					Insira aqui a designação da entidade jurídica registada							
Número do documento: PII17					Título do documento: **Política de gestão da informação documentada e evidência do PIMS**							
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 6.1.3	Both	Supporting	Informação documentada da SoA
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Informação documentada do PIMS
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Controlo de evidência operacional
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Evidência de monitorização
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Evidência de auditoria
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Evidência de revisão pela gestão
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Evidência de não conformidade e ação corretiva
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Registos de tratamento do responsável pelo tratamento
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Evidência de acordo e instruções do subcontratante
ISO/IEC 27701:2025	Annex A.3.14	Both	Primary	Proteção dos registos
GDPR	Article 5(2)	Controller	Supporting	Evidência de responsabilização
GDPR	Article 24	Controller	Supporting	Medidas e evidência do responsável pelo tratamento
GDPR	Article 28	Both	Supporting	Documentação do subcontratante
GDPR	Article 30	Both	Supporting	Registos de tratamento
GDPR	Article 32	Both	Supporting	Proteção da evidência
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Evidência de conformidade em

				matéria de privacidade
ISO/IEC 29151:2022	Clause 18.1.4	Both	Supporting	Proteção dos registos
ISO/IEC 27001:2022	Clause 7.5	Both	Supporting	Controlo da informação documentada
ISO/IEC 27002:2022	Control 5.33	Both	Supporting	Proteção dos registos
ISO/IEC 27002:2022	Control 5.34	Both	Supporting	Proteção da privacidade e de PII

1. Âmbito

1.1 Esta política define requisitos obrigatórios para criar, aprovar, versionar, proteger, reter, recuperar, traduzir, retirar e evidenciar a informação documentada do PIMS.

1.2 Esta política aplica-se a políticas do PIMS, registos, aprovações documentadas, registos de evidência, evidência de auditoria, registos de revisão pela gestão, evidência de ações corretivas e traduções controladas utilizadas para demonstrar a conformidade do PIMS.

1.3 Esta política aplica-se a contextos de responsável pelo tratamento, responsável conjunto pelo tratamento, subcontratante e subcontratante subsequente.

1.4 Esta política não cria um registo separado de controlo documental. A evidência de controlo da informação documentada é mantida através dos objetos canónicos de evidência do PIMS REG01 a REG12, sendo REG03 e REG12 utilizados para evidência de aplicabilidade de controlos, auditoria, não conformidade, ação corretiva e melhoria.

2. Finalidade

2.1 A finalidade desta política é assegurar que a informação documentada do PIMS é exata, controlada, acessível a utilizadores autorizados, protegida contra alteração ou divulgação não autorizada, retida para fins de auditabilidade e retirada quando obsoleta.

2.2 Esta política apoia a preparação para certificação, assegurando que a evidência necessária para demonstrar a conformidade do PIMS pode ser localizada, verificada, recuperada e ligada às políticas, controlos, atividades de tratamento, riscos, auditorias e ações corretivas aplicáveis.

3. Objetivos

3.1 Os objetivos desta política são:

3.1.1 definir requisitos de controlo da informação documentada do PIMS;

3.1.2 manter a integridade da evidência em REG01 a REG12;

3.1.3 assegurar que a aprovação de políticas e evidência é rastreável;

3.1.4 assegurar que o histórico de versões e as decisões de retirada são documentados;

3.1.5 ligar a evidência do PIMS à Declaração de Aplicabilidade e aos mapeamentos de políticas;

3.1.6 controlar o acesso a documentos e registos de evidência do PIMS;

3.1.7 apoiar o controlo de versões de políticas e evidência em várias línguas;

3.1.8 permitir a recuperação atempada da evidência de auditoria;

3.1.9 evitar burocracia desnecessária de controlo documental;

3.1.10 preservar registos prontos para auditoria para certificação, garantia a clientes e melhoria contínua.

4. Declarações da política

4.1 Controlo da informação documentada do PIMS

4.1.1 [All] The Privacy Lead / PIMS Manager DEVE manter um índice de informação documentada do PIMS em REG12 antes da publicação inicial do PIMS e trimestralmente daí em diante.

