					Insira aqui a designação da entidade jurídica registada							
Número do documento: PII15					Título do documento: **Política de Gestão de Incidentes e Violações de PII**							
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

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	Comunicações do PIMS e evidência documentada de violações
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Controlo operacional, avaliação de riscos de privacidade e ligação ao tratamento de riscos
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Monitorização, avaliação, não conformidade, ação corretiva e melhoria
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Planeamento e preparação da gestão de incidentes para tratamento de PII
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Resposta a incidentes de segurança da informação que envolvam PII
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Requisitos legais, estatutários, regulamentares e contratuais, e proteção de registos
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Acordo com clientes do subcontratante e apoio às obrigações do cliente
GDPR	Article 5(2); Article 24	Controller	Supporting	Responsabilização e responsabilidade do responsável pelo tratamento
GDPR	Article 26	Joint Controller	Supporting	Coordenação da responsabilidade pela violação entre

				responsáveis conjuntos pelo tratamento
GDPR	Article 28	Both	Supporting	Assistência do subcontratante e obrigações contratuais do subcontratante
GDPR	Article 32	Both	Supporting	Segurança do tratamento e capacidade de deteção de violações
GDPR	Article 33	Both	Primary	Notificação de violação de dados pessoais e documentação da violação
GDPR	Article 34	Controller	Primary	Comunicação de violações de dados pessoais aos titulares dos dados afetados
GDPR	Article 39	Conditional	Supporting	Aconselhamento do DPO, monitorização, cooperação e apoio como ponto de contacto
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Princípios de segurança da informação e de conformidade em matéria de privacidade
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	Responsabilidades de resposta a incidentes de PII e reporte de eventos
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Planeamento, avaliação, resposta, lições aprendidas e recolha de evidência de incidentes

ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Ciclo de vida do processo de gestão de incidentes
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Política, plano, sensibilização, testes e lições aprendidas sobre incidentes
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12	Both	Supporting	Operações de deteção, notificação, triagem, análise, resposta e reporte
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Expectativas de notificação por subcontratantes cloud e de registo de violações
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Reporte de incidentes significativos quando aplicável
DORA Regulation (EU) 2022/2554	Article 17; Article 18; Article 19	Conditional	Supporting	Gestão, classificação e reporte de incidentes ICT quando aplicável

1. Âmbito

1.1 Esta política define os requisitos para identificar, reportar, triar, avaliar, conter, notificar, documentar, encerrar e melhorar a partir de incidentes de PII e violações de PII no âmbito do PIMS.

1.2 Esta política aplica-se a:

1.2.1 a organização atuando como responsável pelo tratamento de PII;

1.2.2 a organização atuando como responsável conjunto pelo tratamento quando seja necessária coordenação da responsabilidade pela violação;

1.2.3 a organização atuando como subcontratante de PII;

1.2.4 a organização atuando como subcontratante subsequente;

1.2.5 sistemas, aplicações, serviços, processos, fornecedores, subcontratantes, subcontratantes subsequentes e terceiros que tratem, armazenem, transmitam, apoiem, acedam ou afetem de outro modo PII no âmbito do PIMS.

1.3 Esta política utiliza REG10 - Registo de Incidentes e Violações de PII como o objeto de evidência principal para a gestão de incidentes e violações de PII.

1.4 Esta política utiliza objetos de evidência de apoio da seguinte forma:

1.4.1 REG01 para o âmbito do PIMS e o contexto aplicável de partes interessadas, requisitos legais, contratuais, setoriais e de reporte a clientes.

1.4.2 REG02 para atividades de tratamento afetadas, categorias de PII, categorias de titulares dos dados, finalidades e sistemas.

1.4.3 REG03 para a Declaração de Aplicabilidade e atualizações da aplicabilidade dos controlos.

1.4.4 REG04 para a ligação a riscos de privacidade, DPIA e risco residual.

1.4.5 REG08 para evidência da interface de incidentes com subcontratantes, subcontratantes subsequentes, clientes, fornecedores e terceiros.

