Checklist de governance de IA para PME

Vinte pontos em cinco blocos. Cada ponto tem resposta sim/não e um dono. **[lei]** = obrigação legal para todas as PME que usam IA (AI Act, RGPD); **[NIS2]** = só para empresas em âmbito do DL n.º 125/2025. Versão de 26 de novembro de 2026 · HeraPrime.

A. Inventário e alternativa

#	Ponto	Sim	Não	Dono
1	Lista das ferramentas de IA em uso, por área, com tipo de conta (pessoal/empresa) e tipo de dados tratados.	☐	☐	
2	Ficha por ferramenta autorizada: treino? retenção? subcontratação (RGPD art. 28.º)? acesso humano do fornecedor?	☐	☐	
3	Alternativa com contrato para escrita e resumo, acessível com a conta de trabalho.	☐	☐	
4	Ferramentas de consumo com treino ligado por defeito bloqueadas ou sinalizadas (desligar «Improve the model for everyone»).	☐	☐	

B. Dados e permissões

#	Ponto	Sim	Não	Dono
5	Pastas de RH, financeiro, jurídico e dados de clientes com dono e revisão trimestral de acessos.	☐	☐	
6	Etiquetas de sensibilidade nos documentos críticos e política de DLP que cobre o Copilot.	☐	☐	
7	Grupos e canais «para toda a empresa» revistos; os desnecessários fechados.	☐	☐	
8	Regra escrita do que nunca se cola numa IA sem contrato: saúde, dados bancários de terceiros, vencimentos, menores, segredos comerciais.	☐	☐	

C. Processos críticos e agentes

#	Ponto	Sim	Não	Dono
9	Processos em que a IA só propõe e uma pessoa decide (recrutamento, crédito, contabilização, disciplina laboral), com registo de quem decidiu. [lei · alto risco a partir de 2-dez-2027]	☐	☐	
10	Agentes com permissões mínimas; ações irreversíveis (enviar, pagar, apagar, alterar fornecedores) com confirmação humana.	☐	☐	
11	Conteúdo externo tratado como dados e nunca como instruções; teste de prompt injection antes de ligar um agente à produção.	☐	☐	

12	Tudo o que sai para fora da empresa com IA passa por revisão humana nomeada.	☐	☐	

D. Pessoas e lei

#	Ponto	Sim	Não	Dono
13	Formação em IA adaptada às funções, com registo de presenças e conteúdos. [lei · AI Act art. 4.º]	☐	☐	
14	Quem interage com uma IA da empresa é informado; conteúdo gerado está identificado. [lei · AI Act art. 50.º, desde 2-ago-2026]	☐	☐	
15	A gerência participou na formação e aprovou a política. [NIS2 · arts. 25.º e 27.º RJC]	☐	☐	
16	Canal simples para «posso usar isto?» com resposta em 48 horas.	☐	☐	

E. Registo, incidentes e revisão

#	Ponto	Sim	Não	Dono
17	Uso das ferramentas autorizadas registado por utilizador e pesquisável em incidente.	☐	☐	
18	Procedimento «colei o que não devia»: quem avisar, o que apagar, quando comunicar. [lei · RGPD art. 33.º, 72 h]	☐	☐	
19	Avaliada a necessidade de avaliação de impacto para usos de IA com dados pessoais em escala ou decisões com efeitos nas pessoas. [lei · RGPD art. 35.º]	☐	☐	
20	Política com data de revisão (máximo anual) e dono nomeado.	☐	☐	

Fontes: Regulamento (UE) 2024/1689 (AI Act), arts. 4.º, 50.º e 113.º; Regulamento (UE) 2026/1744 (Digital Omnibus on AI, em vigor desde 27-jul-2026); RGPD arts. 28.º, 33.º e 35.º; Decreto-Lei n.º 125/2025 (RJC arts. 25.º e 27.º); OWASP Top 10 for LLM Applications 2025 (LLM01); Microsoft Learn, «Enterprise data protection in Microsoft Copilot»; OpenAI Help Center, «How your data is used to improve model performance» e «Data controls FAQ». Esta checklist é orientação prática, não aconselhamento jurídico. heraprime.com