

LIVE
WEBINAR

O FUTURO DA IA

Inovar com Ética. Regular
com Responsabilidade



28 SET '26



15:00-17:00



YOUTUBE



IAPMEI 50 ANOS

academia de
pme



AI Act: da regulamentação à prática

Modelo operacional e plano de execução para a governação de IA nas organizações

REGULAMENTO (UE) 2024/1689

28 DE SETEMBRO DE 2026



Entrada em vigor: o calendário de implementação

Aplicação faseada do Regulamento com marcos críticos até 2027

1 ago 2024

Entrada em vigor

O Regulamento (UE) 2024/1689 entra em vigor. A aplicação é faseada e não acontece toda no mesmo dia — a organização já tem trabalho a fazer desde este marco.

 MARCO INICIAL

2 fev 2025

Proibições e literacia

Começam a aplicar-se as proibições de práticas de risco inaceitável e a obrigação de literacia em IA para todas as organizações abrangidas.

 RISCO INACEITÁVEL

2 ago 2025

Obrigações GPAI

Aplicam-se as obrigações para modelos de IA de finalidade geral (GPAI), com regras adicionais para modelos com risco sistémico.

 MODELOS FUNDACIONAIS

2 ago 2026

Aplicação geral

Aplicação geral das regras, incluindo transparência e governação/enforcement, com as exceções previstas no regulamento.

 REGIME PLENO

2 dez 2027

Alto risco — categorias específicas

Para sistemas de alto risco, a Comissão Europeia indica marcos específicos para 2027, incluindo 2 de dezembro de 2027 para determinadas categorias, após alterações de implementação. O calendário deve ser acompanhado com atenção.

 ALTO RISCO

Acompanhamento contínuo

Calendário por obrigação e papel

A mensagem prática: criar um calendário de compliance por obrigação e por papel, não um único «prazo AI Act». Sublinhe a diferença entre «entrada em vigor» e «aplicação» — a organização já tem trabalho a fazer mesmo antes dos prazos futuros.

 PLANEAMENTO

 Mensagem-chave: a aplicação do AI Act é faseada — cada obrigação tem o seu próprio marco. O trabalho de conformidade começa já, não no prazo final.

Âmbito de aplicação: quem está abrangido?

Definição dos papéis na cadeia de valor, incluindo fornecedores, utilizadores e importadores, bem como as exceções previstas.



Papéis na cadeia de valor da IA



Fornecedores / provedores

Desenvolvem ou colocam no mercado sistemas ou modelos de IA, assumindo a responsabilidade primária pela conformidade.



Responsáveis pela implementação

Utilizam sistemas de IA, incluindo empresas que os aplicam internamente ou em serviços ao cliente — os chamados deployers.



Importadores e distribuidores

Colocam no mercado europeu sistemas de IA desenvolvidos noutros países, verificando a conformidade antes da distribuição.



Fabricantes de produtos

Integram sistemas de IA em produtos próprios, passando a responder pelas obrigações do regulamento nessa integração.



Entidades públicas e organizações fora da UE

Prestadores de serviços essenciais e organizações que usam IA em contextos regulados estão abrangidos. Organizações fora da UE ficam sujeitas quando colocam sistemas no mercado europeu ou quando o resultado produzido pelo sistema é utilizado na UE.



Mensagem-chave: a pergunta não é apenas “temos IA?”. É “qual é o nosso papel na cadeia de valor e onde ocorre o impacto?”.



Fora do perímetro ou tratamento distinto



Investigação e desenvolvimento

Antes da colocação no mercado: atividades de investigação, testes e desenvolvimento ficam fora do âmbito, em determinadas condições.



Defesa e segurança nacional

Usos militares, de defesa e segurança nacional ficam fora do perímetro do regulamento.



Risco mínimo ou inexistente

Sem obrigações específicas do AI Act, embora a legislação horizontal — como RGPD, setorial ou de defesa do consumidor — continue a aplicar-se integralmente.

Pergunta decisiva: não basta saber se a organização tem IA. É preciso identificar o papel na cadeia de valor e o local onde ocorre o impacto.

