					Insira aqui a designação da entidade jurídica registada							
Número do documento: P17					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, 8.1, 10	Controlos gerais, técnicos e de melhoria contínua relevantes para a proteção de dados
ISO/IEC 27002:2022	Controlos 5.34, 8.10, 8.11, 8.12	Controlos para o tratamento de informações pessoais identificáveis (PII), retenção, eliminação, anonimização e direitos dos titulares dos dados
NIST SP 800-53 Rev.5	AR-1, AR-2, AR-4, AR-5; PL-2, PL-8; AC-2, AC-6; AU-2, AU-6, AU-9; IR-4, IR-5, IR-6; PM-1, PM-21, PM-23	Requisitos de governação, risco, gestão de acessos, registo, resposta a violações e programa de privacidade
RGPD da UE	Artigos 5, 6, 12–23, 25, 28, 30, 32–34; Considerando 78	Todos os requisitos nucleares de privacidade, responsabilização, direitos dos titulares, pedidos dos titulares, violações e princípios de proteção de dados desde a conceção e por defeito
Diretiva NIS2 da UE	Artigo 21(2)(e), (f)	Controlos de segurança baseados no risco para entidades essenciais e importantes
DORA da UE	Artigos 6(2)(d), 11(1)(c), 15(1), 17	Governação, risco de terceiros e prazos para tratamento seguro
COBIT 2019	APO12, DSS01, DSS05, MEA	Gestão de riscos, operações seguras e supervisão da conformidade

1. Finalidade

1.1 A presente política estabelece princípios organizacionais obrigatórios e requisitos técnicos para a proteção de dados pessoais e a aplicação da privacidade desde a conceção em todos os ambientes.

1.2 Formaliza as responsabilidades da organização ao abrigo de normas internacionais e quadros regulamentares, assegurando que os dados pessoais são recolhidos, tratados, conservados, partilhados e eliminados de forma lícita, segura e transparente.

1.3 A presente política reforça ainda o cumprimento da legislação e dos quadros de privacidade aplicáveis, incluindo o Regulamento Geral sobre a Proteção de Dados da UE (RGPD), a Diretiva NIS2 da UE, o DORA da UE, a ISO/IEC 27001:2022 e o COBIT 2019.

2. Âmbito

2.1 A presente política aplica-se a todas as unidades organizacionais, pessoas e sistemas envolvidos no tratamento de dados pessoais, incluindo:

2.1.1 trabalhadores, contratados, consultores e prestadores de serviços terceiros.

2.1.2 dados recolhidos de fontes internas e externas em todas as funções de negócio.

2.1.3 suportes físicos e digitais, incluindo serviços na nuvem, plataformas SaaS, dispositivos móveis e registos em papel.

2.1.4 todos os ambientes, incluindo produção, desenvolvimento, teste e sistemas de cópias de segurança onde possam existir dados pessoais.

2.2 Abrange todas as atividades de tratamento reguladas pela legislação e normas de privacidade aplicáveis, incluindo, entre outras:

2.2.1 recolha, armazenamento, utilização, transmissão e eliminação de dados pessoais.

2.2.2 aplicação dos direitos dos titulares dos dados, documentação do fundamento de licitude e gestão do consentimento.

2.2.3 transferências transfronteiriças, notificação de violações e partilha de dados com terceiros.

2.2.4 conceção segura e aplicação da privacidade por defeito em sistemas e processos.

3. Objetivos

3.1 Assegurar o tratamento lícito, transparente e responsável dos dados pessoais em alinhamento com a ISO/IEC 27001:2022 e com as obrigações legais associadas.

3.2 Incorporar os princípios de privacidade desde a conceção e privacidade por defeito em todos os sistemas de informação, serviços e processos de negócio.

3.3 Aplicar medidas técnicas e organizativas (TOMs) que salvaguardem a confidencialidade, integridade e disponibilidade dos dados pessoais ao longo de todo o seu ciclo de vida.

3.4 Definir papéis de governação e estruturas de responsabilização para a proteção de dados, incluindo as responsabilidades do Encarregado da Proteção de Dados (EPD), da Segurança da Informação, da área Jurídica e dos Proprietários de Dados designados.

