PRIVUS MONTH INSIGHTS · Nº 5 · NOVEMBRO 2026

# Da política à prova: a ISO/IEC 42001, a EN 18286 e a demonstração de conformidade com o AI Act

Como ligar governação de IA, processos de qualidade e evidências de cumprimento, preservando as exigências próprias do RGPD.

GOVERNAÇÃO DE IA · AI ACT · RGPD | LEITURA: 7 MINUTOS

A aprovação de uma política de inteligência artificial é uma decisão de governação. A capacidade de demonstrar como essa política condicionou o desenvolvimento, a aprovação e a alteração de um sistema revela a sua aplicação efetiva.

A diferença torna-se visível quando surge um problema. Quem autorizou a última atualização? Que testes sustentaram essa decisão? Como foram avaliados os riscos? A versão disponibilizada corresponde à versão validada?

É nesta passagem dos compromissos para processos verificáveis que a articulação entre a ISO/IEC 42001 e a EN 18286:2026 ganha relevância. Para os prestadores de sistemas de IA de risco elevado, permite aproximar a estrutura de gestão das exigências regulatórias e da evidência necessária para demonstrar o seu cumprimento.

## A obrigação de organizar e documentar

O artigo 17.º do AI Act exige que os prestadores de sistemas de IA de risco elevado disponham de um sistema de gestão da qualidade documentado. Abrange desenvolvimento, testes, gestão de dados e riscos, acompanhamento após a colocação no mercado, incidentes e responsabilidades. A sua implementação deve ser proporcionada à dimensão da organização, preservando o rigor exigido. [1]

O âmbito desta obrigação depende do papel da organização, da classificação do sistema e do calendário legal aplicável. Utilizar uma ferramenta de IA não transforma automaticamente uma empresa no prestador sujeito ao artigo 17.º.

A exigência tem, contudo, uma consequência operacional clara: a organização abrangida precisa de definir como trabalha, quem decide e que registos conserva.

O ciclo de vida situa essas decisões. O sistema é concebido, desenvolvido, testado, disponibilizado, acompanhado e alterado. A governação distribui responsabilidades ao longo dessas etapas. O sistema de gestão da qualidade organiza os processos e a documentação que permitem verificar o seu funcionamento.

## Da gestão da organização ao cumprimento regulatório

A ISO/IEC 42001 estabelece requisitos para um sistema de gestão de IA. Estrutura políticas, objetivos, responsabilidades, gestão de riscos, avaliação do desempenho e melhoria contínua. Aplica-se a organizações que desenvolvem, fornecem ou utilizam produtos e serviços com IA. [2]

A EN 18286:2026 é uma norma europeia desenvolvida pelo CEN e pelo CENELEC para apoiar o sistema de gestão da qualidade exigido pelo AI Act. Segundo a Comissão Europeia, centra-se no ciclo de vida dos sistemas e complementa referenciais existentes, incluindo a ISO/IEC 42001, a ISO 9001 e sistemas setoriais como a ISO 13485. [3]

A articulação permite aproveitar processos já estabelecidos: controlo documental, aprovação de alterações, auditoria, tratamento de falhas e revisão pela gestão.

O trabalho consiste em verificar se esses processos respondem às obrigações aplicáveis, identificar lacunas e definir as adaptações necessárias. Uma estrutura integrada pode reduzir duplicações, desde que preserve a identificação dos requisitos e das evidências correspondentes.

## Uma presunção delimitada

Em 19 de outubro de 2026, a Comissão Europeia anunciou a publicação da referência à EN 18286:2026 no Jornal Oficial da União Europeia. De acordo com essa comunicação, a aplicação da norma permite beneficiar de uma presunção de conformidade com os requisitos do artigo 17.º por ela abrangidos. [3]

O alcance deve ser lido com precisão. A presunção depende do cumprimento efetivo da norma no âmbito relevante e não se estende automaticamente às restantes obrigações do AI Act.

Comprar a norma, mencioná-la numa política ou declarar a sua adoção não demonstra a sua aplicação. A empresa precisa de conseguir relacionar os requisitos com os processos implementados e os registos produzidos.

A utilização de normas harmonizadas é, em princípio, voluntária. Quando segue outra solução, a organização continua responsável por demonstrar como satisfaz os requisitos legais pertinentes. [1]

## Presunção, certificação e avaliação da conformidade

Estes três conceitos têm funções distintas.

A certificação ISO/IEC 42001 é voluntária e permite uma avaliação independente do sistema de gestão face aos requisitos dessa norma. O seu alcance depende do âmbito certificado; não representa uma aprovação geral de todos os sistemas ou de todas as obrigações legais da organização. [2]

A presunção associada à EN 18286 resulta da aplicação de uma norma harmonizada no âmbito coberto. Não depende, por si só, da obtenção de um certificado voluntário.

Já a avaliação da conformidade segue o procedimento previsto no AI Act. Para os sistemas abrangidos pelos pontos 2 a 8 do anexo III, incluindo os de recrutamento do ponto 4, prevê-se controlo interno. Para determinados sistemas biométricos, a intervenção de um organismo notificado pode ser obrigatória nas condições do artigo 43.º. [1]

Uma consultora pode apoiar a implementação, auditar processos e preparar evidências. Essa intervenção não substitui a avaliação de um organismo notificado quando legalmente exigida.

