					Insira aqui a designação da entidade jurídica registada							
Número do documento: PII07					Título do documento: **Política de avaliação de riscos de privacidade e AIPD**							
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 6.1.1	Both	Primary	Riscos e oportunidades do PIMS
ISO/IEC 27701:2025	Clause 6.1.2	Both	Primary	Avaliação de riscos de privacidade
ISO/IEC 27701:2025	Clause 6.1.3	Both	Primary	Tratamento de riscos de privacidade e ligação à SoA
ISO/IEC 27701:2025	Clause 6.3	Both	Supporting	Alterações planeadas ao PIMS e reavaliação de riscos
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Informação documentada sobre riscos de privacidade e AIPD
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Planeamento e controlo operacional
ISO/IEC 27701:2025	Clause 8.2	Both	Primary	Avaliação operacional de riscos de privacidade
ISO/IEC 27701:2025	Clause 8.3	Both	Primary	Tratamento operacional de riscos de privacidade
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Monitorização e medição de riscos de privacidade
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Revisão pela gestão dos riscos de privacidade
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Não conformidade relacionada com riscos e ação corretiva
ISO/IEC 27701:2025	Annex A.1.2.6	Controller	Primary	Avaliação de impacto sobre a privacidade

ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Registos de tratamento que suportam a avaliação de riscos
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Acordo com cliente do subcontratante e assistência em AIPD
ISO/IEC 27701:2025	Annex A.2.2.6	Processor	Supporting	Informação do subcontratante que suporta o cumprimento pelo cliente
GDPR	Article 5(2)	Controller	Supporting	Evidência de responsabilização
GDPR	Article 24	Controller	Supporting	Responsabilidade e medidas do responsável pelo tratamento
GDPR	Article 25	Controller	Supporting	Proteção de dados desde a conceção e por defeito
GDPR	Article 28	Both	Supporting	Assistência e instruções relativas ao subcontratante
GDPR	Article 30	Both	Supporting	Registos de tratamento que suportam a AIPD
GDPR	Article 32	Both	Supporting	Risco de segurança e salvaguardas
GDPR	Article 35	Controller	Primary	Avaliação de impacto sobre a proteção de dados
GDPR	Article 36	Controller	Primary	Consulta prévia
GDPR	Article 39	Conditional	Supporting	Aconselhamento e monitorização pelo DPO quando aplicável
ISO/IEC 29100:2020	Clause 4.7; Clause 5.11; Clause 5.12	Both	Supporting	Controlos de privacidade, segurança da informação e conformidade de privacidade

ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Primary	Âmbito, benefícios, desencadeador e preparação da PIA
ISO/IEC 29151:2022	Clause 4.1; Clause 4.2	Both	Supporting	Programa de proteção de PII e identificação de requisitos
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 6.4; Clause 6.5; Clause 6.6; Clause 6.7	Both	Supporting	Integração da gestão organizacional de riscos de privacidade

1. Âmbito

1.1 Esta política define os requisitos de avaliação de riscos de privacidade, triagem para AIPD, execução de AIPD completa, tratamento de riscos, aceitação do risco residual, consulta, revisão e gestão de evidência para o tratamento de PII no âmbito do PIMS.

1.2 Esta política aplica-se a:

1.2.1 atividades de tratamento de PII novas e materialmente alteradas;

1.2.2 contextos de tratamento como responsável pelo tratamento, responsável conjunto pelo tratamento, subcontratante e subcontratante subsequente;

1.2.3 sistemas, aplicações, serviços, processos de negócio, fornecedores, subcontratantes, subcontratantes subsequentes, transferências internacionais e acordos de partilha de dados que afetem o tratamento de PII;

1.2.4 evidência de riscos de privacidade e de AIPD mantida em REG04 e evidência de suporte mantida em REG02, REG03, REG08, REG09, REG10, REG11 e REG12.

