					Insira aqui a designação da entidade jurídica registada							
Número do documento: PII21					Título do documento: **Política de privacidade para IA e decisões automatizadas**							
Versão: 1.0		Data de entrada em vigor: 01.01.2025			Proprietário do documento:							
X	Política		Norma		Procedimento		Formulário		Registo		Outro	

Histórico de revisões				
Número da revisão	**Data da revisão**	**Alterações**	**Revisto por**	**Proprietário do processo**

Aprovações			
Nome	**Cargo**	**Data**	**Assinatura**

Alinhada com normas e regulamentos

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Informação documentada e controlo operacional para evidência de tratamento por IA, definição de perfis e decisões automatizadas
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitorização, não conformidade e ação corretiva para controlos de privacidade em IA
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9	Controller	Primary	Finalidade, fundamento de licitude, avaliação de impacto sobre a privacidade e registos do responsável pelo tratamento
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Contratos de subcontratantes e responsabilidades de responsáveis conjuntos pelo tratamento para tratamento de PII relacionado com IA
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4	Controller	Primary	Obrigações perante titulares dos dados e transparência para tratamento relacionado com IA
ISO/IEC 27701:2025	Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11	Controller	Primary	Obrigações relativas a oposição, acesso, retificação, apagamento, tratamento de pedidos e decisões automatizadas

ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5	Controller	Primary	Limites de recolha, tratamento e minimização para entradas, saídas e dados derivados de IA
ISO/IEC 27701:2025	Annex A.1.5.2; Annex A.1.5.3; Annex A.1.5.4; Annex A.1.5.5	Conditional	Supporting	Encaminhamento de transferências internacionais, divulgações e pedidos de divulgação de PII relacionados com IA
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7	Processor	Primary	Acordo com subcontratante, instruções documentadas, apoio às obrigações do cliente e registos
ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.5.2; Annex A.2.5.3; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Apoio do subcontratante a obrigações perante titulares, encaminhamento de transferências e tratamento de divulgações
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Proteção de registos e logging relacionados com o tratamento de PII por IA
GDPR	Article 4(4); Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(d); Article 5(2)	Controller	Primary	Definição de perfis, equidade, transparência, limitação da finalidade, minimização, exatidão e responsabilização
GDPR	Article 6; Article 9; Article 10	Controller	Primary	Licitude, dados de categorias especiais e salvaguardas para dados de condenações penais ou infrações

GDPR	Article 12; Article 13; Article 14; Article 15	Controller	Primary	Informações transparentes, acesso e informações significativas sobre decisões automatizadas
GDPR	Article 16; Article 17; Article 18; Article 21; Article 22	Controller	Primary	Direitos de retificação, apagamento, limitação, oposição e decisões automatizadas
GDPR	Article 24; Article 25; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Responsabilidade do responsável pelo tratamento, conceção/por defeito, responsáveis conjuntos, subcontratantes, registos, segurança, DPIA e tarefas do DPO
GDPR	Article 44	Conditional	Referenced	Encaminhamento de transferências internacionais para tratamento de PII relacionado com IA
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.7	Both	Primary	Princípios de finalidade, recolha, minimização, utilização, retenção, divulgação, exatidão e qualidade
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Transparência, participação individual, responsabilização, segurança da informação e cumprimento da privacidade
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2; Clause 6.3	Both	Supporting	Benefício da PIA, determinação de limiar e preparação para avaliação de riscos de

				privacidade relacionada com IA
ISO/IEC 29151:2022	Annex A.4; Annex A.5; Annex A.7; Annex A.8; Annex A.10	Both	Supporting	Controlos de finalidade, recolha, minimização, utilização, retenção, divulgação, exatidão e participação do titular

1. Âmbito

1.1 Esta política define requisitos obrigatórios de privacidade para atividades de tratamento por inteligência artificial, definição de perfis, pontuação, recomendação, apoio à decisão e decisões automatizadas que utilizem, infiram, gerem, divulguem ou de outro modo tratem PII no âmbito do PIMS.

