



República de Moçambique

PROPOSTA DE LEI DE PROTECÇÃO DE DADOS PESSOAIS

FUNDAMENTAÇÃO

A Evolução das Tecnologias de Informação e Comunicação tem proporcionado avanços de captação e armazenamento de grandes volumes de dados e informações, por isso, é imprescindível um controle do Estado para que os direitos fundamentais previstos constitucionalmente não sejam violados, garantindo assim, maior protecção do cidadão, e consequentemente não permitir o uso impróprio pelas entidades responsáveis pelo tratamento dos dados pessoais.

A protecção de dados pessoais é um direito fundamental que encontra o seu enquadramento jurídico no número 1 do artigo 71 da Constituição da República, que proíbe a utilização de meios informáticos para o registo e tratamento de dados individualmente identificáveis relativos às convicções políticas, filosóficas ou ideológicas, à fé religiosa, à partidária ou sindical e à vida privada, outrossim, o número 2 do mesmo artigo, remete a regulamentação específica a protecção de dados pessoais constantes dos registos informáticos, as condições de acesso as bases de dados, de constituição e utilização por autoridades públicas e entidades privadas destas bases de dados ou de suportes informáticos.

A Lei n.º 3/2017, de 09 de Janeiro, de Transacções Electrónicas, no seu artigo 64, relativo a protecção de dados pessoais electrónicos pessoais, proíbe o acesso a arquivos, a ficheiros e registos informáticos ou de base de dados para conhecimento de dados pessoais relativos a terceiros, nem a transferência de dados pessoais de um para outro ficheiro informático pertencente a distintos serviços ou instituições, salvo nos casos estabelecidos por diploma legal ou por decisão judicial.

A Assembleia da República, através da Resolução n.º 5 de 2019, de 20 de Junho, ratificou a Convenção da União Africana sobre ciber segurança e protecção de dados pessoais, adoptada pela 23ª Sessão da União Africana de Chefes de Estados e de Governo da União Africana, a 27 de Junho de 2014, em Malabo – Guiné Equatorial, cujo objectivo relativamente a protecção de dados pessoais, encontra-se, no artigo 8, onde, cada Estado, se compromete a criar um quadro jurídico, com vista a reforçar os direitos fundamentais e as liberdades públicas, nomeadamente a protecção de dados pessoais físicos, e reprimir qualquer infracção relativa à vida privada, sem prejuízo do princípio da liberdade de circulação de dados pessoais.

Ainda no âmbito da Convenção retro mencionada, no seu artigo 11, estabelece que, cada Estado deve criar uma Autoridade responsável pela matéria de protecção de dados pessoais.

É neste contexto que, ao abrigo da alínea c), do número 1, do artigo 203, da Constituição da República de Moçambique, o Conselho de Ministros submete a presente Proposta de Lei de Protecção de dados pessoais, para apreciação e aprovação pela Assembleia da República.

Novembro 2025



República de Moçambique

Assembleia da República

Lei n.º /2025

de de.....

Havendo necessidade de estabelecer o Regime Jurídico de Protecção de Dados Pessoais, com vista a garantir a segurança de dados pessoais constantes de registos em formato físico e informático, a sua constituição e as condições de acesso a base de dados, sua utilização por entidades públicas e privadas, tendo em conta os desafios impostos pelas tecnologias de informação e comunicação, em conformidade com a legislação nacional e padrões de boas práticas internacionais, ao abrigo do número 1, do artigo 178 da Constituição da República, a Assembleia da República determina:

CAPÍTULO I

DISPOSIÇÕES GERAIS

ARTIGO 1

(Objecto)

A presente Lei estabelece os princípios e as regras aplicáveis ao tratamento de dados pessoais constantes em registos físicos e informáticos por entidades públicas e privadas, bem como proteger os direitos e liberdades fundamentais das pessoas singulares.

ARTIGO 2

(Âmbito)

1. A presente Lei aplica-se a qualquer operação ou conjunto de operações que envolvam o tratamento de dados pessoais, por meios automatizados ou não automatizados, realizado por

peças singulares ou colectivas, de direito público ou privado, independentemente do meio utilizado, do local da sede do agente de tratamento ou do local onde os dados estão armazenados, desde que a operação de tratamento seja realizada no território nacional.