1.3 Esta política não substitui os controlos de inventário de tratamento, controlos de avisos de privacidade, controlos de consentimento, controlos de direitos dos titulares dos dados, controlos de privacidade desde a conceção, controlos de fornecedores, controlos de transferências internacionais, controlos de segurança de PII, controlos de incidentes, controlos de informação documentada nem controlos de monitorização/auditoria/melhoria. Esses requisitos são definidos nas políticas relacionadas indicadas na Secção 12.

1.4 Para efeitos desta política, avaliação de riscos de privacidade significa a identificação, análise, avaliação, tratamento, revisão e monitorização documentados dos potenciais impactos adversos na privacidade decorrentes do tratamento de PII.

1.5 Para efeitos desta política, AIPD significa uma avaliação documentada utilizada para tratamento como responsável pelo tratamento que seja suscetível de resultar em risco elevado para os titulares dos dados e que avalia a necessidade do tratamento, a proporcionalidade, os riscos, as salvaguardas, o risco residual, as necessidades de consulta e as condições de aprovação.

1.6 Para efeitos desta política, risco residual de privacidade elevado significa um risco de privacidade que permanece acima do limiar de aceitação aprovado após o tratamento de riscos proposto ou implementado.

1.7 Para efeitos desta política, uma alteração material significa qualquer alteração que afete o âmbito do PIMS, a finalidade do tratamento, o fundamento de licitude, as categorias de PII, as categorias de titulares dos dados, a escala do tratamento, a tecnologia de tratamento, a monitorização ou definição de perfis, decisões automatizadas, titulares dos dados vulneráveis, destinatários, subcontratantes, subcontratantes subsequentes, transferências internacionais, retenção, controlos de segurança, perfil de risco, instruções de clientes ou âmbito de certificação.

2. Finalidade

2.1 A finalidade desta política é assegurar que os riscos de privacidade e as obrigações de AIPD são identificados, avaliados, tratados, aprovados, revistos e evidenciados antes de o tratamento de PII criar risco inaceitável para os titulares dos dados ou para o PIMS.

2.2 Esta política permite à organização demonstrar governação da privacidade baseada no risco, responsabilização do responsável pelo tratamento quanto à AIPD, assistência do subcontratante na AIPD, tratamento de riscos documentado, aprovação do risco residual, tomada de decisão sobre consulta prévia e melhoria contínua dos controlos de privacidade.

3. Objetivos

3.1 Os objetivos desta política são:

3.1.1 definir desencadeadores obrigatórios de triagem de riscos de privacidade;

3.1.2 definir quando é exigida uma AIPD completa;

3.1.3 assegurar que as decisões de AIPD do responsável pelo tratamento são documentadas e passíveis de revisão;

3.1.4 assegurar que a assistência em AIPD prestada por subcontratantes e subcontratantes subsequentes é documentada quando exigida por instrução ou acordo do cliente;

3.1.5 assegurar que os riscos de privacidade são avaliados antes de avançar com tratamento de PII novo ou materialmente alterado;

3.1.6 assegurar que os tratamentos de riscos de privacidade são atribuídos, implementados e verificados;

3.1.7 assegurar que riscos residuais de privacidade elevados são escalados e aprovados antes de o tratamento começar ou continuar;

3.1.8 assegurar que as decisões de consulta prévia são documentadas quando persistir risco residual elevado;

3.1.9 assegurar que a evidência de riscos de privacidade e de AIPD é mantida em REG04 e ligada aos objetos de evidência relacionados;

3.1.10 evitar a criação de registos separados de AIPD, riscos ou consulta fora de REG04.

4. Declarações da política

4.1 Triagem de riscos de privacidade

4.1.1 [Both] The Process Owner / Business Owner MUST iniciar a triagem de riscos de privacidade em REG04 antes de começar o tratamento de PII novo ou materialmente alterado registado em REG02.

4.1.2 [Both] The Privacy Lead / PIMS Manager MUST manter os critérios de triagem de riscos de privacidade em REG04 antes da operação inicial do PIMS e, posteriormente, anualmente.

4.1.3 [Controller] The Process Owner / Business Owner MUST concluir a triagem para AIPD em REG04 antes de começar o tratamento como responsável pelo tratamento que cumpra os critérios de triagem de riscos de privacidade.