1.2 Esta política aplica-se ao seguinte:

1.2.1 sistemas, aplicações, modelos, serviços, fluxos de trabalho, motores de decisão, ferramentas de pontuação, sistemas de recomendação, modelos analíticos e processos de decisões automatizadas com recurso a IA que tratem PII;

1.2.2 definição de perfis, segmentação, classificação, previsão, inferência, personalização, ordenação, elegibilidade, deteção de fraude, pontuação de risco, decisões de acesso, avaliação relacionada com emprego, definição de perfis relativa a crianças, personalização de marketing e tratamento semelhante quando esteja envolvida PII;

1.2.3 PII relacionada com IA utilizada para treino, teste, validação, ajuste, monitorização, inferência em produção, revisão de saídas, medição de desempenho, investigação de incidentes ou retirada de serviço de modelos;

1.2.4 contextos de responsável pelo tratamento, responsável conjunto pelo tratamento, subcontratante e subcontratante subsequente;

1.2.5 fornecedores, subcontratantes, subcontratantes subsequentes, destinatários de partilha de dados e rotas de transferência internacional relacionados com IA que tratem PII.

1.3 Esta política não cria um quadro completo de governação de IA, sistema de gestão de IA, inventário de IA, inventário de modelos, registo de riscos de modelos, registo de equidade, registo de algoritmos, registo de incidentes de IA, comité de IA, função de proprietário do modelo, função de proprietário do sistema de IA, fluxo de trabalho de assessoria jurídica ou formulário de aprovação de IA separado.

1.4 Esta política não substitui o seguinte:

1.4.1 PII03 para inventário de tratamento, fundamento de licitude e propriedade do ROPA;

1.4.2 PII04 para governação de avisos de privacidade;

1.4.3 PII05 para consentimento e gestão de preferências;

1.4.4 PII06 para fluxo de trabalho de direitos dos titulares dos dados;

1.4.5 PII07 para metodologia de avaliação de riscos de privacidade e DPIA;

1.4.6 PII08 para gates de privacidade desde a conceção e por defeito;

1.4.7 PII09 para controlos de recolha, utilização, divulgação e partilha;

1.4.8 PII10 para execução de retenção, apagamento e eliminação;

1.4.9 PII11 para controlos de exatidão e qualidade;

1.4.10 PII12 para governação do ciclo de vida de subcontratantes, subcontratantes subsequentes e terceiros;

1.4.11 PII13 para controlos de transferências internacionais;

1.4.12 PII14 para segurança e controlo de acesso;

1.4.13 PII15 para tratamento de incidentes e violações;

1.4.14 PII18 para monitorização, auditoria e melhoria;

1.4.15 PII19 para privacidade dos trabalhadores;

1.4.16 PII20 para privacidade das crianças;

1.4.17 PII22 para privacidade em marketing e cookies.

2. Finalidade

2.1 A finalidade desta política é assegurar que as atividades de IA, definição de perfis e decisões automatizadas que envolvam PII sejam identificadas, documentadas, sujeitas a avaliação de risco, transparentes, contestáveis, monitorizadas e controladas através do PIMS, sem criar artefactos duplicados de governação específicos de IA.

2.2 Esta política assegura que as obrigações de privacidade para tratamento de PII relacionado com IA sejam evidenciadas através de REG02, REG04, REG06, REG07, REG08, REG09, REG10 e REG12.

3. Objetivos

3.1 Os objetivos desta política são:

3.1.1 identificar em REG02 o tratamento por IA, definição de perfis e decisões automatizadas que envolva PII;

3.1.2 documentar em REG02 as finalidades relacionadas com IA, fundamento de licitude, categorias de PII, fontes de dados, dados inferidos, saídas, destinatários e efeitos das decisões;

3.1.3 acionar a triagem de riscos de privacidade e o encaminhamento de DPIA através de REG04;

3.1.4 assegurar que os avisos de privacidade e informações significativas relacionados com IA sejam registados em REG07;

3.1.5 encaminhar pedidos relativos a direitos, oposição, revisão humana e possibilidade de contestação através de REG06;

3.1.6 controlar subcontratantes, subcontratantes subsequentes, fornecedores e acordos de partilha de dados relacionados com IA através de REG08;

3.1.7 encaminhar transferências internacionais relacionadas com IA através de REG09;

3.1.8 escalar incidentes suspeitos de PII relacionados com IA, utilização indevida, divulgação não autorizada e resultados adversos de privacidade através de REG10 e REG12;

3.1.9 registar monitorização, exceções, não conformidades, ações corretivas e melhorias em REG12.