1.4.6 REG09 para a ligação a transferências internacionais quando um incidente afeta tratamento transfronteiriço.

1.4.7 REG11 para evidência de formação, sensibilização e competência em resposta a incidentes.

1.4.8 REG12 para evidência de auditoria, não conformidade, ação corretiva e melhoria.

1.5 Esta política baseia-se nas políticas PIMS relacionadas para controlos especializados:

1.5.1 PII03 rege o inventário de tratamento e os registos de fundamento de licitude.

1.5.2 PII04 rege os controlos de aviso de privacidade e transparência fora das comunicações específicas de violação.

1.5.3 PII06 rege os pedidos de exercício de direitos dos titulares dos dados que surjam antes, durante ou depois de um incidente.

1.5.4 PII07 rege a metodologia de avaliação de riscos de privacidade e DPIA.

1.5.5 PII08 rege os controlos de privacidade desde a conceção e por defeito.

1.5.6 PII10 rege os controlos de retenção, apagamento e eliminação.

1.5.7 PII12 rege os controlos das relações de privacidade com subcontratantes, subcontratantes subsequentes, fornecedores e terceiros.

1.5.8 PII13 rege os mecanismos de transferência internacional de PII e os registos de risco de transferência.

1.5.9 PII14 rege os controlos preventivos e de deteção de segurança e acesso a PII.

1.5.10 PII16 rege a formação, sensibilização e competência em privacidade.

1.5.11 PII17 rege a informação documentada e a gestão de evidência.

1.5.12 PII18 rege a monitorização, auditoria interna, revisão pela gestão, não conformidade, ação corretiva e melhoria contínua.

1.6 Para efeitos desta política:

1.6.1 "Incidente de PII" significa um evento suspeito ou confirmado que afetou, possa ter afetado ou possa razoavelmente afetar a confidencialidade, integridade, disponibilidade, tratamento lícito ou manuseamento autorizado de PII.

1.6.2 "Violação de PII" significa um incidente de PII confirmado que envolva destruição, perda, alteração, divulgação, acesso, indisponibilidade ou comprometimento de PII de forma não autorizada, ilícita, acidental ou não pretendida.

1.6.3 "Avaliação da violação de dados pessoais" significa a avaliação documentada de saber se um incidente de PII é uma violação de PII, que PII e titulares dos dados são afetados, que riscos podem surgir, que notificações ou comunicações são necessárias e que ação de remediação é necessária.

1.6.4 "Tomada de conhecimento" significa o momento em que a organização tem um grau razoável de certeza de que ocorreu um incidente de segurança ou privacidade e de que PII foi ou pode ter sido comprometida.

1.6.5 "Incidente de PII de alto impacto" significa um incidente de PII que envolva tratamento de alto risco, categorias especiais ou PII altamente sensível, PII em larga escala, pessoas vulneráveis, clientes regulados, impacto multijurisdicional, impacto material em clientes, comprometimento de acessos privilegiados, exposição pública, ransomware, indisponibilidade de serviço ou impacto operacional ou reputacional significativo.

1.6.6 "Alteração material do incidente" significa informação nova ou alterada que afete o âmbito, severidade, categorias de PII, impacto nos titulares dos dados, decisão de notificação, impacto em clientes, causa raiz, contenção, recuperação, ação corretiva ou obrigações de reporte externo do incidente.

2. Finalidade

2.1 A finalidade desta política é assegurar que os incidentes e violações de PII são tratados de forma consistente, célere, lícita, segura e com evidência pronta para auditoria.

2.2 Esta política apoia a responsabilização ao exigir que os incidentes e violações de PII sejam registados em REG10 e ligados, quando aplicável, aos registos de tratamento afetados, riscos de privacidade, relações com subcontratantes e subcontratantes subsequentes, registos de transferência, ações corretivas e registos de formação.

2.3 Esta política assegura que as obrigações de responsável pelo tratamento, responsável conjunto pelo tratamento, subcontratante e subcontratante subsequente são tratadas através de regras de aplicabilidade distintas, mantendo simultaneamente um modelo integrado de evidência de incidentes e violações.