2. A presente Lei aplica-se também ao tratamento de dados pessoais efectuado fora do território nacional por agente de tratamento sujeito à jurisdição moçambicana, ainda que o titular dos dados não se encontre em território nacional, sempre que tal tratamento possa produzir efeitos jurídicos ou relevantes no país ou envolva a monitorização do comportamento de titulares de dados que se encontrem em território nacional.

3. A presente Lei não se aplica:

- a) ao processamento de dados feitos por uma pessoa singular no quadro exclusivo das suas actividades pessoais ou domésticas, desde que esses dados não sejam destinados a uma comunicação sistemática a terceiros ou à difusão;
- b) as cópias temporárias feitas no quadro das actividades técnicas de transmissão e acesso a uma rede digital, com o objectivo de armazenamento automático, intermédio e temporário de dados, tendo como finalidade exclusiva permitir aos destinatários do serviço o melhor acesso possível às informações enviadas;
- c) ao tratamento de dados pessoais realizado para fins exclusivamente jornalísticos, na medida estritamente necessária ao exercício da liberdade de imprensa, devendo ser respeitados sempre que possível os direitos fundamentais dos titulares;
- d) ao tratamento de dados para expressão artística, expressão literária, investigação científica, desde que seja comprovada a referida actividade e que esta, não viole os direitos fundamentais dos titulares, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas singulares;
- e) ao tratamento de dados realizado para fins de segurança pública ou de defesa nacional, desde que devidamente fundamentado pela autoridade competente e sujeita ao princípio da necessidade e proporcionalidade.

ARTIGO 3

(Definições)

1. Para efeitos da presente Lei, **dados pessoais** é toda informação de qualquer natureza e independentemente do respectivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável, titular dos dados.

2. As demais definições dos termos constam do glossário em anexo, o qual é parte integrante da mesma, contendo natureza normativa e vinculativa para a interpretação e aplicação das suas disposições.

Artigo 4 **(Objectivos)**

1. São objectivos da presente Lei:
 - a) assegurar o respeito à pela privacidade, intimidade, honra e imagem das pessoas singulares;
 - b) garantir a autodeterminação informativa e a protecção contra qualquer forma de discriminação decorrente do tratamento de dados pessoais;
 - c) a liberdade de expressão, de informação, de comunicação e de opinião em equilíbrio com o direito à privacidade;
 - d) promover o livre exercício dos direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas singulares;
 - e) promover o desenvolvimento económico, tecnológico e a inovação de forma ética, segura e sustentável;
 - f) promover a livre iniciativa, a livre concorrência e a protecção do consumidor, em equilíbrio com a protecção dos dados pessoais;
 - g) garantir a interoperabilidade e a portabilidade dos dados de forma segura e responsável, facilitando o fluxo transfronteiriço legítimo dos dados e harmonização com as normas internacionais;
 - h) reforçar a soberania digital nacional, assegurando que o tratamento de dados pessoais respeite tanto os interesses do titular como as leis e fins estratégicos do Estado, sem prejuízo da cooperação internacional e da protecção dos direitos fundamentais.
2. A presente Lei visa igualmente contribuir para:
 - a) o desenvolvimento económico, tecnológico e a inovação;
 - b) a livre iniciativa, a livre concorrência e a defesa do consumidor;
 - c) garantir a interoperabilidade e a portabilidade dos dados de forma segura e responsável, facilitando o fluxo transfronteiriço legítimo de dados e o diálogo com as normas internacionais;

- d) reforçar a soberania digital nacional, assegurando que o tratamento de dados pessoais respeita tanto os interesses do titular como as leis e fins estratégicos do Estado, sem prejuízo da cooperação internacional e da Protecção dos direitos fundamentais.

ARTIGO 5

(Princípios)

O tratamento de dados pessoais deve orientar-se pelos seguintes princípios:

