POLÍTICA INSTITUCIONAL

Política de Privacidade

CÓDIGO DOCUMENTAL	POL/DTI/003
VERSÃO	01 - Versão inicial
DATA DE APROVAÇÃO	30 / 10 / 2026
ÓRGÃO DE APROVAÇÃO	Comissão Executiva
ÁREA RESPONSÁVEL	Direcção de Tecnologia e Inovação

CLASSIFICAÇÃO: **PÚBLICO**

Controlo Documental

Quadro A — Identificação do documento

Designação	Política de Privacidade e Protecção de Dados Pessoais
Código documental	POL/DTI/003
Versão	01 - Versão inicial
Data de aprovação	30 / 10 / 2026
Órgão de aprovação	Comissão Executiva
Periodicidade de revisão	Anualmente ou sempre que ocorram alterações relevantes.
Classificação	Público

Quadro B — Histórico de aprovação e revisões

Documento	Versão	Descrição das alterações	Data de aprovação
Política de Privacidade e Protecção de Dados Pessoais	01	Versão inicial	30 / 10 / 2026

Índice

Capítulo I — Disposições Gerais 4
Artigo 1.º | *Introdução e objectivo* 4
Artigo 2.º | *Âmbito de aplicação* 4
Artigo 3.º | *Identificação da entidade responsável* 5
Capítulo II — Princípios e Categorias de Dados Pessoais 5
Artigo 4.º | *Princípios de protecção de dados* 5
Artigo 5.º | *Categorias de dados pessoais e dados sensíveis* 6
Capítulo III — Responsabilidades 8
Artigo 6.º | *Responsabilidades internas* 8
Capítulo IV — Finalidades, Licitude e Recolha dos Dados 10
Artigo 7.º | *Finalidades e fundamentos de licitude do tratamento* 10
Artigo 8.º | *Recolha dos dados pessoais* 12
Capítulo V — Partilha, Subcontratação e Conservação dos Dados 12
Artigo 9.º | *Partilha de dados e relação com empresas clientes, seguradoras e TPA* 12
Artigo 10.º | *Subcontratação e transferência internacional de dados* 13
Artigo 11.º | *Prazos de conservação dos dados* 14
Capítulo VI — Direitos dos Titulares e Segurança dos Dados 15
Artigo 12.º | *Direitos dos titulares e procedimento para o seu exercício* 15
Artigo 13.º | *Segurança, confidencialidade e violações de dados pessoais* 16
Capítulo VII — Menores, Privacidade desde a Concepção, Comunicações e Contactos 18
Artigo 14.º | *Dados de menores e privacidade desde a concepção e por defeito* 18
Artigo 15.º | *Comunicações electrónicas, marketing e cookies* 18
Artigo 16.º | *Contactos e reclamações* 19
Capítulo VIII — Disposições Finais 20
Artigo 17.º | *Alterações e disposições finais* 20
Anexo I — Matriz de Síntese de Responsabilidades 20

Capítulo I — Disposições Gerais

Artigo 1.º | *Introdução e objectivo*

1. O FIS reconhece a importância da privacidade e da protecção dos dados pessoais como elementos fundamentais para a confiança dos seus clientes, parceiros, beneficiários e demais utilizadores dos seus serviços.
2. No desenvolvimento da sua actividade, o FIS disponibiliza uma solução de gestão de coparticipações de saúde que permite estabelecer uma ligação operacional entre empresas, entidades gestoras de planos de saúde (TPA) e demais intervenientes, através de informação organizada e de processos de tratamento e consolidação de transacções.
3. A execução desta actividade pode implicar o tratamento de dados pessoais de representantes de empresas, colaboradores, beneficiários, dependentes, representantes de parceiros, prestadores de serviços e utilizadores das plataformas e dos canais digitais do FIS.
4. O FIS compromete-se a tratar esses dados de forma lícita, transparente, segura e proporcional, respeitando os direitos dos respectivos titulares e adoptando medidas técnicas e organizativas adequadas à natureza e aos riscos do tratamento.
5. A presente Política de Privacidade e Protecção de Dados Pessoais estabelece os princípios, as finalidades, as categorias de informação e as condições de utilização, partilha, conservação e protecção dos dados pessoais tratados pelo FIS.
6. A presente Política tem como objectivo informar os titulares dos dados sobre a forma como o FIS recolhe, utiliza, conserva, partilha e protege os seus dados pessoais, estabelecendo as regras fundamentais que orientam o respectivo tratamento, pretendendo-se, em particular:
    a. Assegurar o tratamento lícito, leal e transparente dos dados pessoais;
    b. Informar os titulares sobre as finalidades e os fundamentos do tratamento;
    c. Identificar as categorias de dados pessoais que podem ser recolhidas e utilizadas;
    d. Estabelecer os princípios de minimização e limitação do tratamento;
    e. Definir as condições de comunicação de dados a terceiros;
    f. Assegurar a confidencialidade, a integridade e a disponibilidade da informação;
    g. Estabelecer regras para a conservação e a eliminação dos dados;
    h. Salvaguardar os direitos dos titulares dos dados;
    i. Prevenir acessos, utilizações, alterações ou divulgações não autorizados;
    j. Promover uma cultura institucional de privacidade e protecção de dados pessoais.