4.1.2 [All] The Process Owner / Business Owner DEVE identificar, em REG02, a informação documentada necessária para cada atividade de tratamento de PII da sua responsabilidade antes do início da atividade de tratamento e anualmente daí em diante.

4.1.3 [All] The Privacy Lead / PIMS Manager DEVE ligar as políticas, controlos e obrigações de evidência do PIMS aplicáveis a REG03 antes de cada publicação de política e no prazo de 15 dias úteis após qualquer alteração material da aplicabilidade de controlos.

4.1.4 [All] The Privacy Lead / PIMS Manager DEVE atribuir um nível de acesso e uma classificação de sensibilidade da evidência a cada categoria de informação documentada do PIMS em REG12 antes de a categoria ser utilizada.

4.2 Criação, aprovação, controlo de versões e publicação

4.2.1 [All] The Privacy Lead / PIMS Manager DEVE atribuir um identificador de documento, proprietário, número da versão, estado de aprovação, data de entrada em vigor e data de revisão em REG12 antes de publicar informação documentada do PIMS.

4.2.2 [All] Top Management DEVE aprovar as políticas nucleares do PIMS e alterações materiais de políticas em REG12 antes da publicação.

4.2.3 [All] The Privacy Lead / PIMS Manager DEVE aprovar modelos de evidência do PIMS ou secções incorporadas em registos em REG12 antes da utilização operacional.

4.2.4 [All] The Privacy Lead / PIMS Manager DEVE registar o histórico de versões e a justificação da alteração em REG12 antes de disponibilizar informação documentada do PIMS atualizada.

4.2.5 [All] The Privacy Lead / PIMS Manager DEVE registar a comunicação de alterações aprovadas à informação documentada do PIMS em REG11 no prazo de 30 dias após a publicação.

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

9. Exceções

9.1.1 [All] The Process Owner / Business Owner DEVE solicitar em REG12 exceções à informação documentada ou ao controlo da evidência antes de se desviar desta política.

9.1.2 [All] The Privacy Lead / PIMS Manager DEVE avaliar cada exceção à informação documentada ou ao controlo da evidência em REG12 no prazo de 10 dias úteis após o pedido.

9.1.3 [All] The Data Protection Officer / Privacy Advisor DEVE registar aconselhamento em REG12 antes da aprovação de qualquer exceção que envolva divulgação de evidência de PII, discrepância de tradução, conflito de retenção ou limitação de evidência de auditoria.

9.1.4 [All] Top Management DEVE aprovar, em REG12 e antes de a exceção produzir efeitos, exceções à informação documentada que excedam 30 dias ou afetem certificação, tratamento de alto risco ou garantia externa.

9.1.5 [All] The Privacy Lead / PIMS Manager DEVE definir em REG12 uma data de expiração não superior a 90 dias para cada exceção aprovada à informação documentada ou ao controlo da evidência.

9.1.6 [All] The Privacy Lead / PIMS Manager DEVE encerrar ou reavaliar cada exceção à informação documentada ou ao controlo da evidência em REG12 no prazo de cinco dias úteis após a expiração.

10. Aplicação

10.1.1 [All] The Privacy Lead / PIMS Manager DEVE registar informação documentada do PIMS ausente, inexata, não controlada, obsoleta ou irrecuperável como não conformidade em REG12 no prazo de cinco dias úteis após a identificação.

10.1.2 [All] The Privacy Lead / PIMS Manager DEVE impedir a publicação de informação documentada do PIMS quando a evidência exigida de aprovação, versão, proprietário ou data de entrada em vigor estiver ausente de REG12.

10.1.3 [All] The Process Owner / Business Owner DEVE impedir a submissão para auditoria de evidência de tratamento quando a evidência exigida de proprietário, data, estado ou aprovação estiver ausente de REG02.

10.1.4 [All] The System Owner / Application Owner DEVE remover acessos não autorizados a repositórios de informação documentada do PIMS e registar a remoção em REG12 no prazo de um dia útil após a identificação.

