					Insira aqui a designação da entidade jurídica registada							
Número do documento: PII06					Título do documento: **Política de gestão dos direitos dos titulares dos dados**							
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	Evidência de pedidos de exercício de direitos e controlo operacional
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitorização, não conformidade e ação corretiva
ISO/IEC 27701:2025	Annex A.1.3.2	Controller	Primary	Obrigações perante os titulares dos dados
ISO/IEC 27701:2025	Annex A.1.3.6; Annex A.1.3.7	Controller	Primary	Oposição, acesso, correção e apagamento
ISO/IEC 27701:2025	Annex A.1.3.8; Annex A.1.3.9	Controller	Primary	Notificação a terceiros e cópia da PII tratada
ISO/IEC 27701:2025	Annex A.1.3.10; Annex A.1.3.11	Controller	Primary	Tratamento de pedidos e obrigações relativas a decisões automatizadas
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Registos de tratamento do responsável pelo tratamento
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 a obrigações e registos do subcontratante
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Primary	Apoio do subcontratante às obrigações perante titulares dos dados
ISO/IEC 27701:2025	Annex A.3.14	Both	Supporting	Proteção dos registos de pedidos de exercício de direitos
GDPR	Article 5(1)(a); Article 5(2)	Controller	Supporting	Transparência e responsabilização

GDPR	Article 11; Article 12	Controller	Primary	Identificação, modalidades de pedido, prazos e governação da resposta
GDPR	Article 15; Article 16; Article 17	Controller	Primary	Acesso, retificação e apagamento
GDPR	Article 18; Article 19; Article 20	Controller	Primary	Limitação, notificação e portabilidade
GDPR	Article 21; Article 22	Controller	Primary	Oposição e decisões automatizadas
GDPR	Article 24	Controller	Supporting	Responsabilidade e medidas do responsável pelo tratamento
GDPR	Article 26	Joint Controller	Supporting	Repartição de direitos entre responsáveis conjuntos pelo tratamento
GDPR	Article 28	Both	Primary	Assistência do subcontratante em pedidos de exercício de direitos
GDPR	Article 30	Both	Supporting	Ligação aos registos de tratamento
GDPR	Article 32	Both	Supporting	Tratamento seguro da evidência de direitos e das divulgações
GDPR	Article 39	Conditional	Supporting	Aconselhamento e monitorização pelo EPD, quando aplicável
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.12	Both	Supporting	Transparência, participação individual, responsabilização e cumprimento
ISO/IEC 29151:2022	Annex A.10	Controller	Supporting	Participação e acesso dos titulares dos dados

1. Âmbito

1.1 Esta política define requisitos obrigatórios para a receção, validação, avaliação, cumprimento, recusa, prorrogação, encerramento, monitorização e comprovação dos pedidos de exercício de direitos dos titulares dos dados.

1.2 Esta política aplica-se a pedidos apresentados por titulares dos dados ou representantes autorizados relativos a acesso, retificação, apagamento, limitação, portabilidade, oposição, decisões automatizadas, encaminhamento de retirada do consentimento, reclamações e consultas relacionadas.

1.3 Esta política aplica-se a contextos de responsável pelo tratamento, responsável conjunto pelo tratamento, subcontratante e subcontratante subsequente. As obrigações de subcontratantes e subcontratantes subsequentes aplicam-se apenas quando a organização apoia um responsável pelo tratamento, cliente ou subcontratante a montante segundo instruções documentadas.

1.4 Esta política não substitui:

1.4.1 PII03 para o inventário de tratamento e os registos de fundamento de licitude;

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

1.4.3 PII05 para o cumprimento de consentimento e preferências;

1.4.4 PII10 para a execução da retenção, eliminação e descarte;

1.4.5 PII11 para a governação da exatidão e da qualidade;

1.4.6 PII12 para a governação do ciclo de vida de subcontratantes e subcontratantes subsequentes;

1.4.7 PII15 para o tratamento de incidentes e violações.

2. Finalidade

2.1 A finalidade desta política é assegurar que os pedidos de exercício de direitos dos titulares dos dados sejam tratados de forma consistente, lícita e segura, dentro de prazos definidos e com evidência adequada para auditoria.