- a) **consentimento e de legitimidade** - o processamento de dados pessoais é considerado legítimo quando o titular dos dados der o seu consentimento;
- b) **transparência** - consiste na garantia aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento de dados pessoais e os respectivos agentes de tratamento, observados os segredos empresariais;
- c) **finalidade** - determina que o tratamento de dados pessoais deve ser feito para propósitos legítimos e específicos, explícito e informado ao titular sem possibilidade de tratamento posterior de forma incompatível com esses fins;
- d) **da necessidade** - estabelece que o tratamento de dados pessoais deve se limitar ao mínimo necessário para a realização de suas finalidades, abrangendo apenas os dados pertinentes, proporcionais e não excessivos em relação às finalidades para as quais são tratados;
- e) **legalidade** - consiste na observância da lei durante a recolha, registo, processamento, armazenamento, partilha e transmissão de dados pessoais;
- f) **segurança** - os dados pessoais devem ser processados num ambiente protegido, prevenindo contra o tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação accidental, adoptando medidas técnicas e administrativas adequadas;
- g) **prevenção** - o tratamento de dados pessoais deve ser realizado com a adopção de medidas capazes de prevenir a ocorrência de danos em virtude do tratamento, garantindo a protecção contra riscos e irregularidades antes que eles se concretizem;
- h) **livre acesso** - consiste em assegurar ao titular o direito de aceder, de forma fácil e gratuita, informações sobre como seus dados são tratados, em sua integralidade, durante o período de tratamento;

- i) **precaução** - determina que, na ausência de certeza científica sobre os efeitos de uma determinada operação de tratamento de dados, devem ser tomadas medidas para antecipar e mitigar potenciais danos;
- j) **proporcionalidade** - os dados pessoais devem ser pertinentes, adequados e não excessivos à finalidade que legitimou o tratamento;
- k) **exactidão** - os dados pessoais, devem ser exactos, actualizados, tendo em conta os fins para os quais foram recolhidos e posteriormente processados;
- l) **responsabilização e prestação de contas** - consiste na demonstração pelo agente de tratamento da adopção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de protecção de dados pessoais inclusive da eficácia dessas medidas;
- m) **conservação e duração** - os dados pessoais devem ser conservados de forma íntegra durante o período necessário para a finalidade definida para o tratamento ou prazo prescrito, devendo ser posteriormente eliminados ou tornados anónimos;
- n) **não discriminação** - o tratamento de dados pessoais não pode ser realizado para fins discriminatórios ilícitos ou abusivos;
- o) **boa - fé** – o tratamento de dados pessoais, deve cingir-se na lealdade, honestidade e probidade;
- p) **interoperabilidade** - forma de tratamento dos dados que consiste na possibilidade de relacionamento de um ficheiro com os dados de outro ou outros ficheiros mantidos pelo mesmo responsável ou por outro ou outros responsáveis com a mesma finalidade.

CAPÍTULO II

Organização do Sistema Nacional de Protecção de Dados Pessoais

SECÇÃO I

Estrutura do Sistema Nacional de Protecção de Dados Pessoais

ARTIGO 6

(Composição)

1. O Sistema Nacional de protecção de dados pessoais é composto por órgãos e entidades.
2. São órgãos do Sistema Nacional de protecção de dados pessoais:

- a) Conselho Nacional de protecção de dados pessoais;
 - b) Autoridade Nacional de protecção de dados pessoais.
3. São entidades do Sistema Nacional de protecção de dados pessoais:
- a) Provedores Intermediários de Serviços Electrónicos;
 - b) Operadores de Serviços Essenciais;
 - c) Provedores de Serviços Digitais;
 - d) Operadores de Plataformas Digitais;
 - e) Operadores de Centros de Dados;
 - f) Operadores de Plataformas de Computação em Nuvem;
 - g) Operadores de Comunicações Digitais.

Subsecção I

Conselho Nacional de protecção de dados pessoais

ARTIGO 7

(Natureza)

O Conselho Nacional de protecção de dados pessoais (CNPD) é o órgão multisectorial de coordenação e de governação específica para assuntos relativos a protecção de dados pessoais e é presidido pelo Primeiro-Ministro.

ARTIGO 8

(Composição)

1. O Conselho Nacional de protecção de dados pessoais tem a seguinte composição:

- a) Os titulares que superintendem as seguintes áreas:
 - i. Defesa Nacional;
 - ii. Segurança de Estado;
 - iii. Segurança Interna;
 - iv. Tecnologias de Informação e Comunicação;
 - v. Justiça;
 - vi. Transportes;
 - vii. Finanças;
 - viii. Educação;

- ix. Saúde;
- x. Criança e Acção social;
- xi. Energia.

b) Representantes das seguintes entidades:

- i. Regulador de TIC;
- ii. Regulador das Comunicações;
- iii. Regulador do Sector Financeiro;
- iv. Regulador do Sector de Águas;
- v. Regulador do Sector de Energia;
- vi. Regulador do Sector de Investigação Científica em Saúde Humana;
- vii. Ministério Público;
- viii. Serviço Nacional de Investigação Criminal;
- ix. Instituto Nacional de Estatística;
- x. Equipa Nacional de Resposta a Incidentes de Segurança Cibernética (CSIRT Nacional);
- xi. Representante do sector empresarial;
- xii. Representante do sector académico;
- xiii. Representante da sociedade civil.