10.1.5 [All] The Internal Audit / Compliance Reviewer DEVE verificar a eficácia das ações corretivas relativas a não conformidades de informação documentada em REG12 na auditoria programada seguinte ou no prazo de 60 dias após o encerramento, consoante o que ocorrer primeiro.

11. Revisão e manutenção

11.1.1 [All] The Privacy Lead / PIMS Manager DEVE rever esta política anualmente e no prazo de 30 dias após alteração material aos requisitos de informação documentada do PIMS.

11.1.2 [All] The Privacy Lead / PIMS Manager DEVE rever esta política no prazo de 30 dias após uma constatação de auditoria relevante, não conformidade de certificação, alteração da plataforma de repositório ou alteração do processo de publicação multilingue.

11.1.3 [All] The Data Protection Officer / Privacy Advisor DEVE rever em REG12 alterações a esta política com relevância para a privacidade antes da aprovação.

11.1.4 [All] Top Management DEVE aprovar alterações materiais a esta política em REG12 antes da publicação.

11.1.5 [All] The Privacy Lead / PIMS Manager DEVE registar a comunicação de alterações aprovadas a esta política em REG11 no prazo de 30 dias após a publicação.

12. Políticas relacionadas

12.1 Esta política é apoiada pelas seguintes políticas relacionadas:

12.2 PII01 - Política do sistema de gestão de informação de privacidade

12.3 PII02 - Política de papéis, responsabilidades e responsabilização em matéria de privacidade

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

12.5 PII04 - Política de aviso de privacidade e transparência

12.6 PII05 - Política de gestão de consentimento e preferências

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

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

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

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

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

12.12 PII11 - Política de exatidão e qualidade de PII

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

12.14 PII13 - Política de transferência internacional de PII

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

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

12.17 PII16 - Política de formação, sensibilização e competência em privacidade

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

13. Normas e referenciais de referência

13.1 Esta política está mapeada para as seguintes normas e regulamentos. O mapeamento explica como a política apoia os requisitos citados e identifica as cláusulas internas que os implementam ou apoiam.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.3** - Mapeada para a manutenção da Declaração de Aplicabilidade do PIMS, dos registos de aplicabilidade de controlos e da ligação entre políticas e evidência. Addressed by clauses [4.1.3; 4.3.3; 6.1.3; 7.1.2].

13.2.2 **Clause 7.5** - Mapeada para a identificação da informação documentada, aprovação, controlo de versões, acesso, recuperação, preservação, retirada, ligação de versões traduzidas e metadados de retenção. Addressed by clauses [4.1.1; 4.1.4; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.5; 4.4.1; 4.4.2; 4.4.4; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.6.1; 4.6.2; 4.6.3; 4.6.4].

13.2.3 **Clause 8.1** - Mapeada para a evidência de planeamento e controlo operacional relativa a registos de tratamento, modelos de evidência, qualidade da evidência operacional e evidência fornecida externamente. Addressed by clauses [4.1.2; 4.2.3; 4.3.2; 7.1.3; 7.1.4].

13.2.4 **Clause 9.1** - Mapeada para a manutenção de evidência documentada de medição, desempenho de recuperação, lacunas de evidência, divergências de tradução e conclusão da revisão de acessos a repositórios. Addressed by clauses [8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6].

13.2.5 **Clause 9.2** - Mapeada para a recuperação de evidência de auditoria, amostragem de auditoria, rastreabilidade da evidência de auditoria e constatações de auditoria relacionadas com o controlo da informação documentada. Addressed by clauses [4.3.4; 4.4.4; 6.1.3; 8.1.3; 10.1.5].

13.2.6 **Clause 9.3** - Mapeada para a evidência de revisão pela gestão, a consideração do controlo da informação documentada na revisão pela gestão e a revisão do desempenho do controlo da evidência por Top Management. Addressed by clauses [6.1.2; 8.1.1; 8.1.2; 11.1.4].

