					Insira aqui a designação da entidade jurídica registada							
Número do documento: PII09					Título do documento: **Política de recolha, utilização, divulgação e partilha de PII**							
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

Norma / Regulamento	Cláusula / Controlo / Artigo	Aplicabilidade	Tipo de cobertura	Comentário
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Both	Primary	Controlo operacional documentado
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitorização e ação corretiva
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.9	Controller	Primary	Finalidade e registos de tratamento
ISO/IEC 27701:2025	Annex A.1.2.3	Controller	Referenced	Ligação ao fundamento de licitude
ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Supporting	Responsabilidades de partilha entre responsáveis conjuntos pelo tratamento
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
ISO/IEC 27701:2025	Annex A.1.5.2; Annex A.1.5.3	Conditional	Referenced	Ligação ao encaminhamento de transferências
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5	Controller	Primary	Registos de transferências e divulgações
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7	Processor	Primary	Instruções e registos do subcontratante
ISO/IEC 27701:2025	Annex A.2.5.2; Annex A.2.5.3	Processor	Referenced	Ligação ao encaminhamento de transferências pelo subcontratante
ISO/IEC 27701:2025	Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Registos e pedidos de divulgação pelo subcontratante
GDPR	Article 5(1)(b); Article 5(1)(c); Article 5(2)	Controller	Primary	Limitação da finalidade, minimização e responsabilização

GDPR	Article 6	Controller	Referenced	Ligação ao fundamento de licitude
GDPR	Article 24	Controller	Supporting	Responsabilidade do responsável pelo tratamento
GDPR	Article 26	Joint Controller	Supporting	Acordos entre responsáveis conjuntos pelo tratamento
GDPR	Article 28	Both	Supporting	Instruções ao subcontratante e limites de divulgação
GDPR	Article 30	Both	Supporting	Registos de tratamento e de destinatários
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Primary	Finalidade, recolha, minimização e limitação da divulgação
ISO/IEC 29100:2020	Clause 5.10; Clause 5.12	Both	Supporting	Responsabilização e conformidade de privacidade
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7	Both	Supporting	Controlos de finalidade, recolha, minimização, utilização e divulgação

1. Âmbito

1.1 Esta política define requisitos para a recolha, utilização, divulgação e partilha de PII no âmbito do PIMS.

1.2 Esta política aplica-se a:

1.2.1 recolha de PII através de canais diretos, indiretos, automatizados, manuais, internos, externos e de terceiros;

1.2.2 utilização interna aprovada de PII por processos de negócio, sistemas e aplicações;

1.2.3 utilização secundária de PII para uma finalidade nova ou materialmente alterada;

1.2.4 divulgação externa de PII a destinatários, parceiros, autoridades, subcontratantes, subcontratantes subsequentes, fornecedores e outros terceiros;

1.2.5 acordos recorrentes de partilha de dados e divulgações pontuais;

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

1.2.7 REG02 - Inventário de tratamento de PII / ROPA, REG08 - Registo de subcontratantes, subcontratantes subsequentes e partilha de dados, REG09 - Registo de transferências internacionais, e REG12 - Registo de auditoria, não conformidade, ação corretiva e melhoria.

1.3 Esta política não substitui:

1.3.1 PII03 quanto ao inventário de tratamento, fundamento de licitude e propriedade do ROPA;

1.3.2 PII04 quanto ao conteúdo, publicação e controlo de versões do aviso de privacidade;

1.3.3 PII05 quanto à operação de consentimento e preferências;

1.3.4 PII06 quanto ao tratamento de pedidos de exercício de direitos dos titulares dos dados;

1.3.5 PII07 quanto à metodologia de DPIA e à avaliação de riscos de privacidade;

1.3.6 PII08 quanto aos gates de privacidade desde a conceção;

1.3.7 PII10 quanto à execução da retenção, eliminação e descarte;

1.3.8 PII11 quanto à gestão da exatidão e qualidade;

1.3.9 PII12 quanto à governação do ciclo de vida de subcontratantes, subcontratantes subsequentes e terceiros;

1.3.10 PII13 quanto à seleção do mecanismo de transferência internacional e aos controlos de risco de transferência;

1.3.11 PII14 quanto à segurança de PII e ao controlo de acesso;

1.3.12 PII15 quanto ao tratamento de incidentes e violações;

1.3.13 PII18 quanto à governação de monitorização, auditoria, não conformidade, ação corretiva e melhoria em todo o PIMS.

1.4 Para efeitos desta política:

1.4.1 "utilização aprovada" significa uma utilização de PII registada em REG02 para uma atividade de tratamento, finalidade, categoria de PII, categoria de titular dos dados, proprietário do negócio e função PIMS aplicável específicos.