2. Sempre que se mostre necessário, desde que devidamente fundamentada a pertinência, podem ser convidados outras entidades, para matérias específicas.

3. Os representantes do sector empresarial, da academia e da sociedade civil são designados pelas respectivas organizações.

ARTIGO 9 (Competências)

1. Compete ao Conselho Nacional de protecção de dados pessoais:

- a) assegurar a coordenação político-estratégica para a protecção de dados pessoais;
- b) elaborar anualmente, o relatório de avaliação da implementação da Política e Estratégia Nacional de protecção de dados;
- c) responder as solicitações por parte do Governo, no âmbito das suas competências.

2. As regras de organização, funcionamento e demais competências do Conselho Nacional de protecção de dados pessoais são estabelecidos em regulamento específico.

Subsecção II
Autoridade Nacional de protecção de dados pessoais

ARTIGO 10
(Natureza)

A Entidade Reguladora de Tecnologias de Informação e Comunicação é a Autoridade Nacional de protecção de dados pessoais (ANPD) no âmbito da presente Lei.

ARTIGO 11
(Atribuições da ANPD)

1. A ANPD actua com independência funcional e imparcialidade no desempenho de suas competências reguladoras, fiscalizadoras e sancionatórias, nos termos da presente Lei.
2. A ANPD é tutelada pelo Ministro que superintende a área de Tecnologia de Informação e Comunicação (TIC), sem prejuízo da sua independência funcional e decisória.
3. A organização e o funcionamento da ANPD são regulados pelo seu estatuto orgânico, aprovado pelo Conselho de Ministros.
4. A adequação do nível de protecção de dados pessoais de um Estado é apreciada pela ANPD em função de todas as circunstâncias que envolvam a transferência ou o conjunto de transferência de dados pessoais, atendendo em especial a natureza deles, a finalidade e a duração dos tratamentos projectados aos países de destino final e as regras de direito gerais ou sectoriais em vigor no Estado em causa, incluindo as regras profissionais e as medidas de segurança que são respeitadas nele.

ARTIGO 12
(Competências da ANPD)

1. Compete à ANPD:

- a) emitir normas regulamentares, directrizes e orientações técnicas para a aplicação da presente Lei, abrangendo o tratamento de dados pessoais em formato físico e digital;
- b) fiscalizar o cumprimento das disposições da presente Lei, independentemente do meio em que os dados sejam tratados;
- c) aplicar sanções administrativas em casos de infração;
- d) receber reclamações relacionadas com violações da presente lei ou da legislação subsidiária elaborada ao abrigo da presente lei;
- e) registar os responsáveis pelo tratamento de dados e os subcontratantes de importância significativa;
- f) quando necessário, credenciar, licenciar e registar pessoas adequadas para prestar serviços de conformidade com a protecção de dados;
- g) receber e apurar denúncias relacionadas a violações de dados pessoais, tanto em meios físicos quanto informáticos;
- h) promover a sensibilização e a compreensão do público sobre a protecção de dados pessoais, os direitos e obrigações impostos pela presente lei;
- i) promover a sensibilização para as obrigações dos responsáveis pelo tratamento de dados e dos subcontratantes ao abrigo da presente lei;
- j) intervir nos processos judiciais em caso de violação do disposto na presente Lei, devendo comunicar ao Ministério Público as violações de que tenha conhecimento no exercício das suas funções e em consequência das mesmas, bem como adoptar as medidas cautelares necessárias e urgentes para assegurar os meios de prova;
- k) promover a consciencialização pública sobre a protecção de dados pessoais e os direitos dos titulares de dados;
- l) cooperar com autoridades internacionais de protecção de dados pessoais em questões transfronteiriças;
- m) elaborar e publicar relatórios anuais de suas actividades, incluindo fiscalizações realizadas, denúncias tratadas e sanções aplicadas;
- n) zelar pela observância dos segredos comercial e industrial, observada a protecção de dados pessoais, do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do artigo 5 da presente Lei;
- o) promover e elaborar os estudos sobre as práticas nacionais e internacionais de protecção de dados pessoais e privacidade;

