					Insira aqui a designação da entidade jurídica registada							
Número do documento: PII08					Título do documento: **Política de privacidade desde a conceção e por defeito**							
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 6.1.2; Clause 6.1.3	Both	Supporting	Ligação à avaliação de riscos de privacidade e ao tratamento de riscos de privacidade
ISO/IEC 27701:2025	Clause 6.3; Clause 8.1	Both	Primary	Alterações planeadas e controlo operacional
ISO/IEC 27701:2025	Clause 7.5	Both	Supporting	Evidência documentada de privacidade desde a conceção
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.1.2.6; Annex A.1.2.9	Controller	Supporting	Finalidades, desencadeador de PIA e registos
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3	Controller	Primary	Limitação da recolha e do tratamento
ISO/IEC 27701:2025	Annex A.1.4.4; Annex A.1.4.5	Controller	Supporting	Objetivos de exatidão e minimização
ISO/IEC 27701:2025	Annex A.1.4.6; Annex A.1.4.7	Controller	Supporting	Desidentificação, conceção da eliminação e ficheiros temporários
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7	Processor	Supporting	Acordo com o cliente, apoio e registos do subcontratante
ISO/IEC 27701:2025	Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4	Processor	Supporting	Capacidades de conceção do subcontratante
ISO/IEC 27701:2025	Annex A.3.27; Annex A.3.29	Both	Supporting	Ciclo de vida de desenvolvimento e princípios de engenharia

GDPR	Article 5(1)(b); Article 5(1)(c); Article 5(2)	Controller	Supporting	Limitação da finalidade, minimização e responsabilização
GDPR	Article 24	Controller	Supporting	Medidas do responsável pelo tratamento
GDPR	Article 25	Controller	Primary	Proteção de dados desde a conceção e por defeito
GDPR	Article 28	Both	Supporting	Instruções e assistência do subcontratante
GDPR	Article 30	Both	Supporting	Registos de tratamento
GDPR	Article 35	Controller	Supporting	Ligação ao desencadeador de DPIA
ISO/IEC 29100:2020	Clause 4.7	Both	Supporting	Controlos de privacidade desde a conceção
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Primary	Finalidade, recolha, minimização e limitação da utilização
ISO/IEC 29100:2020	Clause 5.7; Clause 5.10; Clause 5.12	Both	Supporting	Exatidão, responsabilização e conformidade
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.8	Both	Primary	Princípios e controlos de proteção de PII

1. Âmbito

1.1 Esta política define os requisitos para incorporar a privacidade desde a conceção e a privacidade por defeito em atividades novas e alteradas de tratamento de PII, projetos, produtos, serviços, sistemas, aplicações, integrações, atividades de aquisição e alterações de processos de negócio dentro do âmbito do PIMS.

1.2 Esta política aplica-se a contextos de responsável pelo tratamento, responsável conjunto pelo tratamento, subcontratante e subcontratante subsequente. As obrigações de subcontratante e de subcontratante subsequente aplicam-se quando a organização concebe, configura, altera ou opera tratamento por conta de um cliente, responsável pelo tratamento ou subcontratante a montante, ao abrigo de instruções documentadas.

1.3 Esta política abrange:

1.3.1 requisitos de privacidade no início do projeto;

1.3.2 controlos de conceção relativos à finalidade, minimização de dados e definições por defeito;

1.3.3 revisão de privacidade desde a conceção antes da entrada em produção;

1.3.4 revisão de privacidade desde a conceção desencadeada por alterações;

1.3.5 verificações de privacidade desde a conceção em aquisições;

1.3.6 ligação à evidência de risco de privacidade, triagem para DPIA e ação corretiva.

1.4 Esta política não substitui:

1.4.1 PII03 para inventário de tratamento, finalidades, fundamento de licitude e registos ROPA;

1.4.2 PII04 para o conteúdo e a publicação de avisos de privacidade;

1.4.3 PII05 para controlos de consentimento e preferências;

1.4.4 PII06 para o tratamento dos direitos dos titulares dos dados;

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

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

1.4.7 PII10 para a execução da retenção, apagamento e eliminação;

1.4.8 PII11 para a operação de exatidão e qualidade;

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

1.4.10 PII13 para mecanismos de transferência internacional;

1.4.11 PII14 para a operação de segurança e controlo de acesso de PII;

1.4.12 PII18 para a governação de monitorização, auditoria, ação corretiva e melhoria em todo o PIMS.

2. Finalidade

2.1 A finalidade desta política é assegurar que os requisitos de privacidade são identificados, implementados e evidenciados antes de o tratamento de PII começar ou sofrer alterações materiais, e que os sistemas e processos são configurados por defeito para limitar a recolha, utilização, exposição, dependência de retenção, dependência de divulgação e identificabilidade da PII ao que é necessário para a finalidade documentada.

