật công nghệ - trừ trường hợp pháp luật có quy định khác (khoản 4 Điều 12).

Tích hợp với Hồ sơ DPIA

Khoản 7 Điều 12 cho phép doanh nghiệp đã có **Hồ sơ Đánh giá Tác động Xử lý Dữ liệu Cá nhân (DPIA)** theo NĐ 13/2023 sử dụng làm thành phần của Hồ sơ phân loại rủi ro AI. Điều này tiết kiệm thời gian và chi phí tuân thủ đáng kể.

6. Mẫu hồ sơ phân loại - 2 ví dụ

Ví dụ 1: Chatbot CSKH (rủi ro trung bình)

Nội dung	Thông tin
Tên hệ thống	ABC Customer Chatbot v2.3
Mã định danh nội bộ	ABC-AI-001
Nhà cung cấp	Công ty TNHH ABC, MST: 0123456789, địa chỉ: ...
Mục đích sử dụng	Trả lời tự động câu hỏi của khách hàng về sản phẩm trên website và Zalo OA
Kiến trúc	Mô hình ngôn ngữ lớn của bên thứ ba (OpenAI GPT-4) + lớp prompt-engineering nội bộ + cơ sở tri thức sản phẩm (RAG)
Nhóm tương tác	Khách hàng cá nhân và doanh nghiệp truy cập website / Zalo OA của ABC
Dữ liệu đầu vào	Tin nhắn của khách hàng (có thể chứa thông tin cá nhân: tên, sđt, email khi khách chủ động cung cấp)
Quản lý rủi ro	(1) Có agent người chuyển tiếp khi chatbot không xử lý được; (2) Lưu nhật ký tương tác 90 ngày; (3) Có thông báo rõ ràng "Bạn đang chat với AI" ở đầu mỗi cuộc hội thoại; (4) Tích hợp DPIA theo NĐ 13/2023

Ví dụ 2: Hệ thống chấm điểm tín dụng (rủi ro cao)

Nội dung	Thông tin
Tên hệ thống	XYZ Credit Scoring Engine v4.0
Mã định danh nội bộ	XYZ-CS-2026-001
Nhà cung cấp	Công ty Cổ phần XYZ Tài chính
Mục đích sử dụng	Hỗ trợ ra quyết định cho vay tiêu dùng cho khoản vay dưới 200 triệu VND
Kiến trúc	Mô hình gradient boosting (XGBoost) + ensemble với 1 mô hình thần kinh sâu; vận hành trên hạ tầng on-premise của XYZ
Nhóm tương tác	Khách hàng cá nhân nộp đơn xin vay; nhân viên thẩm định
Dữ liệu đầu vào	Thông tin định danh (CCCD, sđt), thông tin việc làm, thu nhập, lịch sử tín dụng từ CIC, dữ liệu hành vi giao dịch ngân hàng (với sự đồng ý)
Quản lý rủi ro	(1) HITL bắt buộc - mọi đơn vay phải có nhân viên thẩm định xem xét trước khi quyết định cuối cùng; (2) Khách hàng có quyền yêu cầu giải thích kết quả; (3) Đánh giá tác động xử lý dữ liệu cá nhân (DPIA) theo NĐ 13/2023; (4) Nhật ký vận hành lưu 5 năm; (5) Báo cáo sự cố trong 48h cho Ngân hàng Nhà nước và Bộ KH&CN

PHẦN IV

Đánh giá phù hợp và Thông báo

7. Quy trình đánh giá phù hợp

Theo Điều 13 NĐ 142/2026, hệ thống AI **rủi ro cao** phải đánh giá phù hợp trước khi đưa vào sử dụng. Có 2 phương thức:

Phương thức 1 - Tổ chức đánh giá phù hợp

Áp dụng cho hệ thống thuộc **Danh mục bắt buộc chứng nhận**. Doanh nghiệp phải thuê tổ chức đánh giá phù hợp được cơ quan có thẩm quyền cấp phép thực hiện.

