					Insira aqui a designação da entidade jurídica registada							
Número do documento: PII24					Título do documento: **Política de privacidade de CCTV e monitorização física**							
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	Controlos documentados e operacionais
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.1.2.3; Annex A.1.2.6; Annex A.1.2.9	Controller	Primary	Finalidade, fundamento de licitude, desencadeador de risco e registos
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Repartição relativa ao subcontratante e ao responsável conjunto pelo tratamento
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10	Controller	Supporting	Obrigações perante titulares dos dados e pedidos
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5; Annex A.1.4.8; Annex A.1.4.9	Controller	Primary	Recolha, tratamento, minimização, retenção e eliminação
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5	Controller	Primary	Registos e pedidos de divulgação
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7	Processor	Supporting	Acordos com subcontratantes, instruções, suporte e registos
ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Direitos do subcontratante e suporte à divulgação
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Proteção de registos e logging
GDPR	Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)	Controller	Primary	Princípios e responsabilização
GDPR	Article 6	Controller	Primary	Fundamento de licitude

GDPR	Article 12; Article 13; Article 14	Controller	Primary	Transparência e avisos
GDPR	Article 15; Article 16; Article 17; Article 18; Article 21	Controller	Supporting	Pedidos de exercício de direitos
GDPR	Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Governação, subcontratantes, registos, segurança, DPIA e aconselhamento
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Controller	Supporting	Finalidade, recolha, minimização, retenção e divulgação
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Transparência, participação, responsabilização, segurança e conformidade
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2	Controller	Supporting	Risco de privacidade e desencadeadores de DPIA
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Both	Supporting	Controlos de privacidade para proteção de PII
ISO/IEC 29151:2022	Clause 9.2.3; Clause 9.4.2; Clause 11.1.3	Both	Supporting	Controlos de acesso e de entrada física
ISO/IEC 27002:2022	Controls 5.34; 7.2; 7.4; 8.2; 8.3; 8.15	Both	Supporting	PII, monitorização física, restrição de acesso e logging

1. Âmbito

1.1 Esta política aplica-se a CCTV, videovigilância, monitorização de visitantes, registos de controlo de acesso físico, registos de monitorização operada por vigilantes, sistemas de monitorização das instalações e atividades de monitorização física relacionadas que recolham ou de outra forma tratem PII.

1.2 Esta política aplica-se às organizações que atuam como responsáveis pelo tratamento de PII relativamente às suas próprias instalações e atividades de monitorização física.

1.3 Esta política aplica-se também a atividades de suporte de subcontratante ou subcontratante subsequente quando a organização opera, aloja, revê, armazena, divulga, apaga ou de outra forma trata imagens de videovigilância, dados de visitantes ou registos de acesso físico em nome de um cliente.

1.4 Esta política abrange a definição da finalidade da monitorização, aprovação, aviso e sinalização, restrições de acesso, divulgação, retenção, apagamento, outsourcing, escalonamento de incidentes, encaminhamento de pedidos de exercício de direitos, revisão e gestão de evidência.

1.5 Esta política não fornece aconselhamento em matéria de direito laboral, comentário jurídico sobre comissões de trabalhadores, procedimento de aplicação da lei ou um registo dedicado de CCTV.

1.6 A evidência específica de monitorização é mantida nos objetos canónicos de evidência do PIMS identificados nesta política.

2. Finalidade

2.1 A finalidade desta política é estabelecer controlos de privacidade para CCTV e monitorização física, para que as atividades de monitorização tenham finalidade definida, sejam transparentes, proporcionais, sujeitas a controlo de acesso, retidas por períodos definidos, divulgadas apenas por canais aprovados e suportadas por evidência PIMS auditável.

2.2 Esta política apoia o tratamento consistente de imagens de videovigilância, registos de visitantes, registos de acesso físico e PII de monitorização relacionada, sem criar registos adicionais, comités, painéis de gestão ou funções não canónicas.

3. Objetivos

3.1 Os objetivos desta política são:

3.1.1 definir as finalidades da monitorização e o âmbito do tratamento antes do início da monitorização;

3.1.2 documentar as atividades de CCTV, acesso físico, monitorização de visitantes e monitorização física em REG02;

3.1.3 identificar as atividades de monitorização que exigem revisão de risco de privacidade ou triagem para DPIA em REG04;

3.1.4 manter evidência de aviso e sinalização transparentes em REG07;

3.1.5 restringir o acesso, visualização, exportação, divulgação e retenção de PII de monitorização;

3.1.6 encaminhar pedidos de titulares dos dados através de REG06;

3.1.7 gerir prestadores de monitorização externalizada e evidência de partilha de dados através de REG08;

3.1.8 escalonar incidentes suspeitos relativos a PII associada à monitorização através de REG10;

3.1.9 registar revisões, exceções, não conformidades, ações corretivas, constatações de auditoria e melhorias em REG12.