4. Declarações da política

4.1 Identificação de IA, definição de perfis e decisões automatizadas

4.1.1 [Controller] Quando for proposto um sistema, aplicação, modelo, fluxo de trabalho, serviço ou processo de negócio novo ou materialmente alterado, o Process Owner / Business Owner deve determinar se utiliza IA, definição de perfis, pontuação, recomendação, apoio à decisão ou decisões automatizadas envolvendo PII e registar a determinação em REG02.

4.1.2 [Controller] Antes do início do tratamento de PII relacionado com IA, o Process Owner / Business Owner deve documentar em REG02 a finalidade do tratamento, categorias de PII, categorias de titulares dos dados, fontes de dados, categorias de dados inferidos ou derivados, categorias de saídas, categorias de destinatários, fundamento de licitude e ligação ao calendário de retenção.

4.1.3 [Controller] Antes de a definição de perfis, pontuação, recomendação, apoio à decisão ou decisões automatizadas ser utilizada em produção, o Process Owner / Business Owner deve documentar em REG02 e REG04 o contexto da decisão, o efeito esperado sobre os titulares dos dados, a intervenção humana e a via de exercício de direitos.

4.1.4 [Joint Controller] Antes de o tratamento de PII relacionado com IA ser realizado com um responsável conjunto pelo tratamento, o Privacy Lead / PIMS Manager deve documentar em REG08 a responsabilidade pela definição da finalidade, aviso, tratamento de direitos, apoio à DPIA, governação de subcontratantes e escalonamento de incidentes.

4.1.5 [Processor] Antes de tratar PII através de um serviço relacionado com IA para um cliente, o Process Owner / Business Owner deve confirmar que as instruções do cliente, finalidades permitidas, utilizações proibidas, tratamento de saídas e obrigações de assistência estão documentados em REG08.

4.1.6 [Both] Antes de ativar o tratamento de PII relacionado com IA, o Privacy Lead / PIMS Manager deve confirmar que o tratamento está ligado aos objetos de evidência canónicos aplicáveis e que não é criado qualquer registo específico de IA separado fora de REG02, REG04, REG06, REG07, REG08, REG09, REG10 ou REG12.

4.2 Avaliação de riscos de privacidade e encaminhamento de DPIA

4.2.1 [Controller] Antes de lançar ou alterar materialmente o tratamento de PII relacionado com IA, o Privacy Lead / PIMS Manager deve concluir a triagem de riscos de privacidade e registar a decisão de DPIA em REG04.

4.2.2 [Conditional] Quando o tratamento relacionado com IA envolver definição de perfis, decisões automatizadas, avaliação em grande escala, dados de categorias especiais, dados relativos a infrações penais, titulares dos dados vulneráveis, avaliação de trabalhadores, crianças, monitorização comportamental, dados de localização, dados biométricos, pontuação de alto impacto ou efeitos significativos, o Data Protection Officer / Privacy Advisor deve rever o risco de privacidade e registar o parecer em REG04.

4.2.3 [Controller] Antes da entrada em produção do tratamento de PII relacionado com IA, o Process Owner / Business Owner deve documentar ações de tratamento de riscos, estado do risco residual e evidência de prontidão para entrada em produção em REG04 ou REG12.

4.2.4 [Controller] Antes de a PII ser reutilizada para treino, teste, validação, ajuste, monitorização ou melhoria de modelos de IA para uma finalidade nova ou materialmente alterada, o Process Owner / Business Owner deve concluir a revisão de privacidade e registar a decisão em REG02 e REG04.

4.2.5 [Conditional] Quando o risco residual de privacidade se mantiver elevado após o tratamento planeado, Top Management deve aprovar, rejeitar ou exigir tratamento adicional antes da utilização em produção e registar a decisão em REG04 e REG12.