4.1.4 [Processor] The Vendor / Procurement Owner MUST registar os requisitos de assistência em AIPD do cliente em REG08 antes de começar o tratamento como subcontratante, quando o acordo com o cliente ou a instrução documentada exigir suporte à AIPD.

4.1.5 [Both] The System Owner / Application Owner MUST fornecer evidência de conceção do sistema, acesso, segurança, registo e fluxos de dados em REG04 antes da aprovação da avaliação de riscos de privacidade para sistemas novos ou materialmente alterados que tratem PII.

4.1.6 [Both] The Privacy Lead / PIMS Manager MUST registar o resultado da triagem e a fundamentação da decisão de AIPD completa em REG04 antes de a atividade de tratamento prosseguir.

4.2 Desencadeadores de AIPD e determinação do requisito

4.2.1 [Controller] The Privacy Lead / PIMS Manager MUST exigir uma AIPD completa em REG04 antes de começar o tratamento como responsável pelo tratamento suscetível de resultar em risco elevado.

4.2.2 [Controller] The Process Owner / Business Owner MUST encaminhar o tratamento que envolva grande escala, monitorização sistemática, definição de perfis, decisões automatizadas, categorias especiais de PII, dados relativos a condenações penais ou infrações, titulares dos dados vulneráveis, tecnologia inovadora ou tratamento materialmente alterado para o Privacy Lead / PIMS Manager em REG04 antes de o tratamento começar.

4.2.3 [Controller] The Data Protection Officer / Privacy Advisor MUST registar aconselhamento em REG04 antes da aprovação de uma decisão sobre o requisito de AIPD completa para tratamento de elevado risco como responsável pelo tratamento.

4.2.4 [Both] The Process Owner / Business Owner MUST voltar a triar o risco de privacidade em REG04 antes de utilizar PII para uma nova finalidade, adicionar um novo destinatário, introduzir um novo subcontratante ou subcontratante subsequente, alterar a arquitetura do sistema ou iniciar uma nova transferência internacional.

4.2.5 [Processor] The Privacy Lead / PIMS Manager MUST documentar se é exigido suporte de AIPD pelo subcontratante em REG08 no prazo de 10 dias úteis após receber um pedido de assistência em AIPD do cliente.

4.2.6 [Subprocessor] The Vendor / Procurement Owner MUST documentar os requisitos de assistência em AIPD a montante em REG08 antes de começar o subtratamento, quando o acordo com o cliente a montante ou com o subcontratante exigir essa assistência.

[... 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 relativas a riscos de privacidade e AIPD

9.1.1 [All] The Process Owner / Business Owner MUST solicitar qualquer exceção a esta política em REG12 antes de ocorrer o desvio.

9.1.2 [All] The Privacy Lead / PIMS Manager MUST avaliar o impacto de cada exceção solicitada na privacidade, no plano jurídico, na certificação, na operação e nos titulares dos dados em REG04 ou REG12 no prazo de 10 dias úteis após o pedido.

9.1.3 [All] The Data Protection Officer / Privacy Advisor MUST registar aconselhamento em REG12 antes da aprovação de qualquer exceção que afete tratamento de elevado risco, conclusão de AIPD completa, consulta prévia, risco residual de privacidade elevado ou assistência em AIPD ao cliente.

9.1.4 [All] Top Management MUST aprovar exceções de riscos de privacidade ou AIPD que afetem tratamento de elevado risco, âmbito de certificação, consulta prévia ou risco residual de privacidade elevado não resolvido em REG12 antes de a exceção produzir efeitos.

9.1.5 [All] The Privacy Lead / PIMS Manager MUST definir em REG12 uma data de expiração não superior a 90 dias para cada exceção aprovada de riscos de privacidade ou AIPD antes da aprovação.

9.1.6 [All] The Process Owner / Business Owner MUST encerrar ou reavaliar cada exceção de riscos de privacidade ou AIPD em REG12 no prazo de cinco dias úteis após a expiração.