## A documentação faz parte do cumprimento

Uma equipa pode testar atualizações e discutir riscos sem conservar resultados ou registar aprovações. Quando o artigo 17.º é aplicável, essa informalidade pode representar incumprimento da própria exigência de documentação.

Se o sistema de gestão obrigatório nem sequer existir, a falha é mais ampla. As consequências dependem da obrigação violada e das circunstâncias, podendo incluir medidas corretivas e sanções. O artigo 99.º prevê coimas para o incumprimento de obrigações dos prestadores, com critérios de graduação e regras específicas para PME. [1]

A responsabilidade decorre do incumprimento da lei. A norma técnica oferece uma via estruturada para cumprir e demonstrar.

Considere-se uma empresa que fornece uma ferramenta de recrutamento e altera a forma como os candidatos são ordenados. O processo deve permitir identificar a alteração, avaliar os seus efeitos, executar testes e fundamentar a aprovação.

A evidência liga essas etapas: os resultados correspondem à versão disponibilizada; a aprovação identifica os fundamentos; uma falha posterior desencadeia investigação e correção.

É esta relação entre **obrigação, processo, responsável e evidência** que permite reconstruir uma decisão e verificar se os controlos funcionaram.

## O RGPD mantém exigências próprias

Quando o sistema trata dados pessoais, a organização tem de analisar também o RGPD. Os artigos 5.º, n.º 2, e 24.º exigem responsabilidade pelo cumprimento e pela sua demonstração. Conforme o tratamento, estão em causa a base jurídica, a minimização, a transparência, a segurança e os direitos das pessoas. [4]

No exemplo do recrutamento, uma atualização pode exigir a revisão dos dados utilizados, das finalidades, dos acessos ou da informação prestada aos candidatos.

Essas verificações podem integrar um processo comum de gestão de alterações. A documentação deve, contudo, permitir reconhecer a obrigação a que cada avaliação responde.

**A presunção associada à EN 18286 no AI Act não se estende ao RGPD.** Também não existe equivalência automática entre os papéis de prestador e responsável pela implantação, por um lado, e responsável pelo tratamento e subcontratante, por outro.

A avaliação de impacto sobre a proteção de dados mantém igualmente a sua autonomia. O artigo 35.º do RGPD exige uma AIPD antes do tratamento quando este seja suscetível de implicar elevado risco para os direitos e liberdades. A classificação de risco elevado no AI Act não substitui essa análise. [4]

Existe uma ligação operacional expressa: o artigo 26.º do AI Act prevê que, quando aplicável, o responsável pela implantação utilize informação disponibilizada pelo prestador para cumprir a obrigação de realizar uma AIPD. [1]

A informação pode ser partilhada entre processos; as responsabilidades jurídicas permanecem identificadas.

## Uma continuidade com setembro

No Insight n.º 3, dedicado à continuidade de negócio, analisámos como a ISO 22301 e a ISO/IEC 27001 ajudam a organizar capacidades de disponibilidade, resiliência e recuperação relevantes para o artigo 32.º do RGPD. [6]

A linha mantém-se: transformar exigências jurídicas em capacidade operacional demonstrável.

A diferença está no efeito jurídico. As normas discutidas em setembro apoiam implementação e evidências relevantes, sem criarem uma presunção geral de conformidade com o RGPD. A EN 18286 acrescenta uma presunção delimitada no contexto do AI Act.

### Para qualquer Conselho de Administração

As perguntas são concretas:

**01.** A organização identificou os seus sistemas de IA, os papéis que assume e as obrigações aplicáveis?

**02.** Cada obrigação tem um processo e um responsável definidos?

**03.** Uma alteração pode ser relacionada com os testes e a decisão que a autorizaram?

**04.** A documentação permite demonstrar separadamente o cumprimento do AI Act e do RGPD?

A maturidade da governação revela-se na capacidade de responder com evidências consistentes, atualizadas e acessíveis.

Para a empresa, isso significa maior controlo sobre alterações, menor dependência da memória individual e melhores condições para responder a clientes, parceiros e autoridades.

## A evidência é a alma do compliance.

### Fontes e referências

**[1]** Regulamento (UE) 2024/1689, AI Act, versão consolidada. Designadamente artigos 17.°, 26.°, 40.°, 43.° e 99.°; âmbito e calendário de aplicação devem ser verificados no caso concreto.

**[2]** ISO, ISO/IEC 42001:2023, Artificial intelligence - Management system. Consultar também a explicação da ISO sobre implementação e certificação voluntária.

**[3]** Comissão Europeia, First harmonised standard supporting the AI Act published in the Official Journal. 19 de outubro de 2026. Publicação da referência à EN 18286:2026 e alcance da presunção de conformidade.

**[4]** Regulamento (UE) 2016/679, RGPD. Designadamente artigos 5.°, 24.°, 32.° e 35.°.

**[5]** BSI, apresentação e âmbito da EN 18286:2026. Descrição pública do âmbito da norma e da sua relação com outros sistemas de gestão.

**[6]** Privus Month Insights n.° 3, Continuidade de negócio: a obrigação que o RGPD pressupõe e a ISO 22301 formaliza. Setembro de 2026.

Conteúdo informativo e geral. Não constitui parecer jurídico, auditoria, certificação ou recomendação aplicável sem análise do contexto concreto.