					Insira aqui a designação da entidade jurídica registada							
Número do documento: PII16					Título do documento: **Política de formação, sensibilização e competência em privacidade**							
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 7.2; Clause 7.3	Both	Primary	Competência e sensibilização
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	Comunicação e evidência documentada
ISO/IEC 27701:2025	Clause 8.1; Clause 9.1; Clause 10.2	Both	Supporting	Controlo operacional, medição e melhoria
ISO/IEC 27701:2025	Annex A.3.17	Both	Primary	Sensibilização, educação e formação sobre o tratamento de PII
GDPR	Article 5(2); Article 24; Article 28; Article 32; Article 39	Both	Supporting	Responsabilização, governação de subcontratantes, segurança e tarefas do DPO
ISO/IEC 27001:2022	Clause 7.2; Clause 7.3; Annex A control 6.3	Both	Supporting	Competência, sensibilização e formação
ISO/IEC 27002:2022	Control 6.3	Both	Supporting	Orientações sobre sensibilização, educação e formação
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Segurança da informação e conformidade de privacidade

1. Âmbito

1.1 Esta política define os requisitos da organização para formação, sensibilização e competência em privacidade no âmbito do Sistema de Gestão da Informação de Privacidade.

1.2 Esta política aplica-se ao pessoal, contratados, trabalhadores temporários, terceiros relevantes, subcontratantes, subcontratantes subsequentes e outras partes interessadas cujo trabalho possa afetar o tratamento de PII, o desempenho do PIMS, os direitos dos titulares dos dados, o risco de privacidade, a segurança da informação relacionada com PII, as instruções aplicáveis a subcontratantes, os incidentes de privacidade, a informação documentada ou a evidência de conformidade.

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

1.4 Esta política abrange:

1.4.1 identificação do público-alvo da formação em privacidade;

1.4.2 formação de integração;

1.4.3 formação de reciclagem anual;

1.4.4 formação baseada em funções e formação desencadeada por eventos;

1.4.5 evidência de conclusão da formação;

1.4.6 escalonamento da não conclusão;

1.4.7 revisão da eficácia da formação;

1.4.8 evidência de garantia da formação de subcontratantes, subcontratantes subsequentes e terceiros.

1.5 Esta política não cria uma matriz de formação, painel de gestão de formação, registo de recursos humanos, registo de competências, registo disciplinar ou registo de formação de clientes separado. As atribuições de formação, conclusões, lembretes, evidência de competência e evidência de sensibilização são registadas em REG11, sendo as exceções, escalonamentos, não conformidades, ações corretivas e evidência de revisão registados em REG12. A evidência de garantia da formação de subcontratantes, subcontratantes subsequentes e terceiros é registada em REG08 quando relevante.

1.6 Esta política não duplica:

1.6.1 a atribuição de responsabilização por funções em PII02;

1.6.2 os requisitos de inventário de tratamento e de fundamento de licitude em PII03;

1.6.3 a metodologia de risco de privacidade e DPIA em PII07;

1.6.4 os gates de privacidade desde a conceção em PII08;

1.6.5 a governação do ciclo de vida de subcontratantes em PII12;

1.6.6 a operação de segurança de PII e de controlo de acesso em PII14;

1.6.7 o fluxo de trabalho de incidente de PII e de violação de dados em PII15;

1.6.8 a governação da informação documentada em PII17;

1.6.9 a governação da monitorização, auditoria interna e melhoria em PII18.

2. Finalidade

2.1 A finalidade desta política é assegurar que as pessoas cujo trabalho afeta o tratamento de PII compreendem as suas responsabilidades em matéria de privacidade, concluem formação adequada segundo uma periodicidade definida, mantêm competência relevante para a função e geram evidência auditável de formação, sensibilização e escalonamento.

2.2 Esta política apoia a implementação consistente do PIMS através da utilização de REG11 como objeto principal de evidência de formação e sensibilização e de REG08, REG10 e REG12 como objetos de evidência de suporte.