2.2 Esta política assegura que a organização consegue demonstrar responsabilização pela receção de pedidos, verificação de identidade, avaliação, cumprimento, recusa, prorrogação, cooperação do subcontratante, encerramento e melhoria contínua.

3. Objetivos

3.1 Os objetivos desta política são:

3.1.1 Disponibilizar receção e acompanhamento consistentes para todos os pedidos de exercício de direitos dos titulares dos dados.

3.1.2 Verificar a identidade ou autoridade do requerente antes de qualquer divulgação, correção, eliminação, limitação ou portabilidade.

3.1.3 Avaliar os pedidos face aos registos de tratamento, à classificação do papel, às obrigações legais, às obrigações contratuais e à viabilidade técnica.

3.1.4 Cumprir pedidos válidos dentro dos prazos documentados.

3.1.5 Registar evidência de recusa, cumprimento parcial, prorrogação e encerramento.

3.1.6 Apoiar as obrigações do responsável pelo tratamento quando a organização atua como subcontratante ou subcontratante subsequente.

3.1.7 Proteger os registos de pedidos de exercício de direitos e os pacotes de resposta contra divulgação ou alteração não autorizada.

3.1.8 Monitorizar o desempenho dos pedidos de exercício de direitos e promover ações corretivas quando necessário.

4. Declarações da política

4.1 Receção, registo e classificação

4.1.1 [All] O Privacy Lead / PIMS Manager DEVE registar cada pedido de exercício de direitos do titular dos dados em REG06 no prazo de dois dias úteis após a receção.

4.1.2 [All] O Privacy Lead / PIMS Manager DEVE classificar em REG06 o tipo de pedido, o canal do pedido, a data do pedido, a referência de identidade do requerente, o proprietário designado, a data limite interna, a data limite legal ou contratual e o estado atual antes do início da avaliação.

4.1.3 [Controller] O Privacy Lead / PIMS Manager DEVE acusar a receção ou fornecer a próxima comunicação exigida ao requerente no prazo de cinco dias úteis após a receção e registar a comunicação em REG06.

4.1.4 [Controller] O Process Owner / Business Owner DEVE associar cada pedido à atividade de tratamento REG02 relevante antes de serem atribuídas ações de cumprimento.

4.1.5 [Joint Controller] O Privacy Lead / PIMS Manager DEVE identificar em REG02, REG06 ou REG08 a parte responsável conjunto pelo tratamento encarregada de tratar o pedido antes do início da avaliação substantiva.

4.1.6 [Processor] O Privacy Lead / PIMS Manager DEVE registar em REG06 e REG08 cada instrução do cliente relacionada com um pedido de exercício de direitos do titular dos dados antes do início da atividade de apoio.

4.1.7 [Subprocessor] O Vendor / Procurement Owner DEVE registar em REG06 ou REG08 cada instrução a montante relacionada com um pedido de exercício de direitos do titular dos dados antes do início da atividade de apoio do subcontratante subsequente.

4.1.8 [All] O Incident Response Coordinator DEVE registar um escalonamento REG10 no prazo de um dia útil quando um pedido de exercício de direitos indicar um possível incidente ou violação de PII.

4.2 Verificação de identidade, âmbito e avaliação

4.2.1 [Controller] O Privacy Lead / PIMS Manager DEVE verificar em REG06 a identidade do requerente ou a autoridade do representante antes de divulgar PII ou efetuar uma alteração solicitada.

4.2.2 [Controller] O Privacy Lead / PIMS Manager DEVE solicitar apenas a informação adicional mínima necessária para a verificação e registar o pedido em REG06 quando a identidade ou a autoridade for insuficiente.

4.2.3 [Controller] O Process Owner / Business Owner DEVE identificar em REG02 os sistemas, registos, finalidades, categorias de PII, destinatários e restrições de retenção relevantes antes de avaliar o cumprimento.

4.2.4 [Controller] O Data Protection Officer / Privacy Advisor DEVE rever em REG06 os pedidos de alto risco, contestados, pouco claros, excessivos, repetidos, recusados ou parcialmente cumpridos antes de a decisão ser comunicada.