3.5 Permitir o pleno cumprimento dos artigos 5, 6, 25, 30 e 32 do RGPD, bem como dos requisitos de redução do risco e resiliência ao abrigo da NIS2 e do DORA.

3.6 Assegurar os direitos dos titulares dos dados, incluindo acesso, retificação, apagamento, limitação, portabilidade, oposição e proteção contra decisões automatizadas.

3.7 Mitigar riscos regulamentares, reputacionais, jurídicos e operacionais decorrentes de acesso não autorizado, utilização indevida ou perda de dados pessoais.

4. Papéis e responsabilidades

4.1 Alta Direção

4.1.1 Exerce supervisão estratégica e atribui recursos suficientes para suportar o programa de privacidade.

4.1.2 Aprova a presente política e assegura a sua aplicação em toda a organização.

4.2 Encarregado da Proteção de Dados (EPD)

4.2.1 Atua com independência para supervisionar a conformidade com os regulamentos de proteção de dados.

4.2.2 Mantém o Registo de Atividades de Tratamento (RoPA), nos termos do artigo 30 do RGPD.

4.2.3 Lidera a interação com as autoridades reguladoras, conduz Avaliações de Impacto sobre a Proteção de Dados (AIPD) e gere os processos de notificação de violações.

4.2.4 Revê exceções de privacidade e mantém o Registo de Exceções de Privacidade.

[... 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 A presente política deve ser revista, pelo menos, anualmente, ou antecipadamente nas seguintes condições:

9.1.1 atualizações legais ou regulamentares significativas (por exemplo, alterações ao RGPD ou prazos do DORA).

9.1.2 novos sistemas ou atividades de tratamento que envolvam dados pessoais.

9.1.3 constatações de auditoria interna que indiquem lacunas na política.

9.1.4 incidentes de violação materiais ou feedback das autoridades de controlo.

9.2 Responsabilidades de revisão

9.2.1 O EPD deve iniciar a revisão da política, coordenando-se com Jurídico, Risco, Segurança da Informação e Alta Direção.

9.2.2 Todas as atualizações devem ser registadas no Registo de Controlo Documental do SGSI e distribuídas às partes interessadas afetadas.

9.3 Controlo de alterações

9.3.1 Qualquer revisão da presente política deve ser formalmente aprovada pela Alta Direção.

9.3.2 As versões obsoletas devem ser arquivadas em segurança, e a versão atualizada deve incluir um histórico de alterações documentado.

10. Políticas relacionadas e interligações

10.1 P1 – Política de Segurança da Informação. Estabelece os princípios gerais de governação da segurança que sustentam a presente política de privacidade. A P1 suporta a confidencialidade, integridade e disponibilidade dos dados pessoais em todos os sistemas e serviços.

10.2 P6 – Política de Gestão de Riscos. Define a metodologia de tratamento de riscos da organização, essencial para avaliar riscos de privacidade, processos de AIPD e avaliações de risco residual exigidas pelo RGPD e pela cláusula 6.1.3 da ISO/IEC 27001.

10.3 P13 – Política de Classificação e Rotulagem de Dados. Orienta a categorização de dados pessoais e sensíveis, constituindo a base para a aplicação de controlos de privacidade adequados, incluindo retenção, limitação de acesso e eliminação segura.

10.4 P14 – Política de Retenção e Eliminação de Dados. Suporta diretamente os requisitos de privacidade ao abrigo dos artigos 5(1)(e) e 17 do RGPD, assegurando que os dados pessoais são conservados apenas pelo tempo necessário e eliminados com segurança em conformidade com as obrigações legais.

10.5 P16 – Política de Mascaramento de Dados e Pseudonimização. Estabelece controlos para reduzir a identificabilidade dos dados pessoais através de medidas técnicas como tokenização, mascaramento dinâmico e pseudonimização, aplicando assim o artigo 32 do RGPD e o controlo 5.34 da ISO/IEC 27002.