Tiêu chí của tổ chức đánh giá:

- Đã đăng ký hoạt động đánh giá phù hợp theo pháp luật về tiêu chuẩn và quy chuẩn kỹ thuật
- Bảo đảm tính độc lập, khách quan
- Đội ngũ chuyên gia đáp ứng yêu cầu chuyên môn về AI, an ninh mạng, quản trị dữ liệu
- Chịu sự giám sát định kỳ của cơ quan nhà nước có thẩm quyền

Phương thức 2 - Tự đánh giá

Áp dụng cho hệ thống rủi ro cao **không thuộc Danh mục bắt buộc**. Nhà cung cấp có quyền tự đánh giá hoặc thuê tổ chức đánh giá. Khi tự đánh giá, phải:

- Lập hồ sơ kỹ thuật đầy đủ
- Chịu trách nhiệm pháp lý trước kết quả đánh giá
- Sẵn sàng cung cấp hồ sơ khi cơ quan nhà nước thanh tra, kiểm tra

Khi nào phải đánh giá lại

Trong quá trình sử dụng, phải đánh giá lại khi:

- Thay đổi chức năng chính, mục đích hoặc phạm vi ứng dụng
- Thay đổi kiến trúc, mô hình, cấu hình kỹ thuật chủ yếu
- Thay đổi nguồn dữ liệu, loại dữ liệu đầu vào hoặc phương thức xử lý dữ liệu
- Tích hợp với hệ thống khác làm thay đổi điều kiện vận hành

Các hoạt động **không cần đánh giá lại**: cập nhật dữ liệu định kỳ, sửa lỗi kỹ thuật, tối ưu hiệu năng, nâng cấp phiên bản nhỏ.

8. Thông báo trên Cổng AI

Theo Điều 14, trước khi đưa hệ thống AI **rủi ro trung bình hoặc cao** vào sử dụng, nhà cung cấp **phải thông báo** kết quả phân loại cho Bộ KH&CN qua Cổng thông tin điện tử một cửa AI.

Hai hình thức thông báo

A

Kê khai trực tiếp

Truy cập Cổng AI, đăng nhập tài khoản doanh nghiệp, điền biểu mẫu điện tử với 4 nội dung của Hồ sơ phân loại rủi ro. Phù hợp với doanh nghiệp có ít hệ thống AI hoặc cập nhật không thường xuyên.

B

Gửi qua API

Tích hợp giao diện lập trình ứng dụng (API) của Cổng AI vào hệ thống quản lý nội bộ. Tự động gửi thông báo khi có hệ thống AI mới hoặc cập nhật. Phù hợp với doanh nghiệp lớn có nhiều hệ thống AI.

Sau khi thông báo

Bộ KH&CN qua Cổng AI **tự động cấp mã định danh hệ thống** ngay khi nhà cung cấp hoàn tất việc gửi thông báo. Mã định danh có dạng `VN-AI-2026-XXXXXX` phục vụ quản lý xuyên suốt vòng đời hệ thống.

> **QUAN TRỌNG**
>
> Tự kê khai - tự chịu trách nhiệm. Cơ quan nhà nước có thẩm quyền có thể thanh tra, kiểm tra và hậu kiểm theo quy định pháp luật. Thông tin sai lệch sẽ bị xử phạt theo pháp luật về xử phạt vi phạm hành chính trong lĩnh vực KH&CN.

PHẦN V

Quản lý vận hành

9. Hệ thống giám sát con người (HITL)

Đây là yêu cầu **quan trọng nhất** với AI rủi ro cao theo Điều 15. Doanh nghiệp phải đảm bảo luôn có người giám sát thực chất - không được để AI tự động ra quyết định ảnh hưởng quan trọng đến người dùng.

3 yêu cầu cốt lõi

Đầy đủ thông tin — Người giám sát phải được cung cấp thông tin đầy đủ về quyết định AI - đầu vào, đầu ra, mức tin cậy, các phương án thay thế, lý do chính dẫn đến kết quả.

Đủ thẩm quyền — Người giám sát có quyền can thiệp, sửa đổi, bác bỏ kết quả AI và áp dụng quyết định khác.

Lưu nhật ký — Hệ thống phải lưu đầy đủ nhật ký vận hành, các quyết định can thiệp - sửa đổi - bác bỏ của người giám sát.

Mẫu quy trình HITL

1. Hệ thống AI tạo ra kết quả với độ tin cậy (confidence score)
2. Nếu độ tin cậy < ngưỡng X% (thường 80-90%) → tự động chuyển cho người giám sát review
3. Nếu kết quả ảnh hưởng quan trọng (cho vay, tuyển dụng, dịch vụ thiết yếu) → bắt buộc review bất kể độ tin cậy
4. Người giám sát ra quyết định cuối cùng và ghi nhận lý do
5. Nhật ký lưu vĩnh viễn (hoặc theo quy định lưu trữ ngành)

10. Mẫu báo cáo sự cố

Theo Điều 12 Luật AI và Điều 17 NĐ 142/2026, doanh nghiệp phải báo cáo sự cố nghiêm trọng cho Bộ KH&CN trong vòng **48 giờ** kể từ khi phát hiện.