10. Aplicação

10.1 Aplicação da política de riscos de privacidade e AIPD

10.1.1 [All] The Privacy Lead / PIMS Manager MUST registar evidência de riscos de privacidade ou AIPD em REG04 em falta, inexata, incompleta, em atraso ou não aprovada como não conformidade em REG12 no prazo de cinco dias úteis após a identificação.

10.1.2 [Controller] The Process Owner / Business Owner MUST suspender novo tratamento de elevado risco como responsável pelo tratamento quando a evidência exigida de aprovação de AIPD em REG04 estiver em falta antes do lançamento.

10.1.3 [Both] The System Owner / Application Owner MUST bloquear a entrada em produção de sistemas que tratem PII quando a evidência exigida de tratamento de riscos em REG04 estiver em falta antes da aprovação da entrada em produção.

10.1.4 [Both] The Vendor / Procurement Owner MUST bloquear a integração de fornecedores, subcontratantes, subcontratantes subsequentes ou partilha de dados quando a evidência exigida de riscos de privacidade ou assistência em AIPD em REG04 estiver em falta antes da aprovação do acordo.

10.1.5 [All] Top Management MUST rever não conformidades relevantes de riscos de privacidade ou AIPD não resolvidas em REG12 durante a revisão pela gestão.

10.1.6 [All] The Privacy Lead / PIMS Manager MUST escalar incumprimentos repetidos de prazos de triagem em REG04, revisão de AIPD ou tratamento de riscos para Top Management em REG12 no prazo de cinco dias úteis após a segunda ocorrência num período de 12 meses.

10.1.7 [All] The Internal Audit / Compliance Reviewer MUST verificar a eficácia das ações corretivas relativas a não conformidades de riscos de privacidade e AIPD em REG12 na auditoria agendada seguinte ou no prazo de 60 dias após o encerramento, consoante o que ocorrer primeiro.

11. Revisão e manutenção

11.1 Revisão e manutenção da política

11.1.1 [All] The Privacy Lead / PIMS Manager MUST rever esta política em REG12 anualmente e no prazo de 30 dias após alteração material aos requisitos de riscos de privacidade, AIPD, consulta prévia, assistência por subcontratantes ou certificação.

11.1.2 [All] The Privacy Lead / PIMS Manager MUST rever anualmente em REG12 os critérios de triagem em REG04, critérios de desencadeamento de AIPD, critérios de classificação de risco e critérios de aceitação do risco residual.

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

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

11.1.5 [All] The Privacy Lead / PIMS Manager MUST atualizar REG03 e REG04 no prazo de 15 dias úteis após alterações aprovadas à política que alterem a aplicabilidade de controlos, critérios de risco ou requisitos de triagem para AIPD.

11.1.6 [All] The Privacy Lead / PIMS Manager MUST registar a comunicação das alterações aprovadas a esta política em REG11 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 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 de direitos dos titulares dos dados

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 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 e violações de PII

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 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 6.1.1** - Mapeada para a identificação e o planeamento de ações relativas a riscos e oportunidades de privacidade através de critérios de triagem, limiares de risco, escalonamento e contributos para a revisão pela gestão. Addressed by clauses [4.1.2; 4.4.5; 4.5.6; 6.1.1; 6.1.2; 8.1.2].

13.2.2 **Clause 6.1.2** - Mapeada para a realização de triagem de riscos de privacidade, avaliação de riscos de privacidade, classificação de risco, reavaliação e avaliação de desencadeadores de AIPD antes de avançar com tratamento novo ou materialmente alterado. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.6; 4.2.1; 4.2.4; 4.3.1; 4.3.7; 4.6.1].

13.2.3 **Clause 6.1.3** - Mapeada para o planeamento do tratamento de riscos de privacidade, atualizações da aplicabilidade de controlos, implementação de tratamentos, aceitação do risco residual e ligação à SoA. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 6.1.5; 7.1.7; 11.1.5].

13.2.4 **Clause 6.3** - Mapeada para alterações planeadas ao PIMS e ao tratamento que desencadeiam a reavaliação de riscos de privacidade e a revisão de AIPD. Addressed by clauses [4.2.4; 4.6.1; 11.1.1].