3. Objetivos

3.1 Os objetivos desta política são:

3.1.1 assegurar que incidentes de PII suspeitos são reportados e registados prontamente;

3.1.2 assegurar que incidentes de PII são triados e classificados com critérios consistentes;

3.1.3 assegurar que as avaliações da violação de dados pessoais consideram a PII afetada, os titulares dos dados, sistemas, atividades de tratamento, subcontratantes, subcontratantes subsequentes, transferências, riscos e ações de remediação;

3.1.4 assegurar que as decisões de notificação do responsável pelo tratamento e de comunicação aos titulares dos dados são documentadas;

3.1.5 assegurar que as notificações de violação por subcontratantes e subcontratantes subsequentes aos clientes ou partes a montante são feitas sem demora injustificada e de acordo com os acordos aplicáveis;

3.1.6 assegurar que a evidência é preservada e protegida durante o tratamento do incidente;

3.1.7 assegurar que a contenção, erradicação, recuperação e validação são acompanhadas através de REG10;

3.1.8 assegurar que desencadeadores de reporte regulamentares, contratuais, de clientes e setoriais são avaliados quando aplicável;

3.1.9 assegurar que as lições aprendidas dos incidentes resultam em ação corretiva e melhoria contínua;

3.1.10 assegurar que os registos de incidentes e violações estão disponíveis para auditoria, revisão pela gestão, garantia a clientes e revisão regulatória quando aplicável.

4. Declarações da política

4.1 Preparação e receção de incidentes

4.1.1 [Both] The Privacy Lead / PIMS Manager MUST manter critérios de tratamento de incidentes e violações de PII em REG10 pelo menos anualmente e após qualquer alteração material ao âmbito do PIMS, contexto legal, obrigações contratuais ou tratamento de alto risco.

4.1.2 [All] The Incident Response Coordinator MUST registar cada incidente de PII suspeito reportado ou detetado em REG10 no prazo de um dia útil após a receção, ou mais cedo quando possa ser acionado um prazo de notificação aplicável ou de reporte a clientes.

4.1.3 [Both] The System Owner / Application Owner MUST preservar logs de sistema relevantes, alertas, registos de acesso, evidência de configuração e evidência de recuperação ligados a REG10 quando um incidente suspeito afete um sistema ou aplicação que trate PII.

4.1.4 [Both] The Information Security Lead MUST concluir a triagem técnica inicial de qualquer evento de segurança que envolva PII no prazo de 24 horas após a deteção e registar a severidade inicial, os ativos afetados e o estado da contenção em REG10.

4.2 Classificação e avaliação da violação de dados pessoais

4.2.1 [Both] The Incident Response Coordinator MUST classificar cada entrada de REG10 como evento não relacionado com PII, incidente de PII suspeito, incidente de PII confirmado ou violação de PII confirmada no prazo de 24 horas após a receção, ou atualizar o registo REG10 com a razão pela qual a classificação continua pendente.

4.2.2 [Both] The Privacy Lead / PIMS Manager MUST identificar a atividade de tratamento afetada, as categorias de PII, categorias de titulares dos dados, sistemas, subcontratantes, subcontratantes subsequentes, locais de transferência e riscos de privacidade em REG02, REG04, REG08, REG09 e REG10 antes de a decisão de notificação da violação ser finalizada.

4.2.3 [Controller] The Data Protection Officer / Privacy Advisor MUST avaliar o risco para os titulares dos dados afetados em cada violação de PII confirmada ou razoavelmente suspeita e registar em REG10 a recomendação de notificação, a fundamentação de risco e o aconselhamento antes de ser tomada a decisão de notificação externa.

4.2.4 [Processor] The Privacy Lead / PIMS Manager MUST identificar o responsável pelo tratamento ou cliente afetado e os requisitos contratuais de notificação aplicáveis logo que a organização tome conhecimento de uma violação de PII que afete PII de clientes, e MUST registar o resultado em REG08 e REG10.

4.2.5 [Joint Controller] The Privacy Lead / PIMS Manager MUST verificar a responsabilidade acordada pela violação, a responsabilidade principal pela comunicação e o mecanismo de coordenação antes de qualquer notificação ou comunicação externa por um responsável conjunto pelo tratamento, e MUST registar a decisão em REG08 e REG10.

4.2.6 [Conditional] The Privacy Lead / PIMS Manager MUST avaliar os desencadeadores aplicáveis de reporte legal, setorial, do setor financeiro, de cibersegurança, contratual, de clientes e de destinatários de serviços para cada incidente de PII de alto impacto e registar o resultado da aplicabilidade em REG01, REG08 e REG10.

[... 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 [Both] The Privacy Lead / PIMS Manager MUST registar qualquer exceção a esta política em REG12 antes da implementação, ou no prazo de 24 horas após uma ação de emergência quando a aprovação prévia não tenha sido viável.