- p) autorizar a transferência transfronteiriça de dados pessoais quando o país receptor não tiver lei específica da matéria;
 - q) arrecadar e aplicar as suas receitas;
 - r) estabelecer mecanismos de cooperação com as suas congéneres em matéria de protecção de dados pessoais;
 - s) participar em negociações internacionais em matéria de protecção de dados pessoais.
2. A ANPD determina a elaboração da Avaliação Prévia de Impacto pelos agentes de tratamento de dados pessoais.
 3. A ANPD é responsável por regular todas as operações que envolvam o tratamento de dados pessoais realizados no território nacional, independentemente do formato em que os dados se encontram, além de exercer competência sobre operações transfronteiriças envolvendo tratamento de dados pessoais dos cidadãos moçambicanos fora do território nacional.

CAPÍTULO III

Tratamento de dados pessoais

SECÇÃO I

Requisitos para o tratamento de dados pessoais

ARTIGO 13

(Tratamento de dados pessoais)

1. Salvo disposição legal em contrário, o tratamento de dados pessoais só pode ser efectuado nas seguintes situações:
 - a) quando o seu titular tiver dado de forma expressa e inequívoca o seu consentimento;
 - b) cumprimento de obrigação legal, a que o responsável pelo tratamento esteja sujeito;
 - c) pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos ou instrumentos congêneres, observadas as disposições da presente Lei;
 - d) execução de uma missão de interesse público ou dever social no exercício de autoridade pública em que esteja investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados;

- e) execução de contrato ou contratos em que o titular dos dados seja parte ou de diligências prévias à formação do contrato ou declaração negocial efectuada a seu pedido;
 - f) exercício regular de direitos em processo judicial, administrativo ou arbitral;
 - g) solvabilidade do crédito, inclusive quanto ao disposto na legislação aplicável a matéria;
 - h) para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente;
 - i) legítimo interesse do responsável pelo tratamento dos dados pessoais desde que não suprima o direito fundamental previsto na Constituição da República de Moçambique;
 - j) para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
 - k) o tratamento seja necessário para proteger os interesses vitais do titular de dados ou de outra pessoa singular.
2. O consentimento do titular dos dados pessoais pode ser dispensado quando:
- a) a exigência do consentimento previsto no articulado número 1 do presente artigo para os dados pessoais tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos na presente Lei;
 - b) a eventual dispensa da exigência do consentimento não escusa os agentes de tratamento das demais obrigações previstas na presente Lei, especialmente a observância dos princípios gerais e da garantia dos direitos do titular.
 - c) O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.
3. As regras de processamento de dados pessoais são matéria a regulamentar pela ANDP.

ARTIGO 14
(Do consentimento)

1. A definição do consentimento garante que qualquer autorização seja dada pelo titular de forma livre, explícita, informada e específica.
2. O consentimento deve ser fornecido de forma expressa por escrito ou por outro meio que demonstre a manifestação de vontade do titular.
3. Quando o tratamento for realizado com base no consentimento, o responsável pelo tratamento deve poder demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais.
4. É vedado o tratamento de dados pessoais mediante vício de consentimento.
5. O titular dos dados tem o direito de retirar o seu consentimento a qualquer momento, mediante manifestação expressa do titular, por procedimento gratuito e facilitado, sem prejuízo da licitude do tratamento já realizado com base no consentimento previamente dado.
6. Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto na presente Lei.

ARTIGO 15

(Requisitos específicos para o tratamento de dados sensíveis)

1. É proibido o tratamento de dados pessoais que revelem:
 - a) ascendência, sexo, raça, origem étnica;
 - b) convicções políticas, crenças religiosas ou convicções filosóficas;
 - c) filiação em associação política ou sindical;
 - d) informação médica, vida privada, informação genética ou de forma geral, informações relativas ao estado de saúde do titular dos dados;
 - e) dados biométricos que identificam de forma inequívoca uma pessoa;
 - f) dados relacionados a condenações penais e infracções.
2. A proibição estabelecida no número 1 do presente artigo, não se aplica para as categorias de tratamento de dados pessoais, quando:
 - a) o tratamento dos dados for efectuado com o consentimento inequívoco, expresso e escrito do titular dos dados ou do seu representante legal;
 - b) o processamento for necessário para o cumprimento de uma obrigação legal ou regulamentar à qual o responsável pelo tratamento esteja vinculado;
 - c) o processamento for necessário por motivo de interesse público, especialmente para fins históricos, artísticos, estatísticos, científicos, jornalísticos e de investigação com autorização da ANPD;

- d) o processamento de dados pessoais for necessário para protecção de interesses vitais do titular dos dados, se aquele estiver fisicamente ou legalmente incapaz de dar o seu consentimento;
- e) em caso de processo judicial ou investigação criminal;
- f) para fins de medicina preventiva, diagnósticos médicos ou tratamentos médicos, incluindo dados relacionados à saúde e à vida sexual;
- g) o tratamento for realizado por profissionais de saúde sujeitos ao segredo profissional e em conformidade com normas aplicáveis.