A lógica do regulamento: quatro níveis de risco

A classificação centra-se no caso de uso, não apenas na tecnologia ou no fornecedor.

1

Risco inaceitável — práticas proibidas

Utilizações que distorcem o comportamento, exploram vulnerabilidades ou permitem scoring social por autoridades públicas. Não podem avançar, em nenhuma circunstância.

Ex.: manipulação subliminar, certas formas de identificação biométrica remota em espaços públicos.

2

Alto risco — requisitos robustos antes e depois

Sistemas sujeitos a obrigações rigorosas: gestão de risco, qualidade de dados, supervisão humana, documentação técnica e monitorização pós-mercado.

Ex.: recrutamento, crédito, acesso a serviços essenciais ou infraestruturas críticas, dependendo do caso de uso.

3

Risco de transparência — informar e sinalizar

As pessoas devem saber quando interagem com uma máquina e quando o conteúdo é gerado ou manipulado por IA. Aplicam-se deveres de disclosure no produto e na jornada do utilizador.

Ex.: chatbot de atendimento, deepfakes e conteúdos sintéticos identificáveis.

4

Risco mínimo ou inexistente — sem novas obrigações

Sem obrigações específicas do AI Act, mas sujeito a boas práticas e à legislação horizontal aplicável. A conformidade continua a ser exigida noutros planos.

Ex.: filtro de spam ou sistema simples de recomendação.



Mensagem-chave: classificar o caso de uso é o primeiro controlo; classificar apenas a tecnologia ou o fornecedor é insuficiente.

Práticas de IA proibidas

Utilizações banidas: manipulação, exploração, scoring social e vigilância intrusiva



Manipulação & técnicas subliminares

Distorção material do comportamento de uma pessoa
Exploração de vulnerabilidades de grupos vulneráveis
Práticas que causam dano significativo e previsível



Exploração de vulnerabilidades

Idade, deficiência ou situação social/financeira específica
Distorção do comportamento com dano potencial
Práticas dirigidas a grupos em posição de fragilidade



Social scoring (autoridades públicas)

Avaliação ou classificação de pessoas com base em comportamento social
Tratamento prejudicial sem relação com os dados originais
Proibição absoluta independente do setor



Identificação biométrica remota

Em tempo real em espaços públicos para fins de aplicação da lei, salvo exceções muito limitadas.



Reconhecimento de emoções

Em contexto laboral e educativo, exceto por motivos médicos ou de segurança (limites restritos).



Categorização biométrica & bases de dados

Categorização biométrica para inferir características sensíveis
Recolha indiscriminada de imagens faciais (raspagem) para expandir bases de reconhecimento
Pontuação de risco de criminalidade baseada em perfis ou traços de personalidade



Obrigação transversal

A organização deve demonstrar que identificou e bloqueou usos proibidos, incluindo usos “experimentais” ou adquiridos a terceiros. Não basta uma declaração de intenção — é necessária uma lista clara de usos que não podem avançar.

⊘ **Antes de discutir controlos sofisticados, é preciso ter uma lista clara de usos que não podem avançar.**

Sistemas de alto risco: obrigações operacionais

Requisitos rigorosos para fornecedores e utilizadores, abrangendo gestão de risco, qualidade de dados, documentação técnica, supervisão humana e avaliações de impacto sobre direitos fundamentais.



FORNECEDORES

Obrigações antes e depois da colocação



Sistema de gestão de risco ao longo de todo o ciclo de vida do sistema.



Qualidade e governação dos dados, com controlos de relevância, representatividade e enviesamento.



Documentação técnica completa e registos/logs de funcionamento.



Informação e instruções claras para os responsáveis pela implementação.



Supervisão humana efetiva ao longo da operação.



Precisão, robustez e cibersegurança como requisitos técnicos base.



Avaliação de conformidade, declaração de conformidade e marcação CE quando aplicável.



Monitorização pós-mercado e reporte de incidentes graves.



UTILIZADORES / DEPLOYERS

Responsabilidades na operação diária



Utilizar o sistema de acordo com as instruções fornecidas pelo fornecedor.