13.2.5 **Clause 7.5** - Mapeada para informação documentada controlada relativa a triagem de riscos de privacidade, evidência de AIPD, tratamento de riscos, aceitação do risco residual, decisões de consulta prévia, exceções, não conformidades e evidência de revisão da política. Addressed by clauses [4.1.6; 4.3.7; 4.4.1; 4.5.1; 5.1.2; 7.1.1; 9.1.1; 10.1.1; 11.1.1].

13.2.6 **Clause 8.1** - Mapeada para a operação dos controlos de riscos de privacidade e AIPD antes da entrada em produção, integração, aprovação de tratamento, encerramento de tratamento e ligação a ações corretivas. Addressed by clauses [4.1.1; 4.1.5; 7.1.2; 7.1.3; 7.1.4; 7.1.5; 7.1.6; 7.1.7; 7.1.8].

13.2.7 **Clause 8.2** - Mapeada para a avaliação operacional de riscos de privacidade em alterações de tratamento novas, alteradas, de sistema, fornecedor, transferência e motivadas por incidentes. Addressed by clauses [4.1.1; 4.2.4; 4.3.1; 4.3.5; 4.5.5; 4.6.1].

13.2.8 **Clause 8.3** - Mapeada para o tratamento operacional de riscos de privacidade, atribuição de tratamentos, implementação de tratamentos, escalonamento de tratamentos em atraso e verificação da eficácia. Addressed by clauses [4.4.1; 4.4.3; 4.4.4; 4.4.6; 4.4.7; 8.1.3; 10.1.7].

13.2.9 **Clause 9.1** - Mapeada para a monitorização e medição da cobertura de triagem, estado de AIPD, riscos em aberto, ações de tratamento em atraso, ações de fornecedores, ações de tratamento de segurança, ações de reavaliação de incidentes e constatações de auditoria. Addressed by clauses [4.6.3; 4.6.4; 4.6.5; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 8.1.7; 8.1.8].

13.2.10 **Clause 9.3** - Mapeada para a revisão pela gestão de riscos residuais de privacidade elevados, ações de tratamento em atraso, estado de AIPD completa, decisões de consulta prévia e exceções relevantes de riscos de privacidade. Addressed by clauses [4.6.6; 6.1.1; 6.1.2; 6.1.3; 10.1.5].

13.2.11 **Clause 10.2** - Mapeada para não conformidades de riscos de privacidade e AIPD, exceções, abertura de ações corretivas, escalonamento e verificação da eficácia. Addressed by clauses [4.4.6; 9.1.1; 9.1.2; 9.1.4; 9.1.6; 10.1.1; 10.1.5; 10.1.6; 10.1.7].

13.2.12 **Annex A.1.2.6** - Mapeada para a avaliação da necessidade de uma avaliação de impacto sobre a privacidade, e a sua implementação quando apropriado, para tratamento novo ou alterado como responsável pelo tratamento. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.3.2; 4.5.1; 4.6.2; 7.1.4; 10.1.2].

13.2.13 **Annex A.1.2.9** - Mapeada para registos de tratamento que suportam os contributos de avaliação de riscos de privacidade e AIPD, incluindo finalidade, categorias, sistemas, destinatários, transferências e fornecedores. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.2.14 **Annex A.2.2.2** - Mapeada para acordos com clientes do subcontratante e obrigações de assistência em AIPD ao cliente. Addressed by clauses [4.1.4; 4.2.5; 4.5.4; 5.1.7; 7.1.6].

13.2.15 **Annex A.2.2.6** - Mapeada para a disponibilização pelo subcontratante de informação necessária ao cumprimento pelo cliente, incluindo assistência em AIPD e evidência de suporte ao cliente. Addressed by clauses [4.2.5; 4.2.6; 4.5.4; 8.1.5].

13.3 GDPR

13.3.1 **Article 5(2)** - Mapeado para evidência de responsabilização relativa a triagem para AIPD, decisões de AIPD completa, tratamento de riscos, aceitação do risco residual, decisões de consulta prévia, exceções, constatações de auditoria e ações corretivas. Addressed by clauses [4.1.6; 4.3.7; 4.4.5; 4.5.1; 4.6.4; 10.1.1; 10.1.7].