3. Objetivos

3.1 Os objetivos desta política são:

3.1.1 definir os públicos-alvo da formação em privacidade;

3.1.2 definir os requisitos de formação de integração;

3.1.3 definir os requisitos de formação de reciclagem anual;

3.1.4 definir os requisitos de formação em privacidade baseada em funções;

3.1.5 registar a evidência de conclusão em REG11;

3.1.6 escalonar a não conclusão através de REG12;

3.1.7 manter evidência de garantia da formação de subcontratantes, subcontratantes subsequentes e terceiros em REG08 quando relevante;

3.1.8 rever a eficácia da formação sem criar métricas excessivas ou registos duplicados;

3.1.9 assegurar que o conteúdo da formação permanece alinhado com as políticas PIMS atuais e com as obrigações materiais de privacidade.

4. Declarações da política

4.1 Público-alvo e atribuição da formação

4.1.1 [All] The Privacy Lead / PIMS Manager DEVE definir as categorias de público-alvo da formação PIMS em REG11 antes do início de cada ciclo anual de formação.

4.1.2 [All] The Process Owner / Business Owner DEVE identificar em REG11 o pessoal cujas funções envolvem o tratamento de PII antes da integração, da atribuição de função ou de uma alteração material das funções.

4.1.3 [Conditional] The System Owner / Application Owner DEVE identificar em REG11 os utilizadores que requerem formação em privacidade relativa a sistemas PII, acesso privilegiado ou administração antes de o acesso ser ativado ou materialmente alterado.

4.1.4 [Joint Controller] The Privacy Lead / PIMS Manager DEVE registar a repartição de responsabilidades de formação entre responsáveis conjuntos pelo tratamento em REG11 ou REG08 antes de a atividade de tratamento conjunto começar ou ser materialmente alterada.

4.1.5 [Conditional] The Data Protection Officer / Privacy Advisor DEVE identificar em REG11 necessidades reforçadas de formação em privacidade antes de a formação ser atribuída a funções que lidem com tratamento de alto risco, PII de categoria especial, direitos dos titulares dos dados, DPIAs, transferências internacionais ou avaliação da violação de dados pessoais.

4.1.6 [All] The Privacy Lead / PIMS Manager DEVE registar em REG11 o público-alvo da formação atribuído, o tipo de formação, a data de conclusão exigida e o proprietário da evidência antes do início de cada ciclo anual de formação.

4.2 Integração e periodicidade anual da formação

4.2.1 [All] The Privacy Lead / PIMS Manager DEVE atribuir formação básica de sensibilização para a privacidade em REG11 no prazo de 10 dias úteis após a integração de pessoal com acesso a PII ou responsabilidades PIMS.

4.2.2 [All] The Process Owner / Business Owner DEVE assegurar que o pessoal designado conclui a formação de integração em privacidade em REG11 antes de ser aprovado o acesso não supervisionado a PII ou no prazo de 30 dias após a integração, consoante o que ocorrer primeiro.

4.2.3 [All] The Privacy Lead / PIMS Manager DEVE atribuir formação de reciclagem anual em privacidade em REG11 pelo menos uma vez a cada 12 meses.

4.2.4 [All] The Process Owner / Business Owner DEVE confirmar em REG11 o estado de conclusão da formação de reciclagem anual do pessoal designado até à data limite anual publicada.

4.2.5 [Conditional] The Privacy Lead / PIMS Manager DEVE atribuir formação de reciclagem direcionada em REG11 no prazo de 30 dias após uma alteração material da política de privacidade, alteração material do processo PIMS, constatação de auditoria, falha recorrente na formação ou lição relevante decorrente de incidente 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] The Process Owner / Business Owner DEVE registar um pedido de exceção de formação em privacidade em REG12 antes de uma data limite de conclusão obrigatória ser prorrogada.

9.1.2 [All] The Privacy Lead / PIMS Manager DEVE aprovar ou rejeitar pedidos de exceção de formação em privacidade em REG12 antes de a exceção se tornar ativa.

9.1.3 [Conditional] The Data Protection Officer / Privacy Advisor DEVE aconselhar sobre exceções de formação em REG12 antes da aprovação quando a exceção afetar tratamento de alto risco, PII de categoria especial, tratamento de direitos, tratamento de incidentes, transferências internacionais ou evidência de certificação.

9.1.4 [Conditional] Top Management DEVE aprovar exceções de formação em privacidade em REG12 antes da ativação quando a exceção afetar não conclusão repetida, acesso privilegiado a PII, tratamento de PII de alto impacto ou evidência perante entidades reguladoras.

9.1.5 [All] The Privacy Lead / PIMS Manager DEVE definir em REG12 o proprietário da exceção, a data de expiração, a ação compensatória e a data de revisão antes de aprovar qualquer exceção de formação em privacidade.