ARTIGO 16

(Requisitos específicos para o tratamento de dados de crédito e de solvabilidade)

1. Sem prejuízo das disposições aplicáveis, o tratamento de dados pessoais relativos ao crédito e à solvabilidade só pode ser efectuado mediante:
 - a) cumprimento de obrigações legais ou contratuais, especialmente em situações que envolvam instituições financeiras, operadores de crédito ou outras entidades reguladas;
 - b) garantia de que o tratamento dos dados é limitado à finalidade específica, como a análise de crédito, gestão de risco e prevenção de fraude;
 - c) medidas técnicas e organizativas adequadas, que assegurem a protecção dos dados contra acessos não autorizados, perdas, ou qualquer forma de tratamento ilícito;
 - d) direito do titular dos dados de aceder as informações tratadas, corrigir imprecisões ou solicitar a exclusão dos dados quando não forem mais necessários para as finalidades declaradas.
2. É proibida a utilização dos dados pessoais de crédito e solvabilidade para finalidades incompatíveis com o propósito originalmente informado ao titular, salvo por obrigação legal ou regulamentar devidamente justificada.

ARTIGO 17

(Requisitos específicos para tratamento de dados de crianças)

1. O tratamento de dados pessoais de crianças deve ser realizado no seu melhor interesse, conforme disposto na presente Lei e na legislação específica aplicável.
2. Nos termos previstos na legislação específica, considera-se criança a pessoa menor de 18 anos de idade.
3. É obrigatório obter o consentimento livre, expresso, informado e específico por um dos pais ou responsável legal para o tratamento de dados pessoais de crianças, salvo exceções previstas na presente Lei.
4. A colecta de dados pessoais de crianças sem o consentimento é permitida:
 - a) apenas uma única vez quando necessária para contactar os pais ou representante legal, sem a possibilidade de armazenamento posterior;
 - b) para sua protecção vital quando o tratamento for necessário para garantir a protecção da criança, sendo proibido a transferência dos dados a terceiros sem o consentimento dos pais ou representante legal.
5. Os controladores de dados devem assegurar a transparência, tornando públicas as seguintes informações:
 - a) o tipo de dado pessoal colectado;
 - b) a finalidade específica do uso desses dados;
 - c) os direitos da criança e dos seus responsáveis, bem como os meios para o seu exercício;
 - d) os procedimentos disponíveis para o exercício dos direitos previstos na presente Lei.
6. É proibido condicionar a participação de crianças em jogos online, aplicações de internet ou outras actividades ao fornecimento de informações pessoais que não sejam estritamente necessárias para o uso dessas plataformas.
7. O controlador é responsável por realizar todos os esforços razoáveis para verificar que o consentimento fornecido foi efectivamente dado por um dos pais ou responsável legal da criança, considerando as tecnologias disponíveis.
8. A transferência internacional de dados pessoais de crianças só pode ocorrer para Estados com nível de protecção adequado reconhecido pela ANDP ou mediante garantias contratuais específicas que asseguram protecção equivalente à prevista.
9. As informações sobre o tratamento de dados pessoais devem ser apresentadas de forma simples, clara e acessível, tendo em conta:
 - a) as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais da criança;

- b) a utilização de recursos audiovisuais sempre que apropriado, para garantir a compreensão das informações aos pais ou representante legal e adequada ao entendimento da criança.
10. Exclui-se a responsabilidade do controlador de dados, nos casos em que o consentimento tenha sido viciado por negligência ou acto deliberado do representante legal da criança.