9.1.2 [Both] Top Management MUST aprovar qualquer exceção que afete materialmente o prazo de notificação da violação, comunicação pública, compromisso com clientes, preservação de evidência ou risco para titulares dos dados antes de o incidente ser encerrado, com a evidência de aprovação conservada em REG10 e REG12.

9.1.3 [Conditional] The Data Protection Officer / Privacy Advisor MUST documentar aconselhamento para qualquer notificação atrasada, decisão de não notificação ou abordagem excecional de comunicação antes do encerramento do incidente, com o aconselhamento conservado em REG10.

9.1.4 [Both] The Vendor / Procurement Owner MUST registar em REG08 e REG12, no prazo de cinco dias úteis após identificar a exceção, exceções motivadas por fornecedores, subcontratantes, subcontratantes subsequentes ou clientes que afetem a resposta a incidentes.

10. Aplicação

10.1.1 [All] The Process Owner / Business Owner MUST escalar para Privacy Lead / PIMS Manager, no prazo de dois dias úteis após a descoberta, a falha em reportar um incidente de PII suspeito, preservar evidência, seguir ações atribuídas ou cooperar com a avaliação da violação de dados pessoais, com a evidência conservada em REG12.

10.1.2 [Both] The Privacy Lead / PIMS Manager MUST registar uma não conformidade REG12 quando uma violação desta política afetar a receção de incidentes, triagem, contenção, notificação, integridade da evidência, comunicação ou ação corretiva.

10.1.3 [Both] The Vendor / Procurement Owner MUST iniciar a remediação de fornecedor ou subcontratante através de REG08 e REG12 no prazo de cinco dias úteis quando um subcontratante, subcontratante subsequente, fornecedor ou outro terceiro não cumprir as obrigações de incidentes ou violações acordadas.

10.1.4 [Both] Top Management MUST rever não conformidades materiais ou recorrentes de gestão de incidentes na próxima revisão pela gestão programada, com as decisões e ações exigidas conservadas em REG12.

11. Revisão e manutenção

11.1.1 [Both] The Privacy Lead / PIMS Manager MUST rever esta política pelo menos anualmente e registar o resultado da revisão, alterações necessárias e estado de aprovação em REG12.

11.1.2 [Both] The Incident Response Coordinator MUST acionar uma revisão pós-incidente desta política no prazo de 30 dias de calendário após o encerramento de qualquer incidente de PII

de alto impacto ou violação de PII confirmada, com a evidência de revisão conservada em REG10 e REG12.

11.1.3 [Conditional] The Privacy Lead / PIMS Manager MUST rever esta política no prazo de 30 dias de calendário após tomar conhecimento de uma alteração material aos requisitos aplicáveis de reporte de incidentes legais, setoriais, de clientes, contratuais, de subcontratantes, de subcontratantes subsequentes ou relacionados com transferências, com a evidência de revisão conservada em REG01, REG08, REG09 e REG12.

11.1.4 [Both] The Internal Audit / Compliance Reviewer MUST rever a implementação desta política pelo menos anualmente através do programa de auditoria interna do PIMS, com as constatações de auditoria e ações corretivas conservadas em REG12.

11.1.5 [Both] Top Management MUST rever tendências de incidentes, violações significativas, desempenho de notificação, ações corretivas em atraso e eficácia da política durante a revisão pela gestão programada, com os resultados conservados em REG12.

12. Políticas relacionadas

12.1 Esta política deve ser lida em conjunto com:

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 Aviso de Privacidade e Transparência

12.6 PII06 - Política de Gestão de Direitos dos Titulares dos Dados

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 PII10 - Política de Retenção, Apagamento e Eliminação de PII

12.10 PII12 - Política de Gestão da Privacidade de Subcontratantes, Subcontratantes Subsequentes e Terceiros

12.11 PII13 - Política de Transferência Internacional de PII

12.12 PII14 - Política de Segurança e Controlo de Acesso a PII

12.13 PII16 - Política de Formação, Sensibilização e Competência em Privacidade

12.14 PII17 - Política de Informação Documentada e Gestão de Evidência do PIMS

12.15 PII18 - Política de Monitorização, Auditoria e Melhoria do PIMS

13. Normas e referenciais de referência

13.1 ISO/IEC 27701:2025 - Clause 7.4; Clause 7.5. Addressed by clauses [4.4.7; 4.5.1; 4.5.3; 4.5.4; 5.2.2; 6.2.2; 7.1.1; 7.1.7; 11.1.3].