4. Declarações da política

4.1 Inventário, finalidade e aprovação da monitorização

4.1.1 [Controller] O Process Owner / Business Owner DEVE registar cada atividade de CCTV, monitorização de visitantes, registo de controlo de acesso físico ou monitorização física em REG02 antes do início da atividade.

4.1.2 [Controller] O Privacy Lead / PIMS Manager DEVE validar a entrada em REG02 quanto aos campos de finalidade, fundamento de licitude, local monitorizado, categorias de PII, categorias de titulares dos dados, retenção, aviso, acesso e divulgação antes da ativação de uma atividade de monitorização nova ou materialmente alterada.

4.1.3 [Controller] O Process Owner / Business Owner DEVE registar em REG02 as zonas monitorizadas aprovadas, zonas excluídas e limites de recolha antes de serem ativadas câmaras, sensores, registos de visitantes ou registo de controlo de acesso.

4.1.4 [Conditional] O Process Owner / Business Owner DEVE obter uma decisão de risco de privacidade em REG04 antes de ativar monitorização que envolva monitorização sistemática, gravação de áudio, identificação biométrica, deteção com recurso a analytics, locais sensíveis, pessoas vulneráveis ou monitorização não evidente.

4.1.5 [Joint Controller] O Privacy Lead / PIMS Manager DEVE registar em REG08 a repartição de responsabilidades pela monitorização conjunta antes do início da monitorização partilhada com um senhorio, parceiro de facilities, cliente ou outro responsável conjunto pelo tratamento.

4.1.6 [Processor] O Privacy Lead / PIMS Manager DEVE registar em REG08 as instruções de monitorização do cliente e os limites permitidos de tratamento antes de tratar imagens de videovigilância, registos de visitantes ou registos de acesso físico em nome de um cliente.

4.2 Aviso e transparência

4.2.1 [Controller] O Process Owner / Business Owner DEVE assegurar que a evidência de sinalização de monitorização ou de aviso equivalente just-in-time é registada em REG07 antes de as áreas monitorizadas serem abertas aos titulares dos dados.

4.2.2 [Controller] O Privacy Lead / PIMS Manager DEVE associar cada aviso de monitorização em REG07 à finalidade do tratamento correspondente em REG02 antes da publicação ou de alteração material.

4.2.3 [Processor] O Privacy Lead / PIMS Manager DEVE fornecer informações de suporte ao aviso de monitorização em REG08 quando a organização opera serviços de monitorização segundo instruções do cliente.

4.2.4 [Conditional] O Process Owner / Business Owner DEVE registar medidas alternativas de transparência em REG07 e REG04 antes da ativação de monitorização não evidente ou de emergência.

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

9. Exceções

9.1 [All] O Privacy Lead / PIMS Manager DEVE registar em REG12 cada exceção a esta política antes de a exceção ser utilizada.

9.2 [Conditional] O Data Protection Officer / Privacy Advisor DEVE documentar aconselhamento de privacidade em REG04 ou REG12 antes da aprovação de exceções que envolvam monitorização não evidente, gravação de áudio, identificação biométrica, monitorização com recurso a analytics ou locais de monitorização sensíveis.

9.3 [All] A Top Management DEVE aprovar em REG12 exceções superiores a 90 dias antes da prorrogação para além do período inicial da exceção.

9.4 [All] O Privacy Lead / PIMS Manager DEVE rever exceções de monitorização em aberto em REG12 pelo menos mensalmente até ao encerramento.

10. Aplicação

10.1 [All] O Privacy Lead / PIMS Manager DEVE registar falhas de controlos de monitorização como não conformidades em REG12 no prazo de cinco dias úteis após a confirmação.

10.2 [Both] O Information Security Lead DEVE suspender o acesso não autorizado a sistemas de monitorização no prazo de um dia útil após a confirmação e registar a ação em REG10 ou REG12.

10.3 [All] A Top Management DEVE atribuir a titularidade de ações corretivas em REG12 no prazo de 10 dias úteis para violações repetidas ou materiais da política.

10.4 [Conditional] O Incident Response Coordinator DEVE iniciar o fluxo de trabalho de incidente de PII em REG10 após suspeita de divulgação não autorizada, perda ou comprometimento de PII de monitorização.