Artigo 2.º | *Âmbito de aplicação*

1. A presente Política aplica-se ao tratamento de dados pessoais realizado pelo FIS através de meios digitais, electrónicos, físicos ou quaisquer outros meios utilizados no desenvolvimento da sua actividade, abrangendo:
    a. Os visitantes do website institucional do FIS;
    b. Os utilizadores das plataformas e soluções tecnológicas disponibilizadas pelo FIS;

c. Os representantes e colaboradores das empresas clientes;

d. Os beneficiários e dependentes abrangidos pelos modelos de gestão de coparticipações;

e. Os representantes, colaboradores e contactos das seguradoras e TPA;

f. Os representantes e colaboradores dos prestadores de serviços de saúde;

g. Os fornecedores e prestadores de serviços do FIS;

h. Os candidatos a oportunidades profissionais;

i. Os colaboradores, gestores e demais pessoas que mantenham relações profissionais com o FIS;

j. As pessoas que contactem o FIS através dos seus canais institucionais, comerciais ou de suporte.

2. A presente Política aplica-se igualmente aos colaboradores e prestadores de serviços que, no exercício das respectivas funções, tenham acesso a dados pessoais tratados pelo FIS.

Artigo 3.º | *Identificação da entidade responsável*

1. A entidade responsável pelo tratamento dos dados pessoais abrangidos pela presente Política é o FIS, com os seguintes contactos:

   a. Website: https://www.fis-africa.com

   b. Contacto institucional: comercial@fis-africa.com

   c. Contacto de suporte: suporte@fis-africa.com.

2. Para efeitos de pedidos relacionados com privacidade e protecção de dados, os titulares podem utilizar o contacto institucional referido na alínea b) do número anterior, identificando no assunto «Privacidade e Protecção de Dados».

3. A qualificação do FIS como responsável pelo tratamento ou como entidade que trata dados por conta de terceiros é determinada em função das finalidades e dos meios efectivamente definidos em cada relação contratual.

4. Sempre que o FIS actue como subcontratado de uma empresa cliente, seguradora ou outra entidade, o tratamento deve observar as instruções legítimas e documentadas do respectivo responsável pelo tratamento, bem como as obrigações contratuais e legais aplicáveis.

Capítulo II — Princípios e Categorias de Dados Pessoais

Artigo 4.º | *Princípios de protecção de dados*

1. O FIS orienta o tratamento de dados pessoais pelos seguintes princípios:

   a. **Licitude e lealdade:** os dados pessoais são tratados de forma lícita e leal, respeitando os direitos e interesses legítimos dos respectivos titulares;

   b. **Transparência:** os titulares devem ser informados sobre a recolha e a utilização dos seus dados, incluindo as finalidades, os destinatários e os direitos que lhes assistem;

c. **Limitação das finalidades:** os dados são recolhidos para finalidades determinadas, explícitas e legítimas, não devendo ser utilizados para finalidades incompatíveis com aquelas que justificaram a sua recolha;

d. **Minimização dos dados:** o FIS recolhe e trata apenas os dados adequados, pertinentes e estritamente necessários à finalidade pretendida;

e. **Exactidão:** a informação tratada deve ser exacta e actualizada, devendo ser adoptadas medidas para corrigir os dados incompletos ou desactualizados;

f. **Limitação da conservação:** os dados são conservados apenas durante o período necessário às finalidades do tratamento, sem prejuízo dos prazos legais e contratuais aplicáveis;

g. **Integridade e confidencialidade:** os dados são protegidos contra acessos, utilizações, alterações, perdas, destruições ou divulgações não autorizados;

h. **Responsabilização:** o FIS deve demonstrar a adopção de medidas adequadas para assegurar o cumprimento das regras e dos princípios de protecção de dados.

Artigo 5.º | *Categorias de dados pessoais e dados sensíveis*

1. A natureza dos dados recolhidos depende da relação estabelecida com o titular e do serviço utilizado, podendo o FIS tratar as categorias de dados previstas nos números seguintes.
2. **Dados de identificação:**
    a. O nome completo;
    b. O número de identificação, quando necessário;
    c. A data de nascimento, quando necessária à identificação;
    d. O identificador de beneficiário;
    e. O identificador de utilizador;
    f. A informação de identificação de representantes de entidades.
3. **Dados de contacto:**
    a. O endereço de correio electrónico;
    b. O número de telefone;
    c. A morada, quando necessária;
    d. Os contactos profissionais;
    e. Outros elementos de comunicação disponibilizados pelo titular.
4. **Dados profissionais e institucionais:**
    a. A entidade empregadora;
    b. O cargo ou a função;
    c. A identificação da empresa cliente;
    d. A identificação da seguradora ou da TPA;
    e. A identificação do prestador de serviços;

f. Os dados de representação e de contacto institucional.

5. **Dados operacionais e transaccionais**, no âmbito da gestão de coparticipações:
    a. A referência da transacção;
    b. A identificação do beneficiário;
    c. A identificação da empresa cliente;
    d. A identificação da seguradora e da TPA;
    e. A identificação do prestador de serviços de saúde;
    f. O valor da coparticipação;
    g. A data da operação;
    h. O estado da transacção;
    i. A informação necessária à validação, reconciliação, facturação e liquidação.
6. **Dados financeiros**, quando necessários à execução das operações e das relações contratuais:
    a. Os valores de coparticipações financiadas;
    b. Os valores facturados;
    c. Os valores pagos;
    d. Os valores pendentes ou em cobrança;
    e. As referências de liquidação;
    f. A informação de facturação e cobrança;
    g. Os dados bancários de representantes ou entidades, quando legalmente admissíveis e estritamente necessários.
7. **Dados técnicos e de utilização**, recolhidos no acesso ao website e às plataformas do FIS:
    a. O endereço IP;
    b. A data e a hora de acesso;
    c. O tipo de dispositivo;
    d. O sistema operativo e o navegador;
    e. Os registos de autenticação;
    f. Os registos de actividade e utilização;
    g. Os dados técnicos necessários à segurança e à manutenção dos sistemas.
8. **Dados de comunicação:** a informação incluída em pedidos de contacto, reclamações, solicitações de suporte, comunicações comerciais e demais interacções com os titulares.
9. **Dados pessoais sensíveis e informação de saúde:** o FIS reconhece que os dados relativos à saúde são classificados como dados pessoais sensíveis, estando sujeitos a requisitos especiais de tratamento e protecção.
10. Considerando a natureza da sua actividade, o FIS adopta o princípio de que a gestão financeira e operacional das coparticipações não exige, em regra, o acesso a diagnósticos, relatórios