3. Objetivos

3.1 Os objetivos desta política são:

3.1.1 incorporar requisitos de privacidade nas decisões de início de projeto, conceção, aquisição, alteração e entrada em produção;

3.1.2 assegurar que as conceções de tratamento de PII estão ligadas às finalidades documentadas e aos registos de tratamento REG02;

3.1.3 implementar definições por defeito de minimização de dados e de proteção da privacidade antes de o tratamento começar;

3.1.4 assegurar que a triagem de risco de privacidade e DPIA é desencadeada sem duplicar a metodologia PII07;

3.1.5 assegurar que os requisitos de conceção relativos a aquisições e subcontratantes são registados sem duplicar a governação do ciclo de vida PII12;

3.1.6 assegurar que questões de conceção não resolvidas são escaladas através de REG12;

3.1.7 manter evidência de conceção preparada para auditoria em REG02, REG04, REG08 e REG12.

4. Declarações da política

4.1 Início do projeto e requisitos de privacidade

4.1.1 [Both] The Process Owner / Business Owner DEVE registar uma entrada de privacidade desde a conceção em REG04 antes de iniciar qualquer projeto, produto, serviço, sistema, aplicação, integração ou alteração de processo de negócio que envolva PII.

4.1.2 [Both] The Process Owner / Business Owner DEVE ligar cada entrada de privacidade desde a conceção em REG04 a uma atividade de tratamento REG02 existente ou em minuta antes de os requisitos funcionais serem aprovados.

4.1.3 [Controller] The Privacy Lead / PIMS Manager DEVE registar os requisitos de privacidade desde a conceção do responsável pelo tratamento em REG04 antes da aprovação da conceção funcional do responsável pelo tratamento.

4.1.4 [Processor] The Vendor / Procurement Owner DEVE registar as instruções de conceção de privacidade do cliente e as restrições contratuais de conceção em REG08 antes da aprovação da conceção do serviço de subcontratante ou de uma alteração material do serviço.

4.1.5 [Conditional] The Data Protection Officer / Privacy Advisor DEVE registar aconselhamento em REG04 antes da aprovação de uma conceção de PII de alto risco, nova, sensível, automatizada, em grande escala ou materialmente alterada.

4.1.6 [Both] The Information Security Lead DEVE registar em REG04, antes da aprovação da arquitetura, as dependências de controlos de segurança de PII que suportam a conceção de privacidade.

4.2 Minimização de dados e conceção de privacidade por defeito

4.2.1 [Controller] The Process Owner / Business Owner DEVE documentar as categorias mínimas de PII, categorias de titulares dos dados, fontes e finalidades em REG02 e REG04 antes da aprovação da conceção de recolha ou importação.

4.2.2 [Both] The System Owner / Application Owner DEVE configurar as definições de tratamento por defeito para a recolha e o tratamento mínimos de PII necessários à finalidade documentada e registar a evidência em REG04 antes da entrada em produção.

4.2.3 [Controller] The Process Owner / Business Owner DEVE documentar campos opcionais de PII, opções de tratamento opcionais e definições desligadas por defeito em REG02 e REG04 antes da aprovação da interface de utilizador, formulário ou fluxo de trabalho.

4.2.4 [Both] The System Owner / Application Owner DEVE documentar em REG04, antes da entrada em produção, as definições por defeito de exposição de privacidade para vistas, relatórios, exportações, interfaces e fluxos de trabalho automatizados.

4.2.5 [Both] The Process Owner / Business Owner DEVE documentar em REG04 a viabilidade de desidentificação, pseudonimização, agregação ou tratamento não identificável antes de aprovar PII identificável para testes, análise, reporte ou utilização operacional secundária.