[... As secções 4.3–8 não estão incluídas nesta pré-visualização. Adquira o documento completo para aceder ao conteúdo integral. ...]

9. Exceções

9.1 [All] Antes de se desviar de um requisito de privacidade relacionado com IA nesta política, o Process Owner / Business Owner requerente deve submeter em REG12 a justificação da exceção e evidência de controlo compensatório.

9.2 [Conditional] Quando uma exceção afetar definição de perfis, decisões automatizadas, revisão humana, possibilidade de contestação, transparência, resultado de DPIA, pontuação de alto impacto, tratamento relativo a crianças, tratamento relativo a trabalhadores, restrições de subcontratantes ou transferências internacionais, o Data Protection Officer / Privacy Advisor deve rever a exceção e registar o parecer em REG04 ou REG12.

9.3 [Conditional] Quando uma exceção criar ou preservar risco residual de privacidade elevado, Top Management deve aprovar ou rejeitar a exceção e registar a decisão em REG04 e REG12.

9.4 [All] Antes de uma exceção de privacidade relacionada com IA aprovada expirar, o Privacy Lead / PIMS Manager deve rever o estado de encerramento, renovação ou ação corretiva e registar o resultado em REG12.

10. Aplicação

10.1 [All] Quando for identificado incumprimento desta política, o Privacy Lead / PIMS Manager deve registar a não conformidade e a ação corretiva em REG12.

10.2 [Both] Quando houver suspeita de tratamento, divulgação ou acesso não autorizado a PII relacionada com IA, utilização indevida de modelo, falha no tratamento de direitos ou resultado adverso de privacidade, o Incident Response Coordinator deve iniciar o escalonamento do incidente e registar evidência em REG10 e REG12.

10.3 [Both] Quando um subcontratante, subcontratante subsequente, fornecedor ou destinatário de partilha de dados não cumprir obrigações de privacidade relacionadas com IA, o Vendor / Procurement Owner deve registar a ação de remediação, escalonamento ou cessação em REG08 e REG12.

10.4 [All] Quando ocorrerem não conformidades de privacidade relacionadas com IA repetidas ou sistémicas, Top Management deve rever a questão e registar a ação da gestão em REG12.

11. Revisão e manutenção

11.1 [All] Pelo menos anualmente, o Privacy Lead / PIMS Manager deve rever esta política quanto à sua adequação contínua e registar o resultado da revisão em REG12.

11.2 [Conditional] Quando leis, serviços, modelos, fontes de dados, práticas de definição de perfis, lógica de decisões automatizadas, acordos com fornecedores, rotas de transferência ou riscos de privacidade sofrerem alteração material, o Privacy Lead / PIMS Manager deve rever os controlos de privacidade relacionados com IA afetados e registar o resultado em REG02, REG04 ou REG12.

11.3 [Controller] Pelo menos anualmente e após alterações materiais aos percursos de utilizador relacionados com IA, o Process Owner / Business Owner deve rever a evidência de transparência, informações significativas, revisão humana e via de exercício de direitos, e registar a revisão em REG06 e REG07.

11.4 [All] Após o encerramento de ações corretivas de privacidade relacionadas com IA, o Internal Audit / Compliance Reviewer deve verificar a eficácia e registar evidência da verificação em REG12.