ARTIGO 18

(Requisitos específicos para tratamento de dados pessoais para gravação de chamadas)

1. A gravação de chamadas é admitida quando realizada no âmbito de práticas comerciais lícitas, para o efeito de prova de uma transacção comercial, desde que se verifique uma das seguintes situações:
 - a) o tratamento de dados pessoais cumpra os princípios da legalidade, finalidade, transparência, proporcionalidade, conforme previstos na presente Lei;
 - b) o titular dos dados pessoais tenha dado previamente o seu consentimento expreso e inequívoco à gravação, devendo está iniciar com o registo do consentimento, salvo o disposto no número 1 do artigo 15, da presente Lei;
 - c) a gravação limite-se estritamente à finalidade declarada, sem que os dados pessoais sejam reutilizados ou partilhados para outros fins sem o consentimento adicional do titular, salvo o disposto no número 1 do artigo 15 da presente Lei;
 - d) a ANPD tenha autorizado tal tratamento.
2. Exceptua-se da necessidade de consentimento do titular dos dados pessoais e da autorização prévia da ANPD as gravações de comunicação de serviços públicos destinados a prover situações de emergência de qualquer natureza, tais como:
 - a) serviços de atendimento médico de urgência;
 - b) operações de segurança pública ou defesa nacional;
 - c) serviços de resgate ou assistência em desastres naturais.
3. Os dados obtidos nessas gravações devem ser protegidos por medidas técnicas e organizativas adequadas para garantir sua segurança, evitando acessos não autorizados, uso indevido ou vazamento.
4. Os responsáveis pelo tratamento devem eliminar ou anonimizar os dados pessoais, atingida a finalidade para a qual foram colectados, salvo quando houver previsão legal para sua retenção.

5. O prazo máximo de conservação das gravações será definido pela ANDP.

ARTIGO 19

(Requisitos específicos para tratamento de dados pessoais para fins de interesse público)

O tratamento de dados pessoais para fins de interesse público deve respeitar o princípio da minimização dos dados e incluir a anonimização ou a pseudominização dos mesmos sempre que os visados possam ser abrangidos por uma destas vias.

ARTIGO 20

(Requisitos específicos para o tratamento de dados pessoais relativos a actividades ilícitas, crimes e contravenções)

1. O tratamento de dados pessoais relativos a pessoas suspeitas de actividades ilícitas, crimes e contravenções, bem como penas, medidas de segurança, multas e sanções acessórias aplicadas, os quais são considerados dados sensíveis, só pode ser efectuado por autoridade pública, verificadas as seguintes circunstâncias:

- a) disposição legal que permita tal tratamento por autoridades com competência específica, em respeito as normas procedimentais e de protecção de dados pessoais previstas por lei;
- b) autorização da ANPD, concedida quando tal tratamento for necessário à execução de finalidades legítimas do seu responsável e sejam observadas as normas de protecção de dados pessoais e de segurança pública.

2. Sem prejuízo do disposto em legislação específica, o tratamento de dados pessoais para fins de investigação criminal deve limitar-se ao necessário para o cumprimento de finalidades de prevenção geral e especial ou repressão de uma infracção determinada, nos termos da legislação específica e da presente Lei.

3. O armazenamento dos dados pessoais, para fins de investigação criminal é de um ano e a prorrogação deste prazo deve ser decretada pelo Tribunal.

ARTIGO 21

(Requisitos específicos para o tratamento de dados pessoais em sistemas de vídeo-vigilância e outros meios de controlo electrónico)

1. O tratamento de dados pessoais no âmbito da instalação de sistemas de vídeo-vigilância e outras formas de captação, tratamento e difusão de sons e imagens que permitam identificar pessoas, incluindo os sistemas de vigilância electrónica, está sujeita aos princípios constantes na presente Lei.
2. O responsável pelo tratamento de dados pessoais deve disponibilizar, nos locais com sistemas de vídeo-vigilância, informação relativa à existência dos mesmos.
3. As regras aplicáveis à instalação de sistemas de vídeo-vigilância e ao tratamento de dados pessoais recolhidos neste âmbito são objecto de regulamentação específica.
4. A presente lei não se aplica ao tratamento de dados pessoais em sistema de vídeo-vigilância para efeitos não comerciais e estritamente particular.