9.1.6 [All] The Process Owner / Business Owner DEVE encerrar ou renovar exceções de formação em privacidade aprovadas em REG12 antes da data de expiração da exceção.

10. Aplicação

10.1.1 [All] The Privacy Lead / PIMS Manager DEVE registar uma não conformidade de formação em REG12 no prazo de cinco dias úteis quando a evidência de formação obrigatória em privacidade estiver em falta, incompleta, em atraso ou não for rastreável até REG11.

10.1.2 [All] The Process Owner / Business Owner DEVE assegurar que a formação obrigatória em privacidade em atraso é concluída ou escalonada em REG11 ou REG12 no prazo de 10 dias úteis após o registo do estado de atraso.

10.1.3 [Conditional] The System Owner / Application Owner DEVE restringir novos acessos a PII de alto impacto em REG12 quando a formação de integração ou baseada em funções exigida permanecer incompleta após escalonamento.

10.1.4 [Processor] The Vendor / Procurement Owner DEVE escalonar a evidência de garantia de formação de subcontratantes, subcontratantes subsequentes ou força de trabalho externa em falta em REG08 e REG12 no prazo de cinco dias úteis após a identificação.

10.1.5 [Conditional] The Incident Response Coordinator DEVE ligar as ações de aplicação relacionadas com formação a REG10 no prazo de um dia útil quando a falha de formação tiver contribuído para um incidente de PII suspeito ou confirmado.

10.1.6 [All] The Internal Audit / Compliance Reviewer DEVE verificar a evidência de encerramento das ações corretivas de formação em REG12 na próxima auditoria programada 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 e o conteúdo de formação pelo menos anualmente e registar o resultado da revisão em REG11 ou REG12.

11.1.2 [All] The Privacy Lead / PIMS Manager DEVE rever esta política no prazo de 30 dias após uma alteração material do âmbito do PIMS, legislação de privacidade, atividades de tratamento, modelo de funções, lições de incidentes, constatações de auditoria ou resultados de eficácia da formação.

11.1.3 [Conditional] The Data Protection Officer / Privacy Advisor DEVE rever alterações da política significativas para a privacidade em REG12 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 atualizar o conteúdo de formação e a evidência de atribuição em REG11 no prazo de 30 dias após uma alteração material aprovada da política.

12. Políticas relacionadas

12.1 Esta política deve ser lida em conjunto com:

12.2 PII01 - Política do Sistema de Gestão da Informação de Privacidade;

12.3 PII02 - Política de papéis, responsabilidades e responsabilização em 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 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 de PII e controlo de acesso;

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

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

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

13. Normas e referenciais de referência

13.1 ISO/IEC 27701:2025 - Clause 7.2; Clause 7.3; Clause 7.4. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 7.1.1; 7.1.2; 7.1.3; 11.1.1; 11.1.5].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.4; 4.6.5; 6.1.1; 6.1.2; 6.1.3; 6.1.5; 7.1.7; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 9.1.1; 9.1.2; 9.1.5; 10.1.1; 10.1.2; 10.1.6; 11.1.1; 11.1.2; 11.1.4].

13.3 ISO/IEC 27701:2025 - Annex A.3.17. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 11.1.5].

13.4 GDPR - Article 5(2); Article 24; Article 28; Article 32; Article 39. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.2.2; 4.2.3; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.4.4; 4.5.3; 4.5.4; 4.5.5; 5.1.1; 5.1.3; 5.1.7; 6.1.2; 6.1.3; 6.1.4; 7.1.4; 7.1.5; 9.1.3; 9.1.4; 10.1.3; 10.1.4; 10.1.5; 11.1.3].

13.5 ISO/IEC 27001:2022 - Clause 7.2; Clause 7.3; Annex A control 6.3. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 4.2.1; 4.2.3; 4.3.1; 4.3.5; 4.4.1; 4.4.3; 4.5.1; 4.5.2; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 6.1.1; 7.1.1; 7.1.2; 8.1.1; 8.1.2; 8.1.3; 11.1.1].

13.6 ISO/IEC 27002:2022 - Control 6.3. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 10.1.2].

13.7 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.5.5; 4.6.4; 4.6.5; 5.1.3; 6.1.2; 6.1.3; 6.1.5; 8.1.5; 9.1.3; 10.1.1; 10.1.6; 11.1.2].