4.2.5 [Controller] O System Owner / Application Owner DEVE verificar que os extratos de resposta propostos excluem PII não relacionada e dados não autorizados de terceiros antes da disponibilização do pacote de resposta.

4.2.6 [Controller] O Information Security Lead DEVE rever em REG06 ou REG12 o método de entrega da resposta antes da divulgação de PII de grande volume, sensível, de categoria especial ou de alto risco.

4.2.7 [Controller] O Data Protection Officer / Privacy Advisor DEVE rever em REG06 e REG04 os pedidos relacionados com decisões automatizadas ou definição de perfis antes do cumprimento, recusa ou escalonamento.

4.2.8 [Both] O Privacy Lead / PIMS Manager DEVE registar em REG06 o resultado da avaliação, o tipo de pedido aplicável, a decisão, a fundamentação e a próxima ação antes do cumprimento ou da recusa.

[... 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 solicitar uma exceção em REG12 antes de se desviar dos requisitos aprovados de receção, verificação, cumprimento, resposta ou encerramento de direitos.

9.1.2 [All] O Privacy Lead / PIMS Manager DEVE aprovar ou rejeitar em REG12 cada exceção de tratamento de direitos antes da implementação.

9.1.3 [Controller] O Data Protection Officer / Privacy Advisor DEVE rever qualquer exceção que envolva recusa, cumprimento parcial, incerteza de identidade, PII sensível, decisões automatizadas, pedidos relacionados com crianças ou tratamento de alto risco antes da aprovação.

9.1.4 [Both] O System Owner / Application Owner DEVE bloquear atividades de divulgação, correção, eliminação, limitação ou exportação quando uma exceção exigida não tiver sido aprovada em REG12 antes da ação.

9.1.5 [All] O Privacy Lead / PIMS Manager DEVE atribuir uma data de expiração, um proprietário e um controlo compensatório para cada exceção aprovada de tratamento de direitos em REG12 antes de a exceção se tornar ativa.

10. Aplicação

10.1.1 [All] O Privacy Lead / PIMS Manager DEVE registar uma não conformidade em REG12 no prazo de cinco dias úteis após identificar um registo de pedido de exercício de direitos vencido, em falta, incompleto, não verificado ou não suportado.

10.1.2 [Controller] O System Owner / Application Owner DEVE suspender a divulgação da resposta até que as verificações de identidade, autoridade e pacote de resposta estejam registadas em REG06.

10.1.3 [Both] O Vendor / Procurement Owner DEVE escalar em REG08 e REG12 a falta de cooperação de subcontratantes, subcontratantes subsequentes ou terceiros no prazo de cinco dias úteis após a identificação.

10.1.4 [All] Top Management DEVE atribuir a propriedade da ação corretiva em REG12 quando as falhas de pedidos de exercício de direitos forem sistémicas, repetidas ou relevantes para certificação.

10.1.5 [All] O Internal Audit / Compliance Reviewer DEVE verificar a evidência de encerramento das ações corretivas relacionadas com direitos em REG12 até à data limite atribuída.

10.1.6 [All] O Incident Response Coordinator DEVE iniciar uma revisão REG10 no prazo de um dia útil quando uma não conformidade de pedidos de exercício de direitos indicar divulgação não autorizada, perda, alteração, indisponibilidade ou outro incidente de PII suspeito.

11. Revisão e manutenção

11.1.1 [All] O Privacy Lead / PIMS Manager DEVE rever esta política anualmente e registar o resultado da revisão em REG12.

11.1.2 [All] O Privacy Lead / PIMS Manager DEVE rever esta política no prazo de 30 dias após alteração material à legislação sobre pedidos de exercício de direitos, ao âmbito das atividades de tratamento, às ferramentas de direitos, ao método de verificação de identidade, ao modelo de serviço do subcontratante ou aos requisitos de certificação PIMS.