médicos, exames, prescrições, históricos clínicos ou outros elementos relativos ao estado de saúde dos beneficiários, devendo privilegiar o tratamento dos seguintes elementos:

a. A identificação do beneficiário;
b. A identificação da entidade responsável;
c. A referência da operação;
d. A identificação do prestador;
e. O valor da coparticipação;
f. A data da transacção;
g. O estado da operação.

11. O FIS não deve recolher, armazenar, consultar ou partilhar informação clínica quando esta não seja necessária à finalidade legítima do tratamento.
12. Caso, excepcionalmente, se revele necessário tratar dados pessoais sensíveis, a operação deve ser previamente avaliada pela Direcção de Risco e Compliance, devendo ser assegurados os requisitos legais aplicáveis, incluindo a existência de fundamento jurídico adequado, as autorizações eventualmente exigíveis e medidas reforçadas de segurança.
13. O acesso a dados de saúde, quando legalmente admissível, deve ser limitado aos profissionais e entidades cuja intervenção seja estritamente necessária e devidamente autorizada.

Capítulo III — Responsabilidades

Artigo 6.º | *Responsabilidades internas*

1. Compete à Comissão Executiva:
    a. Aprovar a presente Política e as suas alterações;
    b. Assegurar os recursos necessários à sua implementação;
    c. Aprovar as medidas estratégicas de protecção de dados;
    d. Acompanhar os riscos relevantes de privacidade e segurança;
    e. Deliberar sobre as situações que exijam decisão superior.
2. Compete à Direcção de Risco e Compliance:
    a. Coordenar a implementação da presente Política;
    b. Acompanhar o cumprimento das obrigações legais de protecção de dados;
    c. Avaliar os riscos associados ao tratamento de dados pessoais;
    d. Coordenar o tratamento dos pedidos dos titulares;
    e. Acompanhar as comunicações e partilhas de dados;
    f. Avaliar a necessidade de notificações ou autorizações junto da Agência de Protecção de Dados;
    g. Coordenar a avaliação de violações de dados pessoais;

h. Promover a sensibilização dos colaboradores;

i. Acompanhar a elaboração e a actualização dos instrumentos internos de protecção de dados;

j. Reportar à Comissão Executiva as situações relevantes.

3. Compete à Direcção de Tecnologia e Inovação:

a. Implementar os controlos técnicos de segurança;

b. Assegurar a gestão de acessos e permissões;

c. Proteger os sistemas e as bases de dados;

d. Implementar mecanismos de registo e rastreabilidade;

e. Assegurar a segurança das integrações e das transmissões de informação;

f. Apoiar a gestão de incidentes de segurança;

g. Implementar medidas de recuperação e continuidade;

h. Apoiar a eliminação ou anonimização técnica dos dados, quando autorizada.

4. Compete à Direcção de Contabilidade e Finanças:

a. Assegurar a confidencialidade dos dados financeiros e contabilísticos;

b. Limitar o acesso à informação financeira aos intervenientes autorizados;

c. Garantir a utilização dos dados exclusivamente para finalidades legítimas;

d. Cumprir os requisitos de conservação documental;

e. Apoiar a identificação e a correcção de dados financeiros inexactos;

f. Comunicar os incidentes ou as situações de acesso indevido à informação sob a sua responsabilidade.

5. Compete à Direcção Comercial:

a. Assegurar a recolha adequada de dados no âmbito das relações comerciais;

b. Informar os clientes e parceiros sobre as práticas de tratamento aplicáveis;

c. Garantir que os dados recebidos de empresas clientes e parceiros possuem origem e fundamento legítimos;

d. Evitar a divulgação não autorizada de dados pessoais;

e. Assegurar que as comunicações comerciais respeitam as preferências e os direitos dos titulares;

f. Encaminhar para a área competente os pedidos de titulares e as reclamações relacionados com privacidade.

6. Compete ao Gabinete de Auditoria Interna:

a. Avaliar, de forma independente, a adequação dos controlos de protecção de dados;

b. Verificar o cumprimento da Política e dos procedimentos associados;

c. Avaliar a eficácia dos mecanismos de acesso, conservação e segurança;

d. Identificar deficiências e formular recomendações;

e. Acompanhar, no âmbito das suas competências, a implementação das recomendações emitidas.