13.2 ISO/IEC 27701:2025 - Clause 8.1; Clause 8.2; Clause 8.3. Addressed by clauses [4.2.2; 4.3.4; 4.6.3; 6.3.1; 7.1.4; 11.1.2].

13.3 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.6.1; 4.6.2; 4.6.3; 4.6.4; 6.4.1; 6.5.1; 8.1.1; 8.1.4; 10.1.2; 11.1.4; 11.1.5].

13.4 ISO/IEC 27701:2025 - Annex A.3.11. Addressed by clauses [4.1.1; 4.1.2; 4.2.6; 4.4.1; 5.1.1; 5.4.1; 7.1.1; 7.1.2; 7.1.6].

13.5 ISO/IEC 27701:2025 - Annex A.3.12. Addressed by clauses [4.1.3; 4.1.4; 4.2.1; 4.2.3; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.4.1; 4.4.3; 4.4.4; 4.5.1; 4.5.4; 6.3.1].

13.6 ISO/IEC 27701:2025 - Annex A.3.13; Annex A.3.14. Addressed by clauses [4.2.6; 4.4.6; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.6.4; 6.2.2; 9.1.2; 11.1.3].

13.7 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.6. Addressed by clauses [4.2.4; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5; 10.1.3].

13.8 GDPR - Article 5(2); Article 24. Addressed by clauses [4.1.2; 4.2.2; 4.4.1; 4.5.1; 4.5.3; 4.5.4; 4.6.2; 5.2.1; 6.3.1; 8.1.3; 11.1.5].

13.9 GDPR - Article 26. Addressed by clauses [4.2.5; 4.4.1; 4.4.3; 5.3.1; 6.2.2; 11.1.3].

13.10 GDPR - Article 28. Addressed by clauses [4.2.4; 4.3.5; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5; 10.1.3].

13.11 GDPR - Article 32. Addressed by clauses [4.1.3; 4.1.4; 4.3.2; 4.3.3; 4.5.2; 4.6.3; 5.5.1; 7.1.4; 8.1.2; 11.1.2].

13.12 GDPR - Article 33. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.5.1; 4.5.4; 8.1.3; 9.1.3].

13.13 GDPR - Article 34. Addressed by clauses [4.2.3; 4.2.5; 4.4.2; 4.4.3; 4.4.7; 4.5.4; 8.1.3; 9.1.3].

13.14 GDPR - Article 39. Addressed by clauses [4.2.3; 4.4.2; 5.3.1; 6.2.2; 9.1.3; 11.1.3].

13.15 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.2.2; 4.3.2; 4.3.3; 4.5.3; 4.6.2; 4.6.3; 5.2.2; 6.4.1; 8.1.4; 11.1.4].

13.16 ISO/IEC 29151:2022 - Clause 16.1.2; Clause 16.1.3. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.2.3; 4.4.1; 4.4.3; 4.6.5; 7.1.3; 7.1.6].

13.17 ISO/IEC 27002:2022 - Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.5.1; 4.5.2; 4.6.1; 4.6.2; 7.1.2; 7.1.6].

13.18 ISO/IEC 27035-1:2023 - Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.4.7; 4.5.2; 4.6.1; 5.4.1; 7.1.6; 11.1.2].

13.19 ISO/IEC 27035-2:2023 - Clause 4; Clause 6; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.1; 4.6.1; 4.6.5; 5.1.1; 7.1.1; 7.1.3; 7.1.6; 8.1.6; 11.1.1; 11.1.2].

13.20 ISO/IEC 27035-3:2020 - Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.4.1; 4.4.4; 4.5.1; 5.4.2; 6.1.2; 8.1.2].

13.21 ISO/IEC 27018:2020 - Annex A.10.1. Addressed by clauses [4.2.4; 4.3.5; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5].

13.22 NIS2 Directive (EU) 2022/2555 - Article 23. Addressed by clauses [4.2.6; 4.4.6; 4.4.7; 5.3.1; 6.2.2; 8.1.3; 11.1.3].

13.23 DORA Regulation (EU) 2022/2554 - Article 17; Article 18; Article 19. Addressed by clauses [4.2.1; 4.2.6; 4.4.6; 4.4.7; 5.1.2; 6.2.1; 8.1.3; 11.1.3; 11.1.5].