Atribuir responsabilidade e garantir supervisão humana adequada.



Monitorizar o funcionamento e registar incidentes relevantes.



Manter logs quando estiverem sob o seu controlo.



Realizar avaliação de impacto sobre direitos fundamentais quando aplicável.



Informar trabalhadores e, em certos contextos, pessoas afetadas.



Não usar outputs como única base de decisões críticas sem salvaguardas adequadas.



Exigência de evidência operacional

O alto risco exige políticas, registos, testes, responsáveis nomeados e capacidade de intervenção — não apenas uma declaração de intenção.

IA de finalidade geral e deveres de transparência

Regras para modelos GPAI e sinalização de conteúdos gerados ou manipulados por IA

Modelos de finalidade geral (GPAI)

-  **Documentação técnica** e informação para integradores e downstream providers.
-  **Política de direitos de autor** obrigatória para os fornecedores.
-  **Resumo público** do conteúdo usado no treino, nos termos aplicáveis.
-  **Risco sistémico:** avaliação, mitigação e reporte reforçados.

Transparência

-  As pessoas sabem quando **interagem com uma máquina**, quando não é óbvio.
-  Conteúdos gerados ou manipulados por IA devem ser **identificáveis**.
-  **Deepfakes** e textos de interesse público claramente sinalizados.
-  **Disclosure no produto**, na jornada do utilizador e nos processos internos.

 **Mensagem-chave:** mesmo quem não desenvolve modelos fundacionais pode ser afetado como utilizador, integrador ou distribuidor de soluções GPAI.

Implementação do modelo operativo de governação

Três linhas de defesa e capacidades essenciais para integrar a conformidade na operação

Três linhas de defesa

1.ª linha — Produto & Negócio

Inventário de casos de uso, avaliação inicial, controlos no desenho e operação contínua.

2.ª linha — Jurídico, Compliance, Risco, Segurança & Privacidade

Classificação de risco, políticas, pareceres, testes e aprovação formal de novos usos.

3.ª linha — Auditoria Interna / Externa

Revisão independente do modelo, evidência de conformidade e melhoria contínua.

Capacidades mínimas a criar

Inventário vivo de sistemas e fornecedores de IA

Taxonomia de risco e critérios de escalamento

Aprovação prévia à compra, desenvolvimento ou produção

Biblioteca de evidências: contratos, fichas, logs, testes, incidentes

Canal de incidentes e mecanismo de suspensão / rollback

Formação e literacia em IA por função

Plano de ação: os próximos 90 dias

Roteiro pragmático para execução imediata: responsáveis, contratos, formação e incidentes

30

Saber onde estamos

DIAS



- Nomear sponsor executivo e owner operacional
- Lançar inventário de sistemas, modelos, fornecedores e casos de uso
- Identificar usos potencialmente proibidos e de alto risco
- Mapear dependências GPAL e fluxos de dados/conteúdo

60

Fechar lacunas críticas

DIAS



- Aprovar política de uso aceitável e critérios de classificação
- Rever contratos com fornecedores: documentação, logs, incidentes, auditoria, transparência e direitos de autor
- Definir controlos de supervisão humana, testes, monitorização e conservação de evidência
- Lançar formação dirigida a equipas técnicas, procurement, RH, jurídico e utilizadores

90

Operacionalizar e medir

DIAS



- Criar comité ou fórum de revisão de IA
- Colocar em produção o workflow de aprovação e o canal de incidentes
- Testar um caso de alto risco ou de transparência ponta a ponta
- Medir cobertura do inventário, % de casos classificados, fornecedores avaliados, incidentes e ações corretivas

MÉTRICAS DE SUCESSO

100%

Inventário de sistemas e modelos coberto

100%

Casos de uso classificados por nível de risco

≥90%

Fornecedores avaliados e contratos revistos

0

Incidentes sem ação corretiva documentada

✓ Evidência: registos de aprovação, logs, testes e atas de comité.

OBRIGADA

Pela participação.



IAPMEI 50 ANOS

academia de
pme