1.4.2 "recolha" significa a obtenção de PII diretamente junto de um titular dos dados, indiretamente junto de outra parte, automaticamente a partir de um sistema ou dispositivo, ou através de uma fonte de dados interna ou externa.

1.4.3 "utilização secundária" significa a utilização de PII para uma finalidade que ainda não esteja registada como finalidade aprovada em REG02 para a atividade de tratamento relevante.

1.4.4 "verificação de compatibilidade" significa uma avaliação documentada em REG02 da finalidade original, da finalidade proposta, da dependência do fundamento de licitude, das categorias de PII, das expectativas dos titulares dos dados, da justificação de minimização, do impacto de divulgação ou transferência, e do encaminhamento para outras políticas PIMS quando necessário.

1.4.5 "divulgação externa" significa disponibilizar PII a uma parte externa à organização ou fora da cadeia documentada de instruções do cliente.

1.4.6 "partilha de dados" significa um acordo recorrente ou estruturado ao abrigo do qual PII é divulgada, transferida, acedida, trocada ou disponibilizada a outra parte.

1.4.7 "partilha recorrente sensível" significa partilha recorrente que envolva PII de categorias especiais, PII relativa a infrações penais, PII de crianças, registos de elevado impacto, partilha em larga escala ou partilha externa que envolva uma localização de transferência registada em REG09.

2. Finalidade

2.1 A finalidade desta política é assegurar que PII é recolhida, utilizada, divulgada e partilhada apenas para finalidades documentadas, aprovadas, limitadas e sujeitas a responsabilização.

2.2 Esta política permite à organização demonstrar que a recolha e a utilização estão ligadas aos registos de tratamento em REG02, que as divulgações e os acordos de partilha de dados são registados em REG08, que o encaminhamento de transferências internacionais está ligado a REG09, e que as exceções e não conformidades são tratadas através de REG12.

3. Objetivos

3.1 Os objetivos desta política são:

3.1.1 limitar a recolha à PII necessária para finalidades documentadas;

3.1.2 assegurar que a utilização interna de PII é aprovada antes do início do tratamento;

3.1.3 exigir verificações de compatibilidade antes da utilização secundária;

3.1.4 exigir aprovação e evidência antes da divulgação externa;

3.1.5 manter evidência de partilha de dados em REG08 sem criar um registo de partilha de dados separado;

3.1.6 encaminhar dependências de transferência internacional para REG09 e PII13 sem duplicar controlos do mecanismo de transferência;

3.1.7 definir a cadência de revisão da partilha recorrente;

3.1.8 manter evidência preparada para auditoria relativa a recolha, utilização, divulgação, partilha, exceções e ações corretivas.

4. Declarações da política

4.1 Limitação da recolha

4.1.1 [Controller] O Process Owner / Business Owner deve registar em REG02 a finalidade da recolha, a fonte ou canal, as categorias de PII, as categorias de titulares dos dados e os elementos mínimos de dados antes do início de qualquer nova atividade de recolha ou alteração material da recolha.

4.1.2 [Controller] O Privacy Lead / PIMS Manager deve rever o registo de recolha em REG02 antes do início da recolha quando for adicionada uma nova categoria de PII, fonte, canal ou finalidade.

4.1.3 [Controller] O Process Owner / Business Owner deve registar em REG02 uma justificação de necessidade para cada elemento de dados de PII antes de esse elemento ser recolhido.

4.1.4 [Processor] O Process Owner / Business Owner deve registar em REG02 a referência da instrução do cliente proveniente de REG08 antes de recolher PII em nome de um cliente.

4.1.5 [Joint Controller] O Process Owner / Business Owner deve registar em REG08 a repartição de responsabilidades de recolha entre responsáveis conjuntos pelo tratamento antes do início da recolha conjunta.

4.2 Controlos de utilização interna aprovada

4.2.1 [Controller] O Process Owner / Business Owner deve registar em REG02 as regras aprovadas de utilização interna para cada atividade de tratamento antes do início da utilização.

4.2.2 [Controller] O System Owner / Application Owner deve implementar apenas campos de fluxos de trabalho, relatórios ou exportações de utilização interna que tenham uma regra correspondente de utilização aprovada em REG02 antes da entrada em produção.

4.2.3 [Processor] O Process Owner / Business Owner deve registar em REG08 o alinhamento com as instruções do cliente antes de utilizar PII do cliente em qualquer atividade de subcontratante ou subcontratante subsequente.

4.2.4 [Controller] O Privacy Lead / PIMS Manager deve rever as regras de utilização aprovada em REG02 pelo menos anualmente para cada atividade de tratamento ativa.

4.2.5 [All] O Privacy Lead / PIMS Manager deve registar uma não conformidade em REG12 no prazo de cinco dias úteis quando for identificada utilização interna não documentada de PII.