Định nghĩa "sự cố nghiêm trọng"

- AI gây thiệt hại tài sản trên 100 triệu VND cho 1 cá nhân hoặc trên 1 tỷ VND tổng cộng
- AI ra quyết định sai dẫn đến từ chối dịch vụ thiết yếu (cho vay, bảo hiểm, y tế) cho trên 100 người
- Lộ dữ liệu cá nhân của trên 1.000 chủ thể dữ liệu do lỗi AI
- AI bị tấn công, chiếm quyền điều khiển
- AI tạo ra nội dung sai sự thật, bôi nhọ, vi phạm pháp luật và đã được phát tán

Form báo cáo sự cố (theo Mẫu AI01a)

Trường thông tin	Mô tả
Mã định danh hệ thống	VN-AI-2026-XXXXXX
Thời điểm phát hiện	Ngày, giờ, phút
Mô tả sự cố	Tóm tắt 200 từ về sự cố, hành vi bất thường
Mức độ ảnh hưởng	Số người bị ảnh hưởng, thiệt hại tài chính ước tính, dữ liệu bị lộ (nếu có)
Biện pháp khắc phục đã thực hiện	Liệt kê các hành động đã triển khai
Biện pháp dự kiến	Kế hoạch khắc phục triệt để + lộ trình
Người chịu trách nhiệm	Họ tên, chức vụ, sđt, email

PHẦN VI

Lộ trình tuân thủ 90 ngày

11. Roadmap chi tiết

Lộ trình thực tế áp dụng cho doanh nghiệp vừa và nhỏ đang triển khai 2-5 hệ thống AI:

Tuần 1-2 - Kiểm kê

1 **Liệt kê tất cả hệ thống AI đang dùng**

Phối hợp giữa Pháp chế + IT + các phòng ban. Lập danh sách: tên, mục đích, người dùng, dữ liệu đầu vào, nhà cung cấp.

Kết quả: File Excel danh sách AI inventory.

Tuần 3-4 - Phân loại

2 **Tự phân loại 4 mức rủi ro**

Sử dụng Checklist 12 câu (mục 4 cẩm nang này) cho từng hệ thống. Đối chiếu với Công cụ phân loại tự động trên Cổng AI khi có.

Kết quả: Bảng phân loại rủi ro với đầy đủ căn cứ.

Tuần 5-8 - Lập hồ sơ và triển khai HITL

3 **Lập Hồ sơ phân loại rủi ro**

Áp dụng cho AI rủi ro trung bình + cao. Sử dụng mẫu trong cẩm nang. Tích hợp DPIA nếu đã có.

Kết quả: Bộ Hồ sơ điện tử + lưu trữ trong hệ thống quản lý tài liệu nội bộ.

4 **Thiết lập quy trình HITL**

Áp dụng cho AI rủi ro cao. Phân công người giám sát, viết SOP, cài đặt cơ chế chuyển review tự động.

Kết quả: Quy trình HITL được phê duyệt + đào tạo người giám sát.

Tuần 9-12 - Thông báo và diễn tập

5 Thông báo trên Cổng AI

Khi Cổng vận hành, đăng ký tài khoản doanh nghiệp, kê khai từng hệ thống AI rủi ro trung bình + cao.

Kết quả: Mã định danh cho mỗi hệ thống AI.

6 Diễn tập báo cáo sự cố

Chạy tabletop exercise giả định sự cố AI nghiêm trọng. Đảm bảo quy trình báo cáo trong 48h hoạt động trơn tru.

Kết quả: Báo cáo diễn tập + cải tiến quy trình.