11. Revisão e manutenção

11.1 [All] O Privacy Lead / PIMS Manager DEVE rever esta política e a evidência de monitorização relacionada em REG12 pelo menos anualmente.

11.2 [Controller] O Process Owner / Business Owner DEVE revalidar cada finalidade de monitorização ativa, aviso, âmbito de localização e entrada de retenção em REG02 e REG07 pelo menos anualmente.

11.3 [Both] O System Owner / Application Owner DEVE revalidar os controlos de acesso, logging, apagamento e exportação dos sistemas de monitorização em REG12 pelo menos anualmente e após alteração material do sistema.

11.4 [Conditional] O Vendor / Procurement Owner DEVE revalidar a evidência de fornecedores de monitorização externalizada em REG08 pelo menos anualmente e antes da renovação contratual.

11.5 [All] O Privacy Lead / PIMS Manager DEVE atualizar a evidência relacionada em REG02, REG04, REG07, REG08, REG10 ou REG12 no prazo de 30 dias de calendário após alterações aprovadas à política.

12. Políticas relacionadas

12.1 PII02 - Política de papéis, responsabilidades e responsabilização em matéria de privacidade

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

12.3 PII04 - Política de aviso de privacidade e transparência

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

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

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

12.7 PII09 - Política de recolha, utilização, divulgação e partilha de PII

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

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

12.10 PII13 - Política de transferência internacional de PII

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

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

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

12.14 PII18 - Política de monitorização, auditoria e melhoria do PIMS

12.15 PII19 - Política de privacidade dos trabalhadores

12.16 PII21 - Política de privacidade de IA e decisões automatizadas

12.17 PII23 - Política de subcontratante de PII na nuvem

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** - Mapeada para evidência documentada de monitorização, planeamento operacional, controlos de ativação, registos de finalidade, ligação ao aviso, configuração de acesso, configuração de retenção e controlo de alterações para atividades de CCTV e monitorização física. Addressed by clauses [4.1.1; 4.1.2; 4.2.2; 4.3.1; 4.4.1; 6.2; 7.1; 11.5].

13.2.2 **Clause 9.1; Clause 10.2** - Mapeada para medição de controlos de monitorização, revisão de fornecedores, revisão de acessos, constatações de auditoria, não conformidades, ações corretivas, escalonamento de ações vencidas e evidência de melhoria. Addressed by clauses [4.6.4; 6.4; 6.5; 6.6; 8.1; 8.7; 10.1; 11.1].

13.2.3 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9** - Mapeada para definição da finalidade de monitorização pelo responsável pelo tratamento, documentação do fundamento de licitude, decisões sobre desencadeadores de risco de privacidade e registos de atividades de tratamento de monitorização em REG02 e REG04. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.4.1; 6.2; 7.1; 11.2].

13.2.4 **Annex A.1.2.7; Annex A.1.2.8** - Mapeada para repartição relativa a fornecedores de monitorização externalizada, repartição de responsabilidades pela monitorização conjunta e evidência de subcontratante ou responsável conjunto pelo tratamento em REG08. Addressed by clauses [4.1.5; 4.6.1; 4.6.2; 5.7; 6.2; 7.6].

13.2.5 **Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10** - Mapeada para obrigações perante titulares dos dados relacionadas com monitorização, encaminhamento de pedidos, preservação necessária para avaliar pedidos e evidência de governação para suporte aos direitos. Addressed by clauses [4.5.1; 4.5.2; 5.2; 7.2; 11.5].

13.2.6 **Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5; Annex A.1.4.8; Annex A.1.4.9** - Mapeada para limitação da recolha de monitorização, limites de tratamento, minimização, períodos de retenção, apagamento, sobrescrita, suspensões da eliminação e controlo de cópias extraídas. Addressed by clauses [4.1.3; 4.3.1; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 7.3; 7.5; 8.4].

13.2.7 **Annex A.1.5.4; Annex A.1.5.5** - Mapeada para registos de divulgação externa, tratamento de pedidos de divulgação, minimização antes da divulgação e divulgações ligadas a incidentes que envolvam PII de monitorização. Addressed by clauses [4.3.4; 4.5.4; 7.8; 10.4].

13.2.8 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7** - Mapeada para instruções de cliente ao subcontratante, limites permitidos de tratamento, suporte a avisos, instruções de retenção e apagamento, assistência em matéria de direitos e registos de subcontratante para serviços de monitorização externalizados. Addressed by clauses [4.1.6; 4.2.3; 4.4.5; 4.5.3; 4.6.3].