10.6 P30 – Política de Resposta a Incidentes (P30). Define os protocolos obrigatórios de resposta a violações que se integram com o tratamento e os prazos de notificação de violações de privacidade exigidos pelos artigos 33 e 34 do RGPD.

10.7 P33 – Política de Monitorização de Auditoria e Conformidade. Aplica avaliações programadas da eficácia do programa de privacidade, da aplicação da política e do acompanhamento de ações corretivas nas unidades organizacionais e nos subcontratantes responsáveis pelo tratamento.

11. Normas e quadros de referência

11.1 ISO/IEC 27001

11.1.1 Cláusula 5.1 – Liderança e compromisso: estabelece a responsabilidade ao nível executivo pela proteção dos dados pessoais e pela aplicação dos princípios de privacidade.

11.1.2 Cláusula 6.1.3 – Tratamento de riscos de segurança da informação: suporta a identificação de riscos de privacidade, a avaliação e o tratamento através de AIPD e exceções.

11.1.3 Cláusula 8.1 – Planeamento e controlo operacional: exige salvaguardas técnicas e processuais para assegurar que os dados pessoais são tratados com segurança.

11.1.4 Cláusula 10.1 – Melhoria contínua: determina a avaliação e adaptação periódicas do programa de privacidade.

11.2 ISO/IEC 27002:2022 Controlos 5.34, 8.10, 8.11, 8.12: fornece orientação sobre o tratamento de informações pessoais identificáveis (PII), aplicação da retenção, eliminação, anonimização e transparência no exercício dos direitos dos titulares.

11.3 NIST SP 800-53 Rev.5

11.3.1 AR-1, AR-2, AR-4, AR-5: definem responsabilidades de governação, papéis, responsabilização e formação em privacidade.

11.3.2 PL-2, PL-8: exigem a integração de controlos de privacidade no ciclo de vida dos sistemas e na arquitetura empresarial.

11.3.3 AC-2, AC-6: aplicam o princípio do menor privilégio e a gestão de contas para proteção de dados pessoais.

11.3.4 AU-2, AU-6, AU-9: determinam registo, rastreabilidade e integridade de auditoria para acessos a dados pessoais.

11.3.5 IR-4, IR-5, IR-6: definem processos estruturados de deteção, análise e reporte de violações de privacidade.

11.3.6 PM-1, PM-21, PM-23: estabelecem um programa abrangente de privacidade, alinhado com objetivos estratégicos de risco e governação de dados.

11.4 RGPD da UE (2016/679)

11.4.1 Artigos 5, 6, 12–23, 25, 28, 30, 32–34: regulam o tratamento lícito, a limitação da finalidade, os direitos dos titulares dos dados, a responsabilização, a proteção de dados desde a conceção e por defeito, as obrigações de terceiros e a gestão de violações.

11.4.2 Considerando 78: reforça os princípios de privacidade desde a conceção.

11.5 Diretiva NIS2 da UE (2022/2555)

11.5.1 Artigo 21(2)(e) e (f): exige a implementação de controlos de segurança baseados no risco e a proteção de dados pessoais no âmbito das entidades essenciais e importantes.

11.6 DORA da UE (2022/2554)

11.6.1 Artigo 6(2)(d): impõe governação interna para o risco das TIC relacionado com o tratamento de dados.

11.6.2 Artigo 11(1)(c): determina a supervisão do risco de terceiros para serviços relacionados com dados.

11.6.3 Artigos 15(1) e 17: exigem tratamento seguro dos dados por prestadores de serviços e comunicações atempadas às autoridades de supervisão na sequência de incidentes relacionados com TIC.

11.7 COBIT 2019

11.7.1 APO12 – Gestão de riscos: integra o risco de privacidade na supervisão mais ampla do risco empresarial.

11.7.2 DSS01 – Operações geridas e DSS05 – Gerir Serviços de Segurança: asseguram operações seguras, incluindo controlo de acesso, retenção e integridade dos sistemas.

11.7.3 MEA03 – Monitorização da conformidade: exige revisão contínua do estado de conformidade face a obrigações regulamentares e de privacidade baseadas em políticas.