Bảng RACI - phân vai trong tuân thủ

Hoạt động	CEO	CTO/IT	Pháp chế	HR	Kế toán
Phê duyệt chính sách AI	R	C	C	I	I
Kiểm kê hệ thống AI	I	R	C	C	C
Phân loại rủi ro	I	R	A	I	I
Lập Hồ sơ Điều 12	I	C	R	I	I
Thông báo Cổng AI	I	C	R	I	I
HITL vận hành hàng ngày	I	R	I	C	C
Báo cáo sự cố	A	R	R	C	I

R = Responsible (Thực hiện); A = Accountable (Chịu trách nhiệm); C = Consulted (Tham vấn); I = Informed (Được thông báo)

PHẦN VII

Câu hỏi thường gặp

12. FAQ - 20 câu hỏi điển hình

1. Doanh nghiệp dùng ChatGPT để viết content có cần thông báo trên Cổng AI không?

Không. Khi doanh nghiệp là **người sử dụng cuối** (chỉ dùng cho công việc nội bộ, không tái cung cấp ChatGPT cho khách hàng), không thuộc nhóm phải thông báo. Tuy nhiên nếu nội dung do ChatGPT tạo được dùng để tương tác với khách hàng (chatbot, content marketing tự động), nên xem xét phân loại rủi ro trung bình.

2. Hộ kinh doanh nhỏ có phải tuân thủ Luật AI không?

Có. Luật AI và NĐ 142/2026 áp dụng cho cả tổ chức và cá nhân, không loại trừ theo quy mô. Tuy nhiên hầu hết hộ kinh doanh dùng AI ở mức rủi ro thấp / trung bình, nên nghĩa vụ tuân thủ rất nhẹ - chỉ cần lưu thông tin về hệ thống AI nội bộ.

3. AI nội bộ chỉ nhân viên dùng có khác biệt gì so với AI hướng đến khách hàng?

Có. AI nội bộ thường thuộc rủi ro thấp hơn vì người dùng (nhân viên) đã được đào tạo và có cơ chế giám sát công việc. Nhưng nếu AI nội bộ ra quyết định ảnh hưởng đến khách hàng (cho vay, tuyển dụng, dịch vụ), vẫn phải tuân thủ như AI hướng khách hàng.

4. Doanh nghiệp dùng AI bên thứ ba (OpenAI, Google, Anthropic) - ai chịu trách nhiệm?

Doanh nghiệp triển khai chịu trách nhiệm với người dùng cuối. OpenAI/Google/Anthropic là nhà phát triển - cung cấp mô hình. Doanh nghiệp là **bên triển khai** - phải lập hồ sơ phân loại rủi ro, thông báo Cổng AI, đảm bảo HITL nếu rủi ro cao.

5. Làm gì khi nhà cung cấp AI bên thứ ba không cho thông tin về mô hình?

Khoản 3 Điều 12 NĐ 142/2026 cho phép - khi phát triển trên nền tảng AI bên thứ ba, nhà cung cấp **chỉ phải cung cấp thông tin kỹ thuật và dữ liệu trong phạm vi quyền tiếp cận và kiểm soát hợp pháp của mình**. Doanh nghiệp không phải tiết lộ thông tin bên thứ ba không công khai.

6. Cụm liên kết AI là gì, lợi gì, đăng ký thế nào?

Cụm liên kết AI là tổ chức tự nguyện giữa **doanh nghiệp + cơ sở nghiên cứu / đại học + tổ chức hỗ trợ đổi mới sáng tạo** hợp tác phát triển AI. Lợi: ưu tiên tiếp cận hạ tầng AI quốc gia, dữ liệu dùng chung, chương trình hỗ trợ ngân sách. Đăng ký qua Cổng dịch vụ công quốc gia, thẩm định trong 15 ngày làm việc.

7. Phiếu hỗ trợ AI dùng được vào việc gì?

Phiếu hỗ trợ AI là chứng từ điện tử ghi nhận hạn mức kinh phí từ Quỹ Phát triển AI Quốc gia, dùng thanh toán: hạ tầng tính toán (server, GPU), dữ liệu dùng chung, mô hình ngôn ngữ lớn tiếng Việt, dịch vụ tư vấn - đào tạo. Đối tượng: doanh nghiệp khởi nghiệp sáng tạo, doanh nghiệp nhỏ và vừa, tổ chức KH&CN có dự án AI.

8. Có thể đăng ký Sandbox AI cho ý tưởng chưa thương mại hoá không?

Có. Cơ chế Sandbox dành cho **thử nghiệm có kiểm soát** - phù hợp với startup AI muốn thử nghiệm trong phạm vi giới hạn trước khi thương mại hoá. Tổ chức tham gia sandbox được điều chỉnh nghĩa vụ tuân thủ, có cơ chế hỗ trợ kỹ thuật và pháp lý.