4.2.6 [Both] The System Owner / Application Owner DEVE documentar em REG04, antes da entrada em produção, o tratamento de artefactos temporários de PII, incluindo ficheiros temporários, caches, logs ou registos de staging.

4.2.7 [Both] The Process Owner / Business Owner DEVE encaminhar os requisitos de conceção abrangidos por PII10, PII11, PII13 ou PII14 para o percurso de evidência da política relacionada em REG04 no prazo de cinco dias úteis após a identificação da dependência.

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

9. Exceções

9.1 Exceções de conceção de privacidade

9.1.1 [Both] The Process Owner / Business Owner DEVE solicitar uma exceção de conceção de privacidade em REG12 antes de aprovar uma conceção ou alteração que não consiga cumprir um requisito aplicável de conceção de privacidade.

9.1.2 [Both] The Privacy Lead / PIMS Manager DEVE avaliar o impacto, os controlos compensatórios e a caducidade de cada exceção de conceção de privacidade em REG12 no prazo de cinco dias úteis após o pedido.

9.1.3 [Conditional] The Data Protection Officer / Privacy Advisor DEVE registar aconselhamento em REG12 antes da aprovação de uma exceção de conceção de privacidade que envolva tratamento de alto risco, sensível, automatizado, em grande escala, contestado ou juridicamente material.

9.1.4 [All] Top Management DEVE aprovar em REG12 uma exceção de conceção de privacidade que afete tratamento de elevado impacto, âmbito de certificação, risco maior não resolvido ou obrigação legal antes de a exceção produzir efeitos.

9.1.5 [Both] The Privacy Lead / PIMS Manager DEVE definir em REG12 uma data de expiração não superior a 90 dias para cada exceção de conceção de privacidade aprovada antes da aprovação.

9.1.6 [Both] The Privacy Lead / PIMS Manager DEVE encerrar ou reavaliar cada exceção de conceção de privacidade em REG12 no prazo de cinco dias úteis após a expiração.

10. Aplicação

10.1 Aplicação e tratamento de não conformidades

10.1.1 [Both] The Privacy Lead / PIMS Manager DEVE registar a ausência de revisão de privacidade desde a conceção, a ausência de evidência de minimização, uma falha não resolvida de definições por defeito ou uma entrada em produção não autorizada como não conformidade em REG12 no prazo de cinco dias úteis após a identificação.

10.1.2 [Both] The System Owner / Application Owner DEVE impedir a entrada em produção de um sistema de tratamento de PII quando a revisão de privacidade desde a conceção REG04 estiver incompleta e registar a decisão em REG12 antes da entrada em produção.

10.1.3 [Both] The Vendor / Procurement Owner DEVE impedir a integração de fornecedores ou a assinatura de contrato quando a evidência de conceção de privacidade REG08 exigida estiver ausente e registar a decisão em REG12 antes da integração ou assinatura.

10.1.4 [Both] The Process Owner / Business Owner DEVE suspender a utilização de uma conceção de tratamento de PII nova ou alterada até que a revisão REG04, as atualizações REG02 e as exceções REG12 exigidas estejam concluídas.

10.1.5 [All] Top Management DEVE exigir ação corretiva em REG12 no prazo de 10 dias úteis para falhas de conceção de privacidade repetidas, prolongadas ou de elevado impacto.

10.1.6 [All] The Internal Audit / Compliance Reviewer DEVE verificar a eficácia da ação corretiva relativa a não conformidades de conceção de privacidade em REG12 na auditoria PIMS programada seguinte ou no prazo de 60 dias após o encerramento, consoante o que ocorrer primeiro.

11. Revisão e manutenção

11.1 Revisão da política e dos controlos de conceção

11.1.1 [All] The Privacy Lead / PIMS Manager DEVE rever esta política em REG12 anualmente e no prazo de 30 dias após uma alteração material legal, de tratamento, tecnológica, do âmbito de certificação ou de controlo do PIMS.

11.1.2 [Both] The Process Owner / Business Owner DEVE rever anualmente as atividades de tratamento REG02 ativas quanto a alterações de dependências da conceção de privacidade e no prazo de 30 dias após uma alteração material do tratamento.

11.1.3 [Both] The System Owner / Application Owner DEVE rever anualmente a evidência de configuração de privacidade por defeito em REG04 e no prazo de 30 dias após uma alteração material do sistema.