13.2.9 **Annex A.2.3.2; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6** - Mapeada para suporte do subcontratante às obrigações do cliente, autorização de divulgação, registos de divulgação, notificação de pedidos de divulgação e tratamento de divulgações juridicamente vinculativas relativas a PII de monitorização. Addressed by clauses [4.3.5; 4.5.3; 4.6.2; 4.6.3].

13.2.10 **Annex A.3.14; Annex A.3.25** - Mapeada para proteção de registos de monitorização, acesso restrito, revisão de acessos privilegiados, registo de acessos, contenção de acesso não autorizado e evidência de logging para sistemas de monitorização. Addressed by clauses [4.3.2; 4.3.3; 4.5.5; 5.4; 7.4; 10.2; 11.3].

13.3 GDPR

13.3.1 **Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)** - Mapeada para licitude, lealdade, transparência, limitação da finalidade, minimização de dados, limitação da conservação e evidência de responsabilização para atividades de monitorização. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.4.1; 4.4.2; 4.4.3; 6.1; 8.1; 11.2].

13.3.2 Article 6 - Mapeada para documentação do fundamento de licitude para CCTV, monitorização de visitantes, registos de acesso físico e outras atividades de monitorização física. Addressed by clauses [4.1.2; 4.1.4; 7.1].

13.3.3 **Article 12; Article 13; Article 14** - Mapeada para avisos transparentes de monitorização, evidência de sinalização, ligação do aviso às finalidades do tratamento, informações de suporte a avisos prestadas pelo subcontratante e medidas alternativas de transparência. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 7.2; 8.2; 11.2].

13.3.4 **Article 15; Article 16; Article 17; Article 18; Article 21** - Mapeada para acesso, retificação, apagamento, limitação, oposição, encaminhamento de pedidos, preservação necessária para avaliar pedidos e assistência ao cliente relacionada com monitorização. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 7.8; 11.5].

13.3.5 **Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39** - Mapeada para governação do responsável pelo tratamento, repartição entre responsáveis conjuntos pelo tratamento, governação de subcontratantes, registos de tratamento, segurança de sistemas de monitorização, revisão de risco de privacidade, desencadeadores de DPIA e aconselhamento de privacidade. Addressed by clauses [4.1.4; 4.1.5; 4.1.6; 4.3.2; 4.3.3; 4.5.4; 4.6.1; 4.6.2; 4.6.4; 5.1; 5.3; 6.3; 8.5; 10.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Mapeada para especificação da finalidade, limitação da recolha, minimização de dados, limitação da utilização, limitação da retenção e limitação da divulgação de PII de monitorização. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.4; 4.4.1; 4.4.2; 4.4.4; 7.8].

13.4.2 **Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12** - Mapeada para transparência, participação individual, responsabilização, segurança da informação, revisão de conformidade, revisão de acessos, encaminhamento de direitos, escalonamento de incidentes e evidência de ações corretivas. Addressed by clauses [4.2.1; 4.2.2; 4.3.2; 4.3.3; 4.5.1; 4.5.4; 6.1; 8.7; 10.1].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 5.1; Clause 6.2** - Mapeada para risco de privacidade e triagem de desencadeadores de DPIA para monitorização física sistemática, não evidente, com áudio, biométrica, com recurso a analytics, em local sensível, envolvendo pessoas vulneráveis ou outra monitorização física de maior risco. Addressed by clauses [4.1.4; 4.2.4; 5.3; 6.3; 7.5; 9.2].

13.6 ISO/IEC 29151:2022

13.6.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10** - Mapeada para controlos de proteção de PII relativos a finalidade, recolha, minimização, retenção, divulgação e participação dos titulares dos dados em contextos de monitorização. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.4.1; 4.4.3; 4.5.1; 7.2; 8.2].

13.6.2 **Clause 9.2.3; Clause 9.4.2; Clause 11.1.3** - Mapeada para provisionamento de acessos, restrição de acesso à informação e controlos de entrada física relevantes para o acesso a sistemas de monitorização e registos de controlo de acesso físico. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.5.5; 5.4; 7.4; 10.2; 11.3].

13.7 ISO/IEC 27002:2022

13.7.1 Controls 5.34; 7.2; 7.4; 8.2; 8.3; 8.15 - Mapeada para privacidade e proteção de PII, entrada física, monitorização de segurança física, acesso privilegiado, restrição de acesso à informação e controlos de logging para sistemas de CCTV e monitorização física. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.5.5; 5.4; 7.3; 7.4; 8.3; 10.2; 11.3].