9. Doanh nghiệp đã có hồ sơ DPIA theo NĐ 13/2023 thì có cần lập hồ sơ AI riêng không?

Không cần lập 2 hồ sơ riêng biệt. Khoản 7 Điều 12 NĐ 142/2026 cho phép sử dụng Hồ sơ DPIA để **thay thế hoặc tích hợp** làm thành phần của Hồ sơ phân loại rủi ro AI. Cần bổ sung các nội dung đặc thù về AI (kiến trúc, mô hình, mã định danh).

10. AI nhận diện khuôn mặt cho hệ thống chấm công nội bộ - rủi ro cao hay trung bình?

Rủi ro cao. AI sinh trắc học mặc định thuộc nhóm rủi ro cao theo phụ lục Luật AI, dù là sử dụng nội bộ. Phải lập hồ sơ đầy đủ, đánh giá phù hợp, có HITL khi quyết định bất thường.

11. Mức xử phạt khi không tuân thủ là bao nhiêu?

Hiện chưa có Nghị định xử phạt riêng cho lĩnh vực AI. Tạm thời áp dụng Nghị định 15/2020/NĐ-CP về xử phạt hành chính trong lĩnh vực bưu chính, viễn thông, công nghệ thông tin. Dự thảo Nghị định xử phạt vi phạm AI đang được Bộ KH&CN xây dựng với mức phạt đề xuất 1-5% doanh thu năm liền kề.

12. Có phải đào tạo nhân viên về AI không?

Khuyến nghị nhưng không bắt buộc. Tuy nhiên với AI rủi ro cao, người giám sát (HITL) phải có đủ năng lực chuyên môn để can thiệp. Đào tạo định kỳ là biện pháp tốt nhất để chứng minh tuân thủ.

13. AI dịch tự động (Google Translate API) cho website đa ngôn ngữ có thuộc rủi ro?

Rủi ro **trung bình**. Có tương tác với người dùng cuối, tạo nội dung công khai. Lập hồ sơ đơn giản + thông báo Cổng AI. Không cần HITL bắt buộc trừ khi nội dung dịch ảnh hưởng đến quyết định pháp lý.

14. Doanh nghiệp nước ngoài cung cấp dịch vụ AI tại Việt Nam có phải tuân thủ?

Có. Khoản 2 Điều 2 NĐ 142/2026 áp dụng cho "tổ chức, cá nhân nước ngoài tham gia vào hoạt động AI tại Việt Nam". Phải có đại diện pháp lý tại Việt Nam hoặc liên kết với đối tác nội địa.

15. Nội dung do AI tạo ra có cần gắn nhãn không?

Có, theo Điều 11 NĐ 142/2026. Nội dung do AI tạo ra (deepfake, AI generated text/image/video) có khả năng gây nhầm lẫn phải được gắn nhãn rõ ràng. Hình thức gắn nhãn theo hướng dẫn của Bộ KH&CN.

16. Có thể outsource toàn bộ tuân thủ Luật AI cho công ty tư vấn không?

Có thể outsource thực hiện, nhưng **trách nhiệm pháp lý vẫn thuộc về doanh nghiệp**. Hợp đồng tư vấn nên quy định rõ phạm vi, kết quả bàn giao và trách nhiệm chuyên môn của bên tư vấn.

17. Ngân sách dự kiến cho tuân thủ Luật AI ở SME là bao nhiêu?

Tùy quy mô và số lượng hệ thống AI. Ước tính cho SME 50-200 nhân viên có 2-5 hệ thống AI: **20-50 triệu VND** ban đầu (lập hồ sơ, thiết lập HITL, đào tạo) + **3-5 triệu VND/tháng** duy trì (vận hành HITL, báo cáo định kỳ).

18. AI vận hành nội bộ (RPA, AI tự động hóa) có thuộc phạm vi không?

Có. RPA / AI tự động hóa được coi là hệ thống AI theo Điều 3 Luật AI. Tuy nhiên hầu hết thuộc rủi ro **không đáng kể** nếu chỉ vận hành nội bộ, không quyết định ảnh hưởng đến cá nhân.

19. Doanh nghiệp đã đăng ký Cổng AI, sau đó hệ thống AI ngừng vận hành - cần báo lại không?

Có. Phải thông báo dừng hoạt động qua Cổng AI để cập nhật trạng thái mã định danh. Hồ sơ phân loại rủi ro vẫn lưu trữ tối thiểu 2 năm sau khi ngừng vận hành.

