					Insira aqui a designação da entidade jurídica registada							
Número do documento: P17S					Título do documento: **Política de Proteção de Dados e 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**

Alinhamento com normas e regulamentos

Norma/Regulamento	Cláusula/Artigo	Comentário
ISO/IEC 27001:2022	Cláusulas 5.1, 6.1.3, 8	
ISO/IEC 27002:2022	Controlos 5.34, 8.10–8	
NIST SP 800-53 Rev.5	AR-2, PL-5, AC-6, IR-4	
RGPD da UE	Artigo 5, 6, 12-23, 30, 32-34	
Diretiva NIS2 da UE	Artigo 21(2)(e), 21(2)(f)	
DORA da UE	Artigos 6, 15, 17	
COBIT 2019	APO12, DSS05, MEA	

1. Finalidade

1.1. A presente política define a forma como a organização protege os dados pessoais em conformidade com obrigações legais, requisitos regulamentares e normas internacionais de segurança.

1.2. Assegura que os dados pessoais — de clientes, trabalhadores ou parceiros — são recolhidos, utilizados, armazenados e eliminados de forma lícita, leal e segura.

1.3. Esta política permite igualmente o cumprimento da ISO/IEC 27001:2022 e apoia a demonstração de conformidade em auditoria através da aplicação de uma abordagem consistente e baseada no risco à proteção da privacidade.

1.4. Através desta política, a organização demonstra responsabilização e reforça a confiança dos clientes ao dar prioridade à transparência, à minimização de dados e a uma governação robusta da privacidade.

2. Âmbito

2.1. Esta política aplica-se a:

2.1.1. Todos os trabalhadores, contratados ou prestadores de serviços que acedam, tratem ou gerem dados pessoais

2.1.2. Qualquer sistema, aplicação ou local onde os dados pessoais sejam armazenados ou transmitidos

2.1.3. Todos os dados pessoais, quer armazenados eletronicamente, em papel, em sistemas alojados na nuvem ou em dispositivos móveis

2.2. Esta política aplica-se a dados relativos a clientes, trabalhadores, fornecedores e quaisquer outros indivíduos identificáveis.

2.3. A política mantém-se em vigor independentemente de os dados serem tratados internamente ou por prestadores de serviços terceiros.

3. Objetivos

3.1. Assegurar que os dados pessoais são tratados de acordo com a legislação em matéria de privacidade e as normas de segurança, incluindo o RGPD da UE, a Diretiva NIS2 da UE e a ISO/IEC 27001.

3.2. Proteger os dados pessoais contra acessos não autorizados, utilização indevida, alteração ou perda através de controlos técnicos e organizacionais claramente definidos.

3.3. Respeitar os direitos de privacidade dos titulares dos dados, incluindo os direitos de acesso, retificação e apagamento dos seus dados.

3.4. Estabelecer papéis e responsabilidades claros para a proteção de dados no seio da organização.

3.5. Aplicar a minimização de dados, a retenção segura e a eliminação atempada em todos os sistemas e processos.

3.6. Reduzir o risco de incumprimento, sanções legais, danos reputacionais ou perda de confiança dos clientes.

4. Papéis e responsabilidades

4.1. Diretor-Geral (DG)

4.1.1. Aprova esta política e assegura a sua aplicação

4.1.2. Disponibiliza os recursos necessários para gerir riscos de privacidade e responder a incidentes

4.1.3. Detém a responsabilidade global pelo cumprimento da legislação e das normas aplicáveis em matéria de privacidade

4.2. Coordenador de Privacidade (interno ou externalizado)

4.2.1. Mantém os registos das atividades de tratamento de dados

4.2.2. Responde a pedidos dos titulares dos dados e a solicitações das autoridades reguladoras

4.2.3. Apoia as avaliações de risco, a formação e a implementação da política

4.2.4. Documenta violações de dados pessoais e notifica as autoridades competentes quando exigido

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

9. Requisitos de revisão e atualização

9.1. Revisões programadas

9.1.1. Esta política deve ser revista pelo menos uma vez em cada 12 meses pelo Coordenador de Privacidade e aprovada pelo Diretor-Geral

9.1.2. A revisão deve avaliar a relevância da política, o alinhamento regulamentar e a eficácia operacional

9.2. Fatores desencadeadores de revisão intercalar

9.2.1. As atualizações da política devem também ser iniciadas em resposta a:

9.2.1.1. Legislação nova ou revista em matéria de proteção de dados (por exemplo, RGPD da UE, DORA da UE)

9.2.1.2. Incidentes de segurança ou violações de privacidade envolvendo dados pessoais

9.2.1.3. Implementação de novos sistemas, ferramentas ou serviços que tratem dados pessoais

9.2.1.4. Constatações materiais de auditoria ou recomendações da autoridade reguladora

9.3. Controlo de alterações e comunicação

9.3.1. Todas as alterações à política devem ser formalmente documentadas num registo de alterações

9.3.2. As versões revistas devem ser distribuídas a todos os trabalhadores e contratados aplicáveis

9.3.3. As versões arquivadas devem ser conservadas para efeitos de rasto de auditoria da conformidade

10. Políticas relacionadas e articulações

10.1. Esta política funciona em articulação com outras políticas SME para criar um quadro de privacidade completo e aplicável:

10.1.1. P13S – Política de Classificação e Rotulagem de Dados: Assegura que os dados pessoais são classificados de forma adequada para que as proteções de privacidade possam ser aplicadas com base no risco.