13.3.2 **Article 24** - Mapeado para a responsabilidade do responsável pelo tratamento por medidas adequadas de riscos de privacidade, revisão de risco residual elevado, aprovação pela gestão e manutenção da política. Addressed by clauses [4.4.5; 4.5.3; 6.1.2; 10.1.5; 11.1.4].

13.3.3 **Article 25** - Mapeado para evidência de privacidade desde a conceção e privacidade por defeito utilizada na avaliação de riscos e antes da aprovação da entrada em produção. Addressed by clauses [4.1.5; 4.3.4; 7.1.5].

13.3.4 **Article 28** - Mapeado para assistência em AIPD por subcontratantes e subcontratantes subsequentes, tratamento de instruções de clientes e evidência de tratamento de riscos de fornecedores. Addressed by clauses [4.1.4; 4.2.5; 4.2.6; 4.4.4; 4.5.4; 7.1.6; 8.1.5].

13.3.5 **Article 30** - Mapeado para registos de tratamento que suportam os contributos para avaliação de riscos de privacidade e AIPD. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.3.6 **Article 32** - Mapeado para contributos de riscos de segurança de PII, seleção de salvaguardas, tratamento de riscos de segurança e atualizações do estado dos controlos de segurança. Addressed by clauses [4.1.5; 4.3.3; 4.4.2; 8.1.6].

13.3.7 **Article 35** - Mapeado para triagem para AIPD, determinação do requisito de AIPD completa, conteúdo da AIPD, aconselhamento do DPO, revisão e bloqueio de tratamento de elevado risco sem a aprovação de AIPD exigida. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.3.2; 4.3.6; 4.5.1; 4.6.2; 7.1.4; 10.1.2].

13.3.8 **Article 36** - Mapeado para a tomada de decisão sobre consulta prévia, aconselhamento do DPO, aprovação por Top Management e ações de continuação, suspensão, reformulação ou consulta quando persistir risco residual elevado. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 6.1.2].

13.3.9 **Article 39** - Mapeado para aconselhamento e monitorização pelo Data Protection Officer / Privacy Advisor, quando aplicável, relativamente a decisões de AIPD, tratamento de elevado risco, consulta prévia e alterações à política. Addressed by clauses [4.2.3; 4.3.6; 4.5.2; 5.1.3; 6.1.3; 9.1.3; 11.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7; Clause 5.11; Clause 5.12** - Mapeada para identificação de controlos de privacidade, salvaguardas de segurança, conformidade de privacidade, evidência de riscos de privacidade, monitorização e revisão. Addressed by clauses [4.3.3; 4.4.1; 4.4.2; 4.4.7; 4.6.3; 4.6.5; 8.1.6; 10.1.7].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 1; Clause 5.1; Clause 6.2; Clause 6.3** - Mapeada para o âmbito do processo de PIA, benefícios, determinação de desencadeadores, preparação, contributos da avaliação, evidência de partes interessadas e estrutura do relatório de AIPD mantidos em REG04. Addressed by clauses [4.1.1; 4.1.3; 4.1.6; 4.2.1; 4.3.1; 4.3.2; 4.3.7; 7.1.1].

13.6 ISO/IEC 29151:2022

13.6.1 **Clause 4.1; Clause 4.2** - Mapeada para requisitos do programa de proteção de PII, identificação de requisitos de proteção de PII, seleção de controlos baseada no risco e ligação ao tratamento de riscos de privacidade. Addressed by clauses [4.3.3; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 6.1.5].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 6.4; Clause 6.5; Clause 6.6; Clause 6.7** - Mapeada para princípios organizacionais de riscos de privacidade, liderança, integração, avaliação de riscos, tratamento de riscos, monitorização e revisão, e registo e reporte. Addressed by clauses [4.1.2; 4.3.1; 4.3.7; 4.4.1; 4.4.5; 4.6.3; 4.6.4; 5.1.1; 6.1.1; 6.1.2; 8.1.1; 8.1.3].