11.1.3 [All] O Data Protection Officer / Privacy Advisor DEVE rever em REG12 alterações com significado para a privacidade nesta política 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] O Privacy Lead / PIMS Manager DEVE registar em REG11 a comunicação de alterações aprovadas à política no prazo de 30 dias após a publicação.

12. Políticas relacionadas

12.1 Esta política é suportada 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 privacidade

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

12.5 PII04 - Política de avisos de privacidade e transparência

12.6 PII05 - Política de gestão de consentimento e preferências

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, eliminação e descarte de PII

12.11 PII11 - Política de exatidão e qualidade da PII

12.12 PII12 - Política de gestão de 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 à PII

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

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

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

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 suporta os requisitos citados e identifica as cláusulas internas que os implementam ou suportam.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Mapeada para registos documentados de pedidos de exercício de direitos, fluxo de trabalho operacional de pedidos, verificação de identidade, cumprimento, resposta, encerramento e evidência de apoio por subcontratantes. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 4.2.1; 4.2.2; 4.2.3; 4.2.8; 4.3.10; 4.4.5; 7.1.1; 7.1.2; 7.1.3].

13.2.2 **Clause 9.1; Clause 10.2** - Mapeada para métricas de pedidos de exercício de direitos, monitorização de pedidos vencidos, amostragem de auditoria, registo de não conformidades, ação corretiva e verificação de eficácia. Addressed by clauses [4.5.6; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 10.1.1; 10.1.3; 10.1.4; 10.1.5].

13.2.3 **Annex A.1.3.2** - Mapeada para a determinação e o cumprimento de obrigações perante titulares dos dados através de categorias documentadas de direitos, canais de receção, verificação, avaliação, resposta e critérios de encerramento. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.2.8; 4.4.1; 4.4.4; 6.1.1; 7.1.1].

13.2.4 **Annex A.1.3.6; Annex A.1.3.7** - Mapeada para o tratamento de oposição, acesso, correção, apagamento e limitação, verificação, cumprimento e tratamento de exatidão contestada. Addressed by clauses [4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.6; 4.4.6].

13.2.5 **Annex A.1.3.8; Annex A.1.3.9** - Mapeada para a notificação de terceiros após resultados relativos a direitos e para a disponibilização de cópias ou pacotes de resposta portáveis. Addressed by clauses [4.3.5; 4.3.8; 4.5.5].

13.2.6 **Annex A.1.3.10; Annex A.1.3.11** - Mapeada para o tratamento documentado de pedidos legítimos, prazos, prorrogações, recusa, encerramento e revisão de pedidos relativos a decisões automatizadas. Addressed by clauses [4.1.2; 4.2.4; 4.2.7; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5].

13.2.7 **Annex A.1.2.9** - Mapeada para a associação de pedidos de exercício de direitos a registos de tratamento, finalidades do tratamento, sistemas, categorias, destinatários e restrições de retenção. Addressed by clauses [4.1.4; 4.2.3; 4.3.8; 7.1.3].

13.2.8 **Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7** - Mapeada para instruções em acordos com clientes, apoio do subcontratante às obrigações do cliente e registos do subcontratante relativos a atividades de apoio a direitos. Addressed by clauses [4.1.6; 4.1.7; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 7.1.7].

13.2.9 **Annex A.2.3.2** - Mapeada para os meios do subcontratante que suportam as obrigações do responsável pelo tratamento perante titulares dos dados, incluindo apoio à recuperação, correção, limitação, eliminação e exportação segundo instrução documentada. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 7.1.7].

13.2.10 **Annex A.3.14** - Mapeada para a proteção dos registos de pedidos de exercício de direitos, tratamento seguro dos pacotes de resposta, verificações de entrega da resposta e proteção da evidência de encerramento. Addressed by clauses [4.2.5; 4.2.6; 4.4.5; 4.4.7; 7.1.4; 7.1.5; 10.1.2].

13.3 GDPR

13.3.1 **Article 5(1)(a); Article 5(2)** - Mapeada para o tratamento transparente de direitos, evidência de responsabilização, registos de pedidos, registos de resposta, amostragem de auditoria e ação corretiva. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.4.4; 4.4.5; 8.1.5; 10.1.1].