13.2.7 **Clause 10.2** - Mapeada para não conformidades de informação documentada, ações corretivas, tratamento de exceções, encerramento e verificação de eficácia. Addressed by clauses [4.3.4; 6.1.4; 9.1.1; 9.1.2; 9.1.4; 9.1.5; 9.1.6; 10.1.1; 10.1.5].

13.2.8 **Annex A.1.2.9** - Mapeada para registos de tratamento do responsável pelo tratamento, registos de responsabilização, qualidade da evidência de tratamento e retenção de evidência que apoia as obrigações do responsável pelo tratamento. Addressed by clauses [4.1.2; 4.3.2; 4.5.1; 7.1.3].

13.2.9 **Annex A.2.2.2** - Mapeada para acordo de subcontratante, instruções de clientes, evidência fornecida externamente e controlo da evidência da relação com subcontratantes. Addressed by clauses [5.1.7; 7.1.4].

13.2.10 **Annex A.3.14** - Mapeada para a proteção dos registos do PIMS contra perda, alteração não autorizada, acesso não autorizado, divulgação não autorizada e eliminação indevida. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.2; 4.5.4; 4.5.5; 10.1.4].

13.3 GDPR

13.3.1 **Article 5(2)** - Mapeado para evidência de responsabilização, rastreabilidade da evidência, recuperação da evidência, registos de não conformidade e registos prontos para auditoria que demonstram conformidade. Addressed by clauses [4.1.1; 4.3.2; 4.3.3; 4.4.4; 4.5.4; 6.1.3; 8.1.3; 10.1.1].

13.3.2 **Article 24** - Mapeado para evidência de governação do responsável pelo tratamento, registos de aprovação, controlo de políticas, medidas de responsabilização, revisão documentada e supervisão por Top Management. Addressed by clauses [4.2.2; 4.3.3; 6.1.2; 9.1.4; 11.1.4].

13.3.3 **Article 28** - Mapeado para documentação de subcontratantes e subcontratantes subsequentes, evidência de instruções de clientes, evidência de processos fornecida

externamente e controlo da divulgação de evidência. Addressed by clauses [4.4.5; 5.1.7; 7.1.4].

13.3.4 **Article 30** - Mapeado para evidência de registos de tratamento, requisitos de qualidade da evidência, referências de atividades de tratamento e metadados de proprietário/estado da evidência de tratamento. Addressed by clauses [4.1.2; 4.3.2; 7.1.3; 10.1.3].

13.3.5 **Article 32** - Mapeado para a proteção de repositórios de evidência, restrições de acesso, aprovações de acesso, revisão da proteção de repositórios e remoção de acessos não autorizados. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 10.1.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.12** - Mapeada para evidência de conformidade em matéria de privacidade, recuperação de evidência de auditoria, rastreabilidade da evidência, apoio a revisão independente e evidência de ações corretivas. Addressed by clauses [4.3.3; 4.4.4; 4.6.3; 6.1.3; 8.1.3; 10.1.5].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 18.1.4** - Mapeada para a proteção de registos relacionados com PII, preservação de registos e controlos de acesso e apagamento dos repositórios de evidência. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.5.2; 4.5.5; 10.1.4].

13.6 ISO/IEC 27001:2022

13.6.1 **Clause 7.5** - Mapeada para identificação, aprovação, disponibilidade, proteção, controlo de versões, retenção, disposição e controlo de informação documentada exigida externamente. Addressed by clauses [4.1.1; 4.2.1; 4.2.4; 4.3.1; 4.4.1; 4.5.1; 4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.6.4].

13.7 ISO/IEC 27002:2022

13.7.1 Control 5.33 - Mapeado para a proteção dos registos do PIMS contra perda, destruição, falsificação, acesso não autorizado, divulgação não autorizada e eliminação indevida. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 10.1.4].

13.7.2 Control 5.34 - Mapeado para a proteção da privacidade e de PII na informação documentada, repositórios de evidência, divulgações e registos com acesso controlado. Addressed by clauses [4.1.4; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 6.1.5].