7. O Gabinete de Auditoria Interna não deve assumir a execução dos controlos operacionais nem a gestão corrente dos dados pessoais que posteriormente possa auditar.
8. Todos os colaboradores e prestadores de serviços que tenham acesso a dados pessoais devem:
    a. Cumprir a presente Política e os procedimentos aplicáveis;
    b. Utilizar os dados exclusivamente para as finalidades autorizadas;
    c. Respeitar os deveres de confidencialidade;
    d. Proteger as credenciais e os equipamentos utilizados;
    e. Não partilhar informação com pessoas não autorizadas;
    f. Comunicar imediatamente os incidentes ou as suspeitas de violação;
    g. Participar nas acções de sensibilização e formação aplicáveis.
9. A síntese das responsabilidades previstas na presente Política consta do Anexo I.

Capítulo IV — Finalidades, Licitude e Recolha dos Dados

Artigo 7.º | *Finalidades e fundamentos de licitude do tratamento*

1. O FIS trata dados pessoais para as finalidades previstas nos números seguintes.
2. **Gestão de coparticipações:**
    a. Identificar os beneficiários abrangidos pelo modelo operacional;
    b. Registar e validar as transacções;
    c. Confirmar os valores de coparticipação;
    d. Prevenir duplicações e inconsistências;
    e. Consolidar as operações por período;
    f. Assegurar a reconciliação dos valores;
    g. Apoiar os processos de facturação, liquidação e recuperação.
3. **Gestão das relações contratuais:**
    a. Formalizar e executar contratos;
    b. Gerir as relações com empresas clientes e parceiros;
    c. Cumprir obrigações comerciais e operacionais;
    d. Acompanhar os níveis de serviço;
    e. Prestar informações relativas às operações realizadas.
4. **Segurança e funcionamento das plataformas:**
    a. Assegurar a autenticação e a gestão de acessos;

   b. Prevenir acessos não autorizados;
   c. Detectar actividades suspeitas;
   d. Monitorizar falhas e incidentes tecnológicos;
   e. Assegurar a disponibilidade e a integridade dos sistemas.

5. **Atendimento e suporte:**
   a. Responder a pedidos de informação;
   b. Tratar reclamações e solicitações;
   c. Prestar suporte técnico;
   d. Acompanhar ocorrências e pedidos de esclarecimento.
6. **Cumprimento de obrigações legais e contratuais:**
   a. Cumprir obrigações contabilísticas, fiscais e comerciais;
   b. Responder a solicitações legítimas de autoridades competentes;
   c. Assegurar a conservação de evidências;
   d. Prevenir e investigar irregularidades, nos limites legalmente permitidos.
7. **Comunicação institucional e comercial:**
   a. Enviar comunicações institucionais;
   b. Divulgar informações sobre os serviços do FIS;
   c. Apresentar novas funcionalidades e soluções;
   d. Desenvolver iniciativas de relacionamento comercial.
8. As comunicações de natureza promocional dirigidas a pessoas singulares devem observar os requisitos legais aplicáveis, incluindo a obtenção de consentimento quando exigível e a possibilidade de oposição ou de cancelamento da subscrição.
9. **Fundamentos de licitude:** o FIS assegura que cada actividade de tratamento dispõe de fundamento jurídico adequado, em função da finalidade, da categoria dos dados e da relação estabelecida com o titular, podendo o tratamento fundamentar-se, conforme aplicável, em:
   a. Consentimento inequívoco, expresso e informado do titular, quando legalmente exigido;
   b. Necessidade de execução de contrato em que o titular seja parte ou de diligências pré-contratuais a seu pedido;
   c. Cumprimento de obrigação legal;
   d. Protecção de interesses vitais, nos casos legalmente admissíveis;
   e. Outros fundamentos expressamente previstos na legislação aplicável.
10. O consentimento, quando utilizado como fundamento, deve ser livre, específico, informado e demonstrável, podendo o titular retirá-lo nos termos legalmente aplicáveis.
11. A retirada do consentimento não prejudica a licitude do tratamento efectuado antes da sua retirada, nem elimina a possibilidade de conservação de dados quando exista outro fundamento legal válido.

12. O tratamento de dados sensíveis deve observar os requisitos especiais previstos na legislação angolana, não sendo suficiente a existência de uma autorização genérica ou de uma cláusula contratual sem fundamento legal adequado.

Artigo 8.º | *Recolha dos dados pessoais*

1. Os dados pessoais podem ser recolhidos directamente junto dos titulares ou através das entidades que participam no modelo operacional do FIS, podendo as fontes de recolha incluir:
    a. O website institucional;
    b. As plataformas e aplicações digitais;
    c. Os formulários electrónicos ou físicos;
    d. As empresas clientes;
    e. As seguradoras;
    f. As TPA;
    g. Os prestadores de serviços de saúde;
    h. Os fornecedores e parceiros;
    i. As comunicações efectuadas pelos titulares;
    j. Outros meios legítimos de recolha.
2. Quando os dados não sejam recolhidos directamente junto do titular, o FIS deve assegurar que a disponibilização da informação e a comunicação ao titular respeitam os requisitos legais aplicáveis.
3. As entidades que forneçam dados ao FIS devem assegurar que possuem legitimidade para o efeito e que a comunicação respeita as condições legais e contratuais aplicáveis.
4. O FIS não deve aceitar ou utilizar dados cuja origem ou legitimidade de disponibilização não possa ser adequadamente justificada.