11.1.4 [Both] The Vendor / Procurement Owner DEVE rever as obrigações de conceção de privacidade de fornecedores, subcontratantes, subcontratantes subsequentes e terceiros em REG08 antes da renovação e no prazo de 30 dias após uma alteração material da relação.

11.1.5 [Conditional] The Data Protection Officer / Privacy Advisor DEVE rever o impacto na privacidade de alterações materiais da política em REG12 antes da aprovação.

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

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 matéria de privacidade

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

12.4 PII04 - Política de aviso de privacidade e transparência

12.5 PII05 - Política de gestão de consentimento e 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 PII09 - Política de recolha, utilização, divulgação e partilha de PII

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

12.10 PII11 - Política de exatidão e qualidade de PII

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

12.12 PII13 - Política de transferências internacionais de PII

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

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

12.15 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 6.1.2; Clause 6.1.3** - Mapeadas para a triagem de riscos de privacidade, a ligação das ações de tratamento, a análise de dependências de conceção, o escalonamento e a ação corretiva, sem duplicar a metodologia completa de risco de privacidade e DPIA. Addressed by clauses [4.1.5; 4.3.1; 4.3.2; 4.3.4; 4.5.5; 5.1.3; 7.1.7].

13.2.2 **Clause 6.3; Clause 8.1** - Mapeadas para alterações de privacidade planeadas, início de projeto, revisão operacional de privacidade desde a conceção, controlo de entrada em produção e revisão de alterações materiais. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.3; 4.3.5; 4.5.1; 4.5.3; 4.5.4; 4.5.6; 7.1.2; 7.1.5; 10.1.2].

13.2.3 **Clause 7.5** - Mapeada para evidência documentada de privacidade desde a conceção retida em REG02, REG04, REG08 e REG12. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.2.3; 4.4.1; 4.4.2; 4.4.3; 5.1.2; 5.1.5; 5.1.6; 5.1.7; 7.1.1; 7.1.3; 7.1.4].

13.2.4 **Clause 9.1; Clause 10.2** - Mapeadas para métricas de conceção de privacidade, amostragem de evidência, registo de não conformidades, ação corretiva e verificação da eficácia. Addressed by clauses [4.3.6; 4.4.5; 4.5.5; 6.1.1; 6.1.2; 6.1.4; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 10.1.1; 10.1.5; 10.1.6].

13.2.5 **Annex A.1.2.2; Annex A.1.2.6; Annex A.1.2.9** - Mapeados para a documentação das finalidades do tratamento, registos de tratamento, ligação à conceção de privacidade e desencadeadores de triagem de risco de privacidade ou DPIA para tratamento pelo responsável pelo tratamento. Addressed by clauses [4.1.2; 4.2.1; 4.3.1; 4.4.2; 4.5.2; 5.1.5; 7.1.3; 11.1.2].

13.2.6 **Annex A.1.4.2; Annex A.1.4.3** - Mapeados para a limitação da recolha e do tratamento de PII através de requisitos mínimos de dados baseados na finalidade, tratamento opcional desligado por defeito e definições mínimas de tratamento por defeito. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.5.4; 7.1.5; 11.1.3].

13.2.7 **Annex A.1.4.4; Annex A.1.4.5** - Mapeados para o encaminhamento de dependências de exatidão, objetivos de minimização, viabilidade de desidentificação e evidência de conceção para minimizar PII identificável. Addressed by clauses [4.2.5; 4.2.7; 4.3.2; 4.5.2; 7.1.3; 11.1.2].

13.2.8 **Annex A.1.4.6; Annex A.1.4.7** - Mapeados para a identificação, na fase de conceção, de desidentificação, dependência de eliminação, artefactos temporários de PII e encaminhamento para controlos do ciclo de vida, sem duplicar a execução da retenção ou da eliminação. Addressed by clauses [4.2.5; 4.2.6; 4.2.7; 4.3.3; 4.5.4; 7.1.5; 11.1.3].

13.2.9 **Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7** - Mapeados para instruções de clientes ao subcontratante, informações de apoio ao cliente, registos de conceção do subcontratante e alterações de conceção do serviço autorizadas pelo cliente. Addressed by clauses [4.1.4; 4.4.1; 4.4.3; 4.4.6; 5.1.7; 7.1.4; 11.1.4].