[... 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] O Process Owner / Business Owner deve registar um pedido de exceção em REG12 antes de se desviar de uma regra aprovada de recolha, utilização, divulgação ou partilha.

9.1.2 [All] O Privacy Lead / PIMS Manager deve registar uma decisão de aprovação ou rejeição em REG12 antes de uma exceção ser ativada.

9.1.3 [Conditional] O Data Protection Officer / Privacy Advisor deve registar aconselhamento em REG12 antes da aprovação de uma exceção que envolva utilização secundária incompatível, partilha recorrente sensível, conflito relativo a divulgação juridicamente vinculativa ou encaminhamento de transferência.

9.1.4 [All] Top Management deve registar aprovação em REG12 antes da ativação de qualquer exceção com duração superior a 30 dias de calendário ou que afete mais do que uma atividade de tratamento.

9.1.5 [All] O Process Owner / Business Owner deve encerrar uma exceção em REG12 até à data de expiração ou no prazo de cinco dias úteis após o termo da condição da exceção.

10. Aplicação

10.1.1 [All] O Privacy Lead / PIMS Manager deve registar recolha, utilização, divulgação ou partilha não aprovada como não conformidade em REG12 no prazo de cinco dias úteis após a identificação.

10.1.2 [Controller] O Process Owner / Business Owner deve suspender a recolha, utilização, divulgação ou partilha no prazo de um dia útil quando o Privacy Lead / PIMS Manager registar em REG12 a ausência de evidência aprovada em REG02 ou REG08.

10.1.3 [Processor] O Process Owner / Business Owner deve registar uma decisão de interrupção ou escalonamento em REG08 e REG12 no prazo de um dia útil quando PII do cliente for utilizada ou divulgada fora das instruções documentadas.

10.1.4 [All] Top Management deve rever em REG12 as não conformidades de elevado impacto não resolvidas relativas a recolha, utilização, divulgação ou partilha no prazo de 30 dias de calendário após o escalonamento.

10.1.5 [All] O Internal Audit / Compliance Reviewer deve verificar a evidência de encerramento de ações corretivas em REG12 no prazo de 15 dias úteis após o Privacy Lead / PIMS Manager assinalar o encerramento.

11. Revisão e manutenção

11.1.1 [All] O Privacy Lead / PIMS Manager deve rever esta política pelo menos anualmente e registar a decisão em REG12.

11.1.2 [All] O Privacy Lead / PIMS Manager deve rever esta política no prazo de 30 dias de calendário após uma alteração material ao âmbito do PIMS, às finalidades de tratamento, ao modelo de partilha, ao encaminhamento de transferências ou à obrigação aplicável, e registar o resultado em REG12.

11.1.3 [All] O Process Owner / Business Owner deve recertificar os registos ativos de REG02 e REG08 pelo menos anualmente e no prazo de 30 dias de calendário após uma alteração material do tratamento.

11.1.4 [All] O Internal Audit / Compliance Reviewer deve incluir os controlos PII09 na amostragem anual de auditoria e registar a cobertura em REG12.

11.1.5 [All] O Privacy Lead / PIMS Manager deve atualizar as referências a políticas relacionadas em REG12 no prazo de dez dias úteis quando PII03, PII08, PII10, PII12, PII13, PII14 ou PII18 alterarem o limite operacional desta política.

12. Políticas relacionadas

12.1 Esta política deve ser lida em conjunto com:

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

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

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

12.1.4 PII04 - Política de aviso de privacidade e transparência

12.1.5 PII05 - Política de gestão de consentimento e preferências

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

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

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

12.1.9 PII10 - Política de retenção, eliminação e descarte de PII

12.1.10 PII11 - Política de exatidão e qualidade de PII

12.1.11 PII12 - Política de gestão de privacidade de subcontratantes, subcontratantes subsequentes e terceiros

12.1.12 PII13 - Política de transferência internacional de PII

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

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

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

12.1.16 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 7.5; Clause 8.1** - Mapeado para registos operacionais documentados e controlo sobre evidência de recolha, utilização aprovada, utilização secundária, divulgação, partilha e encaminhamento de transferências. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.3; 4.3.5; 4.4.1; 4.4.2; 4.5.1; 7.1.1; 7.1.4].

13.2.2 **Clause 9.1; Clause 10.2** - Mapeado para monitorização, medição, revisão, tratamento de exceções, não conformidade e ação corretiva relativos aos controlos de recolha, utilização, divulgação e partilha. Addressed by clauses [4.2.4; 4.2.5; 6.1.1; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 9.1.1; 10.1.1; 10.1.5; 11.1.4].

13.2.3 **Annex A.1.2.2; Annex A.1.2.9** - Mapeado para finalidades documentadas do responsável pelo tratamento, registos de utilização aprovada e evidência de tratamento em REG02. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.4; 4.3.1; 4.3.2; 4.3.4; 4.5.5].