Capítulo V — Partilha, Subcontratação e Conservação dos Dados

Artigo 9.º | *Partilha de dados e relação com empresas clientes, seguradoras e TPA*

1. O FIS pode comunicar dados pessoais a terceiros sempre que exista fundamento jurídico adequado e a comunicação seja necessária para uma finalidade legítima, podendo as categorias de destinatários incluir:
    a. **Empresas clientes**, para efeitos de identificação dos beneficiários abrangidos, acompanhamento das coparticipações, consolidação dos valores e execução das obrigações contratuais;
    b. **Seguradoras**, quando necessário à articulação operacional, à validação das informações disponibilizadas e à execução das responsabilidades contratuais e institucionais;
    c. **TPA**, para efeitos de gestão, validação, consolidação e reconciliação das transacções de coparticipação;

d. **Prestadores de serviços de saúde**, quando necessário à identificação e à confirmação das operações abrangidas pelo modelo operacional;

e. **Prestadores de serviços tecnológicos**, para alojamento, manutenção, suporte, segurança, comunicação e funcionamento das plataformas, nos limites das obrigações contratuais e legais aplicáveis;

f. **Prestadores de serviços profissionais**, como auditores, consultores jurídicos, contabilistas e outros prestadores, sempre que a sua intervenção seja necessária e legítima;

g. **Autoridades públicas e entidades reguladoras**, quando exista obrigação legal, ordem ou solicitação legítima emitida por autoridade competente.

2. A comunicação de dados deve respeitar o princípio da necessidade de conhecer, limitando-se aos elementos estritamente necessários à finalidade da partilha.
3. O FIS não comercializa nem disponibiliza indiscriminadamente os dados pessoais dos seus titulares.
4. A existência de uma relação contratual entre o FIS e uma entidade terceira não constitui, por si só, autorização para a partilha irrestrita de dados pessoais.
5. **Relação com empresas clientes, seguradoras e TPA:** o FIS reconhece que estas entidades podem assumir responsabilidades próprias no tratamento de dados pessoais, em função das respectivas atribuições e finalidades, devendo a partilha de dados entre elas respeitar as seguintes regras:
    a. Cada entidade deve actuar dentro das suas competências e responsabilidades;
    b. A informação partilhada deve limitar-se ao necessário à execução do modelo operacional;
    c. A entidade que disponibiliza os dados deve possuir legitimidade para o efeito;
    d. Devem existir regras contratuais que definam as responsabilidades de cada interveniente;
    e. Devem ser estabelecidos mecanismos seguros de transmissão e recepção de informação;
    f. Os dados não devem ser reutilizados para finalidades incompatíveis com aquelas que justificaram a sua comunicação;
    g. As ocorrências de segurança ou as violações de dados devem ser comunicadas e tratadas nos termos contratualmente definidos e legalmente aplicáveis.
6. Sempre que o FIS trate dados por conta de outra entidade, deve existir instrumento contratual adequado que estabeleça, entre outros aspectos, o objecto, a duração, a finalidade, as categorias de dados, as obrigações de segurança, a confidencialidade e as condições de subcontratação.

Artigo 10.º | *Subcontratação e transferência internacional de dados*

1. O FIS pode recorrer a prestadores de serviços externos para assegurar o funcionamento das suas actividades, incluindo serviços de alojamento, armazenamento, manutenção tecnológica, suporte, comunicação e processamento de informação.

2. Sempre que esses prestadores tenham acesso a dados pessoais, o FIS deve assegurar:
    a. A avaliação prévia da adequação do prestador;
    b. A formalização das obrigações de confidencialidade;
    c. A definição das finalidades e das instruções de tratamento;
    d. A limitação do acesso aos dados necessários;
    e. A adopção de medidas de segurança adequadas;
    f. A proibição de utilização dos dados para finalidades próprias não autorizadas;
    g. A comunicação de incidentes de segurança;
    h. As regras de devolução, conservação ou eliminação dos dados após o termo da prestação de serviços;
    i. O controlo de eventuais subcontratados adicionais, quando aplicável.
3. A utilização de fornecedores tecnológicos não afasta a responsabilidade do FIS pelo cumprimento das obrigações que lhe sejam legalmente imputáveis.
4. **Transferência internacional de dados:** o FIS pode utilizar serviços tecnológicos ou prestadores localizados fora de Angola, situação que pode implicar o armazenamento, o alojamento, o acesso ou a transferência internacional de dados pessoais.
5. Qualquer transferência internacional deve ser previamente avaliada, tendo em consideração:
    a. A identificação do país de destino;
    b. A natureza e as categorias de dados transferidos;
    c. A finalidade da transferência;
    d. A entidade destinatária;
    e. O nível de protecção assegurado no destino;
    f. A existência de fundamento jurídico para a transferência;
    g. As notificações, autorizações ou formalidades eventualmente exigíveis junto da Agência de Protecção de Dados;
    h. A existência de garantias contratuais e técnicas adequadas.
6. O FIS não deve efectuar transferências internacionais de dados pessoais sem verificar previamente as condições legais aplicáveis.
7. Sempre que sejam utilizados fornecedores internacionais de serviços de alojamento, computação em nuvem, correio electrónico, análise ou suporte tecnológico, a localização dos dados e os acessos efectuados a partir do estrangeiro devem ser considerados na avaliação.

Artigo 11.º | *Prazos de conservação dos dados*

1. Os dados pessoais são conservados pelo período necessário à prossecução das finalidades que justificaram a sua recolha e tratamento, devendo a definição dos prazos considerar:
    a. A duração da relação contratual;
    b. Os prazos de execução e acompanhamento das transacções;

c. As obrigações contabilísticas e fiscais;

d. As obrigações legais e regulamentares aplicáveis;

e. A necessidade de conservação de evidências para auditorias ou defesa de direitos;

f. A existência de reclamações, litígios ou investigações pendentes;

g. Os requisitos de segurança e rastreabilidade.