10.1.2. P14S – Política de Conservação e Eliminação de Dados: Define regras claras sobre durante quanto tempo os dados pessoais devem ser mantidos e os métodos seguros para a sua eliminação após expiração.

10.1.3. P16S – Política de Mascaramento e Pseudonimização de Dados: Especifica como os identificadores pessoais devem ser transformados antes de os dados serem utilizados em ambiente de não produção ou partilhados externamente.

10.1.4. P30S – Política de Resposta a Incidentes: Abrange as etapas necessárias para responder a violações de dados, incluindo a notificação a reguladores e a indivíduos afetados dentro dos prazos exigidos.

10.1.5. P2S – Política de Papéis e Responsabilidades de Governação: Clarifica a estrutura de responsabilização e os papéis de tomada de decisão aplicáveis à aplicação e supervisão da privacidade.

10.2. Estas políticas relacionadas devem ser revistas e aplicadas em conjunto para assegurar uma cobertura de privacidade de ponta a ponta em sistemas, pessoal e fornecedores.

11. Normas e quadros de referência

11.1. ISO/IEC 27001

11.1.1. Cláusula 5.1 – Exige que a Alta Direção demonstre liderança e compromisso na proteção de dados pessoais.

11.1.2. Cláusula 6.1.3 – Determina o tratamento dos riscos relacionados com o tratamento de informações pessoais.

11.1.3. Cláusula 8.1 – Exige a implementação de controlos operacionais para salvaguardar os dados ao longo do seu ciclo de vida.

11.2. ISO/IEC 27002

11.2.1. Controlo 5.34 – Fornece orientações de implementação sobre a proteção da privacidade e o tratamento seguro de informações pessoalmente identificáveis (PII).

11.2.2. Controlo 8.10 – Trata da eliminação segura de dados pessoais para evitar divulgação residual.

11.2.3. Controlo 8.11 – Apoia a utilização de mascaramento e pseudonimização para minimização de dados.

11.2.4. Controlo 8.12 – Previne fugas de dados não autorizadas através de controlos sobre o acesso e a utilização dos dados.

11.3. NIST SP 800-53 Rev.5

11.3.1. AR-2 – Atribui papéis e responsabilidades para a gestão do risco de privacidade.

11.3.2. PL-5 – Exige documentação do plano de privacidade que abranja a utilização e a proteção de dados.

11.3.3. AC-6 – Determina o princípio do menor privilégio e os controlos de acesso para dados pessoais.

11.3.4. IR-4 – Exige processos de tratamento de incidentes para violações que envolvam dados pessoais.

11.4. RGPD da UE

11.4.1. Artigo 5 – Define os princípios fundamentais do tratamento de dados lícito, leal e transparente.

11.4.2. Artigo 6 – Exige fundamento jurídico válido para cada atividade de tratamento de dados pessoais.

11.4.3. Artigos 12–23 – Estabelecem os direitos dos titulares dos dados, incluindo acesso, retificação, apagamento e oposição.

11.4.4. Artigo 30 – Determina os registos das atividades de tratamento.

11.4.5. Artigo 32 – Exige medidas técnicas e organizativas de segurança adequadas.

11.4.6. Artigos 33–34 – Definem obrigações de notificação de violações às autoridades e aos titulares dos dados.

11.5. Diretiva NIS2 da UE

11.5.1. Artigo 21(2)(e) – Exige medidas para assegurar a proteção de dados alinhada com as políticas de cibersegurança.

11.5.2. Artigo 21(2)(f) – Determina mecanismos para gerir a segurança de dados pessoais e confidenciais em sistemas TIC.

11.6. DORA da UE

11.6.1. Artigo 6 – Exige quadros internos de governação que assegurem a gestão do risco e a proteção dos dados.

11.6.2. Artigo 15 – Obriga as entidades financeiras a assegurar que os prestadores terceiros protegem os dados pessoais e apoiam o cumprimento regulamentar.

11.6.3. Artigo 17 – Exige que as organizações assegurem que os sistemas TIC que tratam dados pessoais são seguros, resilientes e monitorizados.

11.7. COBIT 2019

11.7.1. APO12 – Gerir o Risco: Exige a identificação e o tratamento dos riscos de privacidade e de proteção de dados.

11.7.2. DSS05 – Gerir Serviços de Segurança: Determina salvaguardas para prevenir acessos não autorizados a dados pessoais.

11.7.3. MEA03 – Monitorizar, Avaliar e Analisar a Conformidade: Exige que as organizações assegurem o cumprimento contínuo da legislação de privacidade e de proteção de dados.