20. ILED có dịch vụ tư vấn tuân thủ Luật AI không?

Có. Phòng Tư vấn ILED hỗ trợ rà soát hệ thống AI, lập Hồ sơ phân loại rủi ro, thiết lập quy trình HITL, đào tạo nhân sự pháp chế. Liên hệ Hotline 091 847 6556 hoặc email **daotao@phapluatgiaoduc.org.vn**.

PHẦN VIII

Phụ lục

13. Bảng đối chiếu nghĩa vụ theo vai trò

Nghĩa vụ	Nhà phát triển	Nhà cung cấp	Bên triển khai	Người sử dụng
Lập Hồ sơ phân loại rủi ro	★★★	★★★	★★	-
Đánh giá phù hợp (rủi ro cao)	★★★	★★★	★	-
Thông báo Cổng AI	★★	★★★	★★	-
HITL vận hành	★	★★	★★★	★
Báo cáo sự cố	★★★	★★★	★★★	-
Lưu nhật ký	★★	★★	★★★	-
Bảo mật dữ liệu	★★★	★★★	★★★	★★

★★★ = Bắt buộc hoàn toàn; ★★ = Bắt buộc một phần; ★ = Khuyến nghị; - = Không áp dụng

14. Email template - Báo cáo sự cố

```
Kính gửi: Bộ Khoa học và Công nghệ
          Cục Quản lý Hệ thống Trí tuệ Nhân tạo

V/v: Báo cáo sự cố hệ thống trí tuệ nhân tạo
     Mã hệ thống: VN-AI-2026-XXXXXX

[Tên doanh nghiệp] kính báo cáo sự cố hệ thống AI sau:

1. Mã định danh hệ thống: VN-AI-2026-XXXXXX
2. Thời điểm phát hiện: ___/___/2026 lúc ___:___
3. Mô tả sự cố:
   [Tóm tắt 2-3 câu]

4. Mức độ ảnh hưởng:
   - Số người bị ảnh hưởng: ___
```

```
   - Thiệt hại tài chính ước tính: ___
   - Dữ liệu cá nhân bị ảnh hưởng: [có/không]

5. Biện pháp khắc phục đã thực hiện:
   [Liệt kê hành động]

6. Biện pháp dự kiến + lộ trình:
   [Kế hoạch tiếp theo]

7. Người chịu trách nhiệm:
   - Họ tên: ___
   - Chức vụ: ___
   - Sđt: ___
   - Email: ___

Trân trọng,
[Người đại diện pháp luật]
[Tên doanh nghiệp]
[Ngày báo cáo]
```

15. Liên hệ ILED

Cẩm nang này được biên soạn bởi **Ban Đào tạo ILED** với chuyên môn pháp lý của **LG. Trương Hữu Hiệp - Phó Viện trưởng Luật học**.

Doanh nghiệp cần hỗ trợ chuyên sâu, soạn thảo Hồ sơ tuân thủ AI cụ thể, hoặc đào tạo nhân sự pháp chế về AI - vui lòng liên hệ:

Hotline: **091 847 6556**

Email: **daotao@phapluatgiaoduc.org.vn**

Website: viennghiencuuphapluat.com.vn

Trụ sở chính: L17-11, Tầng 17, Tòa nhà Vincom, 72 Lê Thánh Tôn, Phường Sài Gòn, TP.HCM

Cảm ơn anh chị đã đọc

ILED hy vọng cẩm nang này giúp doanh nghiệp Việt Nam tự tin hơn trong việc triển khai AI một cách **an toàn, có trách nhiệm và đúng pháp luật**.

Phụ trách Nghiên cứu Pháp luật:	LG. Trương Hữu Hiệp - Phó Viện trưởng Luật học
Đại diện pháp luật:	ThS. Nguyễn Văn Kính - Viện trưởng
Giấy CN ĐK:	613/ĐK-KHCN - Sở KH&CN TP.HCM
Ngày thành lập:	23/06/2025

Cẩm nang này được biên soạn dựa trên Luật Trí tuệ Nhân tạo số 134/2025/QH15 và Nghị định 142/2026/NĐ-CP có hiệu lực tại thời điểm phát hành. Nội dung mang tính chất hướng dẫn tham khảo, không thay thế tư vấn pháp lý chính thức từ luật sư hoặc tổ chức hành nghề pháp luật. Doanh nghiệp nên đối chiếu với văn bản pháp luật cập nhật nhất và liên hệ chuyên gia pháp lý trước khi áp dụng vào trường hợp cụ thể.