13.3.2 **Article 11; Article 12** - Mapeada para identificação, informação adicional quando necessária, prazos de resposta, comunicações, prorrogação, recusa e encerramento de pedidos. Addressed by clauses [4.2.1; 4.2.2; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5].

13.3.3 **Article 15; Article 16; Article 17** - Mapeada para resultados de pesquisa de acesso, retificação, apagamento, verificação, evidência de cumprimento e entrega do pacote de resposta. Addressed by clauses [4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.5; 4.3.10].

13.3.4 **Article 18; Article 19; Article 20** - Mapeada para limitação, notificação dos resultados relativos a direitos às partes relevantes e entrega de portabilidade ou cópia. Addressed by clauses [4.3.4; 4.3.5; 4.3.8; 4.5.5].

13.3.5 **Article 21; Article 22** - Mapeada para avaliação de oposição e revisão de pedidos relativos a decisões automatizadas ou definição de perfis. Addressed by clauses [4.2.7; 4.3.6; 4.3.7].

13.3.6 **Article 24** - Mapeada para medidas de governação do responsável pelo tratamento, papéis, propriedade do fluxo de trabalho, revisão, exceções, ação corretiva e supervisão pela gestão do tratamento de direitos. Addressed by clauses [5.1.1; 5.1.2; 6.1.1; 6.1.3; 6.1.4; 9.1.1; 9.1.2; 10.1.4; 11.1.1].

13.3.7 **Article 26** - Mapeada para a identificação da responsabilidade do responsável conjunto pelo tratamento pelo tratamento de pedidos antes do início da avaliação substantiva. Addressed by clauses [4.1.5; 6.1.5].

13.3.8 **Article 28** - Mapeada para assistência por subcontratantes e subcontratantes subsequentes, instruções documentadas do cliente, prazos de apoio, ausência de resposta direta sem autorização e escalonamento de falta de cooperação. Addressed by clauses [4.1.6; 4.1.7; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.6; 6.1.6].

13.3.9 **Article 30** - Mapeada para a associação de pedidos de exercício de direitos a registos de tratamento, atividades de tratamento, sistemas, categorias de PII, destinatários e registos de subcontratantes. Addressed by clauses [4.1.4; 4.2.3; 4.3.8; 4.5.1; 7.1.3].

13.3.10 **Article 32** - Mapeada para tratamento seguro de pedidos de exercício de direitos, proteção da entrega de respostas, prevenção de divulgação não autorizada e proteção da evidência de direitos. Addressed by clauses [4.2.5; 4.2.6; 7.1.4; 7.1.5; 10.1.2; 10.1.6].

13.3.11 **Article 39** - Mapeada para aconselhamento e monitorização pelo Data Protection Officer / Privacy Advisor relativamente a pedidos de exercício de direitos de alto risco, contestados, recusados, prorrogados e relacionados com decisões automatizadas. Addressed by clauses [4.2.4; 4.2.7; 4.3.7; 4.4.3; 6.1.3; 9.1.3; 11.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.12** - Mapeada para transparência dos canais de direitos, participação e acesso individuais, responsabilização, procedimentos de reclamação/reparação, monitorização do cumprimento de privacidade e evidência de auditoria. Addressed by clauses [4.1.3; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.8; 4.4.6; 7.1.1; 8.1.5; 10.1.1].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.10** - Mapeada para participação e acesso dos titulares dos dados, verificação de identidade, acesso, retificação, eliminação, atualizações de estado, apoio do subcontratante e mecanismos de reclamação/reparação. Addressed by clauses [4.1.1; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.4.4; 4.5.1; 4.5.4; 8.1.6].

13.6 Requisitos internos

13.6.1 Requisito interno - As cláusulas que definem REG06 como o principal objeto de evidência de direitos, formação, aprovação de fluxos de trabalho não normalizados, expiração de exceções, revisão da política e comunicação de alterações à política suportam a consistência da implementação, mas não estão diretamente mapeadas para uma única cláusula externa. Addressed by clauses [5.1.2; 6.1.7; 7.1.6; 9.1.4; 9.1.5; 11.1.2; 11.1.4; 11.1.5].