13.2.4 **Annex A.1.2.3** - Mapeado para a ligação ao fundamento de licitude aplicável à recolha, utilização e encaminhamento de utilização secundária, sem substituir PII03. Addressed by clauses [4.3.4; 6.1.2; 7.1.1].

13.2.5 **Annex A.1.2.8** - Mapeado para evidência de responsabilidades de recolha e partilha entre responsáveis conjuntos pelo tratamento em REG08. Addressed by clauses [4.1.5; 4.4.4; 6.1.4].

13.2.6 **Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5** - Mapeado para limitação da recolha, limitação do tratamento e justificação de minimização antes de PII ser recolhida ou utilizada. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.3.1; 4.3.2; 7.1.2].

13.2.7 **Annex A.1.5.2; Annex A.1.5.3** - Mapeado para a ligação ao encaminhamento de transferências através de REG09 sem substituir os controlos do mecanismo de transferência de PII13. Addressed by clauses [4.5.1; 4.5.2; 7.1.4].

13.2.8 **Annex A.1.5.4; Annex A.1.5.5** - Mapeado para registos de transferências, divulgações e acordos recorrentes de partilha de dados em REG08. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.5.1; 4.5.3; 4.5.4; 4.5.5].

13.2.9 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7** - Mapeado para o alinhamento com instruções do cliente pelo subcontratante e registos do subcontratante relativos a limites de recolha, utilização e utilização secundária. Addressed by clauses [4.1.4; 4.2.3; 4.3.6; 7.1.3; 10.1.3].

13.2.10 **Annex A.2.5.2; Annex A.2.5.3** - Mapeado para a ligação ao encaminhamento de transferências pelo subcontratante através de REG09 sem substituir os controlos do mecanismo de transferência de PII13. Addressed by clauses [4.5.1; 4.5.2; 7.1.4].

13.2.11 **Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6** - Mapeado para registos de divulgação pelo subcontratante, estado da notificação de pedidos de divulgação e evidência de autorização de divulgação em REG08. Addressed by clauses [4.4.5; 4.4.6; 4.4.7; 10.1.3].

13.3 GDPR

13.3.1 **Article 5(1)(b); Article 5(1)(c); Article 5(2)** - Mapeado para limitação da finalidade, minimização de dados e evidência de responsabilização relativamente a recolha, utilização, utilização secundária, divulgação e partilha. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.3.1; 4.3.2; 4.4.1; 4.4.2; 4.5.3; 8.1.3; 10.1.1].

13.3.2 Article 6 - Mapeado para a ligação ao fundamento de licitude e encaminhamento de utilização secundária nova ou incompatível sem substituir PII03. Addressed by clauses [4.3.4; 6.1.2; 7.1.1].

13.3.3 **Article 24** - Mapeado para governação, aprovações, revisão e medidas de responsabilização do responsável pelo tratamento relativas a recolha, utilização, divulgação e

partilha. Addressed by clauses [4.1.2; 4.2.4; 4.3.2; 4.3.3; 4.3.5; 4.4.1; 6.1.1; 9.1.2; 10.1.4; 11.1.1].

13.3.4 **Article 26** - Mapeado para evidência de responsabilidades de recolha e partilha entre responsáveis conjuntos pelo tratamento. Addressed by clauses [4.1.5; 4.4.4; 6.1.4].

13.3.5 **Article 28** - Mapeado para alinhamento com instruções de subcontratantes e subcontratantes subsequentes, autorização do cliente e limites de divulgação. Addressed by clauses [4.1.4; 4.2.3; 4.3.6; 4.4.5; 4.4.6; 4.4.7; 7.1.3; 10.1.3].

13.3.6 **Article 30** - Mapeado para registos de tratamento, destinatários, divulgação e partilha em REG02 e REG08. Addressed by clauses [4.1.1; 4.2.1; 4.4.2; 4.4.3; 4.5.1; 4.5.5; 8.1.1; 8.1.2].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Mapeado para especificação da finalidade, limitação da recolha, minimização de dados, limitação da utilização e limitação da divulgação. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.3.1; 4.3.2; 4.4.1; 4.4.2; 4.5.3].

13.4.2 **Clause 5.10; Clause 5.12** - Mapeado para responsabilização, evidência de conformidade, revisão, gestão de exceções, amostragem de auditoria e ação corretiva. Addressed by clauses [4.2.4; 4.2.5; 5.1.2; 6.1.1; 8.1.1; 9.1.1; 10.1.1; 11.1.4].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7** - Mapeado para finalidade, limitação da recolha, minimização, limitação da utilização, limitação da divulgação e apoio ao registo de divulgações. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.4.6; 4.5.3].