2. Após o termo do período de conservação aplicável, os dados devem ser eliminados, anonimizados ou submetidos a outra forma de tratamento legalmente admissível.

3. Quando exista obrigação legal ou necessidade legítima de conservação, os dados podem permanecer armazenados durante o período correspondente, com acesso limitado e utilização restrita à finalidade que justifica a conservação.

4. Os prazos concretos devem ser definidos numa matriz interna de conservação de dados, aprovada pela Comissão Executiva.

Capítulo VI — Direitos dos Titulares e Segurança dos Dados

Artigo 12.º | *Direitos dos titulares e procedimento para o seu exercício*

1. Nos termos da legislação aplicável, os titulares dos dados podem exercer os direitos que lhes sejam legalmente reconhecidos, incluindo:

   a. **Direito à informação:** obter informação sobre a identidade da entidade responsável, as finalidades do tratamento, as categorias de dados, os destinatários e os demais elementos legalmente exigidos;

   b. **Direito de acesso:** solicitar informação sobre os dados pessoais que são tratados pelo FIS, nos termos legalmente aplicáveis;

   c. **Direito de rectificação e actualização:** solicitar a correcção ou a actualização de dados pessoais inexactos, incompletos ou desactualizados;

   d. **Direito de cancelamento ou eliminação:** solicitar o cancelamento ou a eliminação dos dados, quando estejam reunidos os pressupostos legais e não exista fundamento legítimo para a sua conservação;

   e. **Direito de oposição:** opor-se ao tratamento de dados pessoais nas situações e condições previstas na legislação aplicável;

   f. **Direito de retirada do consentimento:** retirar o consentimento anteriormente concedido, quando o tratamento se fundamente nesse consentimento, sem prejuízo da licitude do tratamento efectuado anteriormente e da existência de outros fundamentos legais;

   g. **Direito de reclamação:** apresentar reclamação junto da Agência de Protecção de Dados ou recorrer aos mecanismos administrativos e judiciais legalmente disponíveis.

2. O exercício dos direitos deve respeitar as limitações legalmente previstas e não prejudica as obrigações de conservação decorrentes da legislação aplicável.

3. **Procedimento para o exercício dos direitos:** os titulares podem apresentar pedidos relacionados com os seus dados pessoais através do correio electrónico comercial@fis-africa.com, indicando no assunto «Privacidade e Protecção de Dados», devendo o pedido, sempre que necessário, conter:
    a. A identificação do titular;
    b. A descrição do direito que pretende exercer;
    c. A identificação dos dados ou do tratamento a que o pedido se refere;
    d. Os elementos necessários à confirmação da identidade;
    e. O contacto para resposta.
4. O FIS pode solicitar informação adicional quando seja necessária para confirmar a identidade do requerente ou delimitar o pedido, evitando recolher elementos excessivos.
5. Os pedidos são encaminhados à Direcção de Risco e Compliance, que coordena a sua análise em articulação com as áreas responsáveis pelo tratamento dos dados.
6. Quando o FIS actue como subcontratado, o pedido deve ser encaminhado ao responsável pelo tratamento competente, sempre que a decisão sobre o exercício do direito lhe caiba, sem prejuízo do apoio que o FIS deva prestar.
7. A resposta é prestada nos prazos legalmente aplicáveis e de acordo com os procedimentos internos estabelecidos.

Artigo 13.º | *Segurança, confidencialidade e violações de dados pessoais*

1. O FIS adopta medidas técnicas e organizativas destinadas a proteger os dados pessoais contra destruição, perda, alteração, divulgação ou acesso não autorizados, proporcionais à natureza dos dados, às finalidades do tratamento e aos riscos associados.
2. Entre as medidas que podem ser implementadas incluem-se:
    a. O controlo de acessos por perfis e permissões;
    b. A autenticação dos utilizadores;
    c. A protecção das credenciais de acesso;
    d. A cifragem da informação, quando adequada;
    e. A protecção das comunicações e das integrações tecnológicas;
    f. O registo de acessos e actividades relevantes;
    g. A monitorização de eventos e actividades suspeitas;
    h. As cópias de segurança e os mecanismos de recuperação;
    i. A actualização e a manutenção dos sistemas;
    j. A protecção contra software malicioso e acessos indevidos;
    k. A formação e a sensibilização dos colaboradores;
    l. Os compromissos de confidencialidade;
    m. Os procedimentos de gestão de incidentes.