13.2.10 **Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4** - Mapeados para capacidades de conceção do subcontratante relativas a ficheiros temporários, dependência de devolução ou eliminação e dependência de controlo de transmissão registadas como evidência de conceção, sem duplicar procedimentos operacionais de eliminação ou de controlos de segurança. Addressed by clauses [4.2.6; 4.2.7; 4.4.3; 4.4.4; 4.4.6; 7.1.4; 7.1.6; 11.1.4].

13.2.11 **Annex A.3.27; Annex A.3.29** - Mapeados para requisitos de privacidade no ciclo de vida de desenvolvimento, princípios de engenharia, pontos de controlo de proteção de PII e

evidência de configuração de privacidade por defeito. Addressed by clauses [4.1.6; 4.3.3; 4.3.4; 4.4.4; 4.5.1; 4.5.4; 5.1.4; 5.1.6; 7.1.5; 7.1.6; 10.1.2; 11.1.3].

13.3 GDPR

13.3.1 **Article 5(1)(b); Article 5(1)(c); Article 5(2)** - Mapeados para limitação da finalidade, conceção de PII mínima, ligação aos registos de tratamento, minimização por defeito, evidência e responsabilização. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.4.2; 4.5.2; 5.1.5; 8.1.1; 10.1.1].

13.3.2 **Article 24** - Mapeado para medidas do responsável pelo tratamento, revisão da governação, aprovação de exceções, ação corretiva e manutenção da política para implementação da privacidade desde a conceção. Addressed by clauses [4.1.3; 4.5.6; 5.1.1; 6.1.2; 9.1.2; 9.1.4; 10.1.5; 11.1.6].

13.3.3 **Article 25** - Mapeado para início do projeto, requisitos de privacidade na fase de conceção, definições de privacidade por defeito, minimização, verificações de conceção em aquisições, revisão de entrada em produção e revisão desencadeada por alterações. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.5; 4.4.1; 4.5.1; 4.5.3; 4.5.4; 10.1.2].

13.3.4 **Article 28** - Mapeado para instruções ao subcontratante, apoio à conceção pelo subcontratante, evidência de conceção de privacidade de fornecedores e alterações de conceção autorizadas pelo cliente. Addressed by clauses [4.1.4; 4.4.1; 4.4.3; 4.4.5; 4.4.6; 5.1.7; 7.1.4; 10.1.3; 11.1.4].

13.3.5 **Article 30** - Mapeado para ligação aos registos de tratamento, atualizações REG02, dependências de conceção das atividades de tratamento e evidência dos registos de tratamento. Addressed by clauses [4.1.2; 4.2.1; 4.4.2; 4.5.2; 5.1.5; 7.1.3; 11.1.2].

13.3.6 **Article 35** - Mapeado para desencadeadores de triagem de risco de privacidade e DPIA na fase de conceção, aconselhamento para alto risco e verificações pós-implementação, sem duplicar a metodologia de DPIA. Addressed by clauses [4.1.5; 4.3.1; 4.3.6; 5.1.3; 6.1.3; 9.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7** - Mapeada para a identificação de controlos de privacidade na fase de conceção, ligação ao risco de privacidade e evidência de conceção para implementação de controlos. Addressed by clauses [4.1.1; 4.1.3; 4.1.5; 4.3.1; 4.3.2; 4.3.3; 4.3.5; 4.5.1].

13.4.2 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Mapeadas para especificação da finalidade, limitação da recolha, minimização de dados, utilização limitada e definições de tratamento por defeito. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.4.2; 4.5.2].

13.4.3 **Clause 5.7; Clause 5.10; Clause 5.12** - Mapeadas para encaminhamento de dependências de exatidão, evidência de responsabilização, monitorização da conceção de privacidade, auditoria e ação corretiva. Addressed by clauses [4.2.7; 4.3.6; 4.5.5; 6.1.1; 6.1.4; 8.1.1; 8.1.2; 10.1.1; 10.1.6].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.8** - Mapeados para legitimidade da finalidade, limitação da recolha, minimização de dados, limitação da utilização e divulgação, dependência de retenção, tratamento de ficheiros temporários e controlos de conceção de dependências de exatidão. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 4.4.2; 4.5.2; 4.5.4; 7.1.3; 7.1.5].