12. Políticas relacionadas

12.1 PII01 - Política do sistema de gestão da informação de privacidade

12.2 PII02 - Política de papéis, responsabilidades e responsabilização em privacidade

12.3 PII03 - Política de inventário de tratamento de PII e fundamento de licitude

12.4 PII04 - Política de avisos de privacidade e transparência

12.5 PII05 - Política de consentimento e gestão de preferências

12.6 PII06 - Política de gestão dos direitos dos titulares dos dados

12.7 PII07 - Política de avaliação de riscos de privacidade e DPIA

12.8 PII08 - Política de privacidade desde a conceção e por defeito

12.9 PII09 - Política de recolha, utilização, divulgação e partilha de PII

12.10 PII10 - Política de retenção, apagamento e eliminação de PII

12.11 PII11 - Política de exatidão e qualidade de PII

12.12 PII12 - Política de gestão da privacidade de subcontratantes, subcontratantes subsequentes e terceiros

12.13 PII13 - Política de transferência internacional de PII

12.14 PII14 - Política de segurança e controlo de acesso de PII

12.15 PII15 - Política de gestão de incidentes e violações de PII

12.16 PII17 - Política de informação documentada e gestão de evidência do PIMS

12.17 PII18 - Política de monitorização, auditoria e melhoria do PIMS

12.18 PII19 - Política de privacidade dos trabalhadores

12.19 PII20 - Política de privacidade das crianças

12.20 PII22 - Política de privacidade em marketing e cookies

13. Normas e referenciais de referência

13.1 ISO/IEC 27701:2025 - Clause 7.5; Clause 8.1. Addressed by clauses [4.1.6; 4.8.1; 6.1; 7.1; 7.5; 11.1].

13.2 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.6.2; 4.6.5; 4.8.2; 6.5; 8.1; 8.2; 8.3; 8.4; 8.5; 10.1; 11.4].

13.3 ISO/IEC 27701:2025 - Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.2.3; 4.2.4; 4.8.1; 7.1; 7.2].

13.4 ISO/IEC 27701:2025 - Annex A.1.2.7; Annex A.1.2.8. Addressed by clauses [4.1.4; 4.7.1; 4.7.2; 4.7.3; 5.7; 6.3; 7.6].

13.5 ISO/IEC 27701:2025 - Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 7.3; 11.3].

13.6 ISO/IEC 27701:2025 - Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11. Addressed by clauses [4.1.3; 4.3.2; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 7.4; 11.3].

13.7 ISO/IEC 27701:2025 - Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5. Addressed by clauses [4.2.4; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 7.1; 7.5].

13.8 ISO/IEC 27701:2025 - Annex A.1.5.2; Annex A.1.5.3; Annex A.1.5.4; Annex A.1.5.5. Addressed by clauses [4.7.3; 4.7.4; 4.7.5; 7.7].

13.9 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7. Addressed by clauses [4.1.5; 4.3.5; 4.5.5; 4.7.1; 4.7.2; 5.7; 6.3; 7.6].

13.10 ISO/IEC 27701:2025 - Annex A.2.3.2; Annex A.2.5.2; Annex A.2.5.3; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6. Addressed by clauses [4.3.5; 4.5.5; 4.7.1; 4.7.2; 4.7.4; 4.7.5; 7.6; 7.7].

13.11 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.25. Addressed by clauses [4.4.4; 4.6.1; 4.6.3; 4.8.1; 5.4; 7.5; 7.8; 10.2].

13.12 GDPR - Article 4(4); Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(d); Article 5(2). Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.1; 4.4.1; 4.4.2; 4.4.5; 4.8.1; 8.1].

13.13 GDPR - Article 6; Article 9; Article 10. Addressed by clauses [4.1.2; 4.2.4; 4.4.3; 4.7.3; 7.1].

13.14 GDPR - Article 12; Article 13; Article 14; Article 15. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.5.2; 4.5.3; 7.3; 11.3].

13.15 GDPR - Article 16; Article 17; Article 18; Article 21; Article 22. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 7.4].

13.16 GDPR - Article 24; Article 25; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.2.2; 4.2.5; 4.4.4; 4.7.1; 4.8.2; 5.3; 6.2; 6.4; 7.2].

13.17 GDPR - Article 44. Addressed by clauses [4.7.4; 7.7; 8.4].

13.18 ISO/IEC 29100:2020 - Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.7. Addressed by clauses [4.1.2; 4.2.4; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.7.5].

13.19 ISO/IEC 29100:2020 - Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12. Addressed by clauses [4.3.1; 4.3.2; 4.5.1; 4.5.2; 4.6.3; 4.8.1; 4.8.2; 8.5; 10.1].

13.20 ISO/IEC 29134:2020 - Clause 5.1; Clause 6.2; Clause 6.3. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.5; 4.6.4; 6.4; 7.2; 9.2].

13.21 ISO/IEC 29151:2022 - Annex A.4; Annex A.5; Annex A.7; Annex A.8; Annex A.10. Addressed by clauses [4.3.1; 4.3.2; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.5.2; 4.5.4; 4.7.5].