3. A Direcção de Tecnologia e Inovação é responsável pela implementação e manutenção dos controlos tecnológicos, em articulação com a Direcção de Risco e Compliance.
4. A segurança dos dados pessoais deve ser considerada em todas as fases de desenvolvimento, aquisição, configuração e utilização das soluções tecnológicas do FIS.
5. **Confidencialidade e dever de sigilo:** todas as pessoas que, no exercício das suas funções, tenham acesso a dados pessoais tratados pelo FIS estão obrigadas a preservar a sua confidencialidade.
6. O dever de sigilo mantém-se mesmo após o termo da relação laboral, contratual ou profissional, sem prejuízo das comunicações legalmente obrigatórias.
7. A informação pessoal não deve ser divulgada, reproduzida, transmitida ou utilizada para finalidades estranhas às funções desempenhadas.
8. O FIS deve assegurar que os colaboradores e prestadores de serviços assumem formalmente as obrigações de confidencialidade aplicáveis.
9. **Violações de dados pessoais e incidentes de segurança:** o FIS deve adoptar mecanismos para identificar, registar, avaliar e tratar os incidentes que possam comprometer a confidencialidade, a integridade ou a disponibilidade dos dados pessoais, constituindo exemplos de incidentes:
    a. O acesso não autorizado a dados pessoais;
    b. A divulgação indevida de informação;
    c. A perda ou o roubo de equipamentos ou suportes;
    d. O envio de informação a destinatário incorrecto;
    e. A alteração ou a eliminação não autorizada de dados;
    f. O comprometimento de credenciais;
    g. Os ataques cibernéticos que afectem dados pessoais;
    h. A exposição indevida de informação em plataformas ou sistemas.
10. Todos os colaboradores e prestadores de serviços devem comunicar imediatamente os incidentes identificados através dos canais internos estabelecidos.
11. A Direcção de Tecnologia e Inovação deve assegurar a contenção técnica e a preservação de evidências.
12. A Direcção de Risco e Compliance deve coordenar a avaliação dos impactos sobre os titulares, o enquadramento legal e as medidas de comunicação ou reporte que se revelem necessárias.
13. O FIS deve comunicar as violações de dados às autoridades competentes e aos titulares afectados sempre que tal seja legalmente exigido, observando os requisitos e prazos aplicáveis.
14. As ocorrências devem ser documentadas, incluindo a natureza do incidente, os dados afectados, as consequências identificadas, as medidas adoptadas e as acções correctivas.

Capítulo VII — Menores, Privacidade desde a Concepção, Comunicações e Contactos

Artigo 14.º | *Dados de menores e privacidade desde a concepção e por defeito*

1. O FIS pode tratar dados de menores quando estes sejam beneficiários ou dependentes abrangidos pelos planos de saúde e pelas relações contratuais estabelecidas com as empresas clientes.
2. Nestas situações, o tratamento deve limitar-se aos elementos estritamente necessários à identificação do beneficiário e à execução das operações de coparticipação.
3. O FIS deve assegurar que o tratamento respeita as regras legais aplicáveis à representação dos menores e ao exercício dos respectivos direitos.
4. Sempre que exigível, a informação e as autorizações necessárias devem ser obtidas junto dos pais, dos representantes legais ou das entidades legitimadas.
5. O FIS não deve utilizar os dados de menores para finalidades comerciais ou promocionais incompatíveis com a finalidade que justificou a sua recolha.
6. **Privacidade desde a concepção e por defeito:** o FIS deve integrar requisitos de privacidade e protecção de dados desde a concepção, o desenvolvimento, a aquisição e a actualização das suas plataformas e soluções tecnológicas, implicando este princípio:
    a. Recolher apenas os dados necessários;
    b. Definir finalidades específicas para cada operação de tratamento;
    c. Configurar permissões de acesso adequadas;
    d. Evitar a exposição desnecessária de informação;
    e. Implementar mecanismos de protecção por defeito;
    f. Limitar a conservação dos dados;
    g. Avaliar os riscos antes da introdução de novos tratamentos;
    h. Considerar a privacidade na integração com terceiros;
    i. Assegurar que os dados não ficam acessíveis por defeito a pessoas não autorizadas.
7. Sempre que uma actividade de tratamento apresente riscos elevados para os direitos e liberdades dos titulares, deve ser avaliada a necessidade de uma análise de impacto e das formalidades legalmente aplicáveis.

Artigo 15.º | *Comunicações electrónicas, marketing e cookies*

1. O FIS pode utilizar os contactos disponibilizados pelos titulares para comunicações relacionadas com a execução dos serviços, informações operacionais, suporte, segurança e cumprimento de obrigações contratuais.
2. As comunicações promocionais e de marketing são efectuadas de acordo com os requisitos legais aplicáveis, devendo o FIS, quando o consentimento seja necessário, assegurar que este é obtido de forma livre, específica e informada.

3. Os titulares devem dispor de mecanismos adequados para deixar de receber comunicações promocionais, sem que tal prejudique as comunicações necessárias à execução dos serviços ou ao cumprimento de obrigações legais.
4. O FIS não deve utilizar dados pessoais obtidos no âmbito da gestão de coparticipações para campanhas comerciais incompatíveis com a finalidade original da recolha.
5. **Cookies e tecnologias de rastreamento:** o website do FIS pode utilizar cookies e tecnologias semelhantes para assegurar o seu funcionamento, melhorar a experiência de navegação, compreender a utilização das páginas e reforçar a segurança.
6. Os cookies são pequenos ficheiros ou identificadores que podem ser armazenados no dispositivo do utilizador durante a navegação, podendo ser utilizadas, conforme a sua finalidade, as categorias constantes do Quadro 1.
7. A utilização de cookies não essenciais deve respeitar os requisitos legais aplicáveis, incluindo a prestação de informação e a obtenção de consentimento quando exigível.
8. Os utilizadores podem gerir as preferências de cookies através das funcionalidades disponibilizadas pelo website e das configurações do respectivo navegador.
9. O FIS deve manter informação actualizada sobre os cookies efectivamente utilizados, incluindo a sua finalidade, duração e eventual partilha com terceiros.

Quadro 1 — Categorias de cookies

Categoria	Finalidade
Cookies estritamente necessários	Assegurar as funcionalidades essenciais do website, incluindo a navegação, a segurança e o funcionamento técnico
Cookies de desempenho e análise	Compreender a forma como os visitantes utilizam o website, identificar dificuldades de navegação e melhorar os serviços disponibilizados
Cookies de funcionalidade	Recordar determinadas preferências e melhorar a experiência de utilização
Cookies de publicidade ou marketing	Medir campanhas ou apresentar conteúdos promocionais, quando existam e estejam devidamente implementados

Artigo 16.º | *Contactos e reclamações*

1. Para esclarecimentos, pedidos de informação ou exercício dos direitos relacionados com a privacidade e a protecção de dados, os titulares podem contactar o FIS através de:
    a. Correio electrónico institucional: comercial@fis-africa.com;
    b. Correio electrónico de suporte: suporte@fis-africa.com;
    c. Website: https://www.fis-africa.com.
2. Os titulares podem igualmente recorrer à Agência de Protecção de Dados, enquanto autoridade competente em matéria de protecção de dados pessoais em Angola, sem prejuízo dos demais mecanismos administrativos e judiciais legalmente disponíveis.

Capítulo VIII — Disposições Finais

Artigo 17.º | *Alterações e disposições finais*

1. O FIS pode actualizar a presente Política sempre que ocorram alterações relevantes na legislação, no modelo de negócio, nas tecnologias utilizadas, nas finalidades de tratamento ou nas relações com terceiros.
2. As alterações são divulgadas através do website institucional ou de outros canais adequados, com indicação da data da última actualização.
3. Quando as alterações impliquem modificações relevantes nas condições de tratamento dos dados pessoais, os titulares são informados nos termos legalmente aplicáveis.
4. A presente Política constitui o referencial institucional do FIS em matéria de privacidade e protecção de dados pessoais.
5. A sua aplicação deve ser articulada com as políticas e os procedimentos internos relacionados com segurança cibernética, gestão operacional, controlo de transacções, gestão de reclamações, gestão de riscos, compliance e controlo interno.
6. Nenhuma disposição da presente Política deve ser interpretada como autorização para o tratamento de dados pessoais em desconformidade com a legislação aplicável.
7. As situações omissas ou as dúvidas de interpretação devem ser submetidas à Direcção de Risco e Compliance, em articulação com as áreas competentes, para apreciação pela Comissão Executiva sempre que necessário.
8. A presente Política entra em vigor na data da sua aprovação pela Comissão Executiva e é disponibilizada aos titulares e demais interessados através dos canais institucionais do FIS.

Anexo I — Matriz de Síntese de Responsabilidades

Interveniente	Responsabilidade / Competência	Referência
Comissão Executiva	Aprovar a Política e as suas alterações; assegurar os recursos necessários à sua implementação; aprovar as medidas estratégicas de protecção de dados e a matriz interna de conservação de dados; acompanhar os riscos relevantes de privacidade e segurança; deliberar sobre as situações que exijam decisão superior, incluindo as situações omissas.	Art. 6.º, 11.º e 17.º
Direcção de Risco e Compliance	Coordenar a implementação da Política; acompanhar o cumprimento das obrigações legais de protecção de dados; avaliar os riscos do tratamento e, previamente, o tratamento excepcional de dados sensíveis; coordenar o tratamento dos pedidos dos titulares; acompanhar as comunicações e partilhas de dados; avaliar a necessidade de notificações ou autorizações junto da APD; coordenar a avaliação de violações de dados; promover a sensibilização; acompanhar os instrumentos internos; reportar à Comissão Executiva.	Art. 5.º, 6.º, 12.º, 13.º e 17.º

Direcção de Contabilidade e Finanças	Assegurar a confidencialidade dos dados financeiros e contabilísticos; limitar o acesso à informação financeira aos intervenientes autorizados; garantir a utilização dos dados exclusivamente para finalidades legítimas; cumprir os requisitos de conservação documental; apoiar a correcção de dados financeiros inexactos; comunicar incidentes ou acessos indevidos à informação sob a sua responsabilidade.	Art. 6.º
Direcção de Tecnologia e Inovação	Implementar e manter os controlos técnicos de segurança; assegurar a gestão de acessos e permissões; proteger os sistemas e as bases de dados; implementar mecanismos de registo e rastreabilidade; assegurar a segurança das integrações e transmissões; assegurar a contenção técnica dos incidentes e a preservação de evidências; implementar medidas de recuperação e continuidade; apoiar a eliminação ou anonimização técnica dos dados.	Art. 6.º e 13.º
Direcção Comercial	Assegurar a recolha adequada de dados no âmbito das relações comerciais; informar os clientes e parceiros sobre as práticas de tratamento; garantir a origem e o fundamento legítimos dos dados recebidos; evitar a divulgação não autorizada de dados pessoais; assegurar que as comunicações comerciais respeitam as preferências e os direitos dos titulares; encaminhar os pedidos e reclamações sobre privacidade para a área competente.	Art. 6.º
Gabinete de Auditoria Interna	Avaliar, de forma independente, a adequação dos controlos de protecção de dados; verificar o cumprimento da Política e dos procedimentos associados; avaliar a eficácia dos mecanismos de acesso, conservação e segurança; identificar deficiências e formular recomendações; acompanhar a implementação das recomendações; não assumir a execução dos controlos operacionais nem a gestão corrente dos dados pessoais.	Art. 6.º
Colaboradores e prestadores de serviços	Cumprir a Política e os procedimentos aplicáveis; utilizar os dados exclusivamente para as finalidades autorizadas; respeitar os deveres de confidencialidade e de sigilo, mesmo após o termo da relação; proteger as credenciais e os equipamentos; não partilhar informação com pessoas não autorizadas; comunicar imediatamente incidentes ou suspeitas de violação; participar nas acções de sensibilização e formação.	Art. 6.º e 13.º