ARTIGO 22

(Dados pessoais de pessoas falecidas)

1. O direito de acesso, rectificação e eliminação dos dados pessoais das pessoas falecidas podem ser exercidos por quem a pessoa falecida tenha designado para o efeito ou, na sua falta, pelos respectivos herdeiros, salvo cumprimento de obrigação legal ou regulação sectorial.
2. O direito de acesso, rectificação e eliminação dos dados pessoais das pessoas falecidas podem ser exercidos, conforme o caso, por:
 - a) pessoa expressamente designada pelo titular em directiva póstuma formalizada em vida;
 - b) na falta de designação expressa, mediante prova documental da sua, salvo cumprimento de obrigação legal ou regulação sectorial específica.
 - c) na ausência de directiva póstuma ou de mandatário designado, e havendo divergência entre os herdeiros sobre o exercício do direito de eliminação, previsto neste artigo, o agente de tratamento deverá buscar a deliberação conjunta, prevalecendo a decisão da maioria, persistindo a divergência, o agente de tratamento pode exigir decisão judicial ou arbitral.
3. O titular pode, em vida, determinar instruções claras e específicas quanto ao destino de seus dados pessoais após a morte, com força vinculante para os agentes de tratamento, salvo exigência legal em contrário ou decisão judicial.

4. O tratamento de dados relativos a imagens, informações de saúde, dados genéticos, biométricos e demais categorias sensíveis de pessoas falecidas depende de autorização expressa dos legitimados previstos no número 1, salvo quando:
 - a) houver obrigação legal ou determinação judicial;
 - b) quando o tratamento for necessário para fins de saúde pública, investigação criminal, pesquisa histórica e científica autorizada, com garantias de anonimização ou pseudonimização sempre que possível e mediante aprovação de comitê de ética em pesquisa;
 - c) for indispensável à constituição de arquivo de interesse público, cultural ou científico, conforme regulamento da Autoridade Nacional de Protecção de Dados.
5. Os agentes de tratamento devem:
 - a) manter registro detalhado das solicitações recebidas relativas a dados de pessoas falecidas, incluindo a identificação dos solicitantes e a fundamentação das decisões;
 - b) notificar os legitimados sobre o tratamento de dados do falecido que possa afectar seus interesses;
 - c) adoptar medidas de segurança técnicas e organizacionais equivalentes às aplicáveis aos dados de pessoas vivas, especialmente quando a divulgação ou acesso indevido colocar em risco a dignidade, a memória póstuma ou terceiros.
6. Compete à ANDP regulamentar, de forma complementar, os procedimentos relativos:
 - a) prova documental da condição de herdeiro ou do interessado;
 - b) requisitos de forma e validade das directivas póstumas, incluindo a possibilidade de registro em plataformas digitais ou com notários;
 - c) memorialização e exclusão de contas digitais e outros activos digitais, considerando as especificidades de cada serviço;
 - d) critérios de autorização de uso de dados de pessoas falecidas para fins científicos, históricos e arquivísticos, garantindo a protecção da privacidade e da dignidade;
 - e) mecanismos de mediação e conciliação para resolução de conflitos entre herdeiros e agentes de tratamento.
7. O disposto no presente artigo não prejudica a aplicação das normas civis relativas a direitos de personalidade, sucessórios, direito autoral e protecção da honra e imagem, que deverão ser interpretadas em conjunto com as disposições da presente Lei para garantir a protecção integral dos direitos do falecido e de seus sucessores.
8. A ANPD deve dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no presente artigo, considerados a natureza das informações tratadas, as características

específicas do tratamento e o estado actual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no artigo 5 da presente Lei.

SECÇÃO II

Termo do tratamento de dados pessoais

ARTIGO 23

(Termo do tratamento de dados pessoais)

1. O termo do tratamento de dados pessoais ocorre nas seguintes hipóteses:
 - a) verificação de que a finalidade foi alcançada ou de que os dados pessoais deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
 - b) fim do período de tratamento;
 - c) comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto na presente Lei, resguardado o interesse público ou quando a lei complementar assim dispor de tempo de guarda maior, mesmo quando o titular solicitar a exclusão dos dados pessoais;
 - d) quando haja um interesse legítimo do controlador ou pendências contratuais;
 - e) determinação da ANPD, quando houver violação ao disposto da presente Lei.
2. Os dados pessoais são eliminados após o termo do seu tratamento, no âmbito e nos limites técnicos das actividades e é autorizada a conservação para as seguintes finalidades:
 - a) cumprimento de obrigação legal ou regulatória pelo controlador;
 - b) estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
 - c) transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na presente Lei;
 - d) uso exclusivo do controlador, vedado o seu acesso por terceiro, e desde que anonimizados os dados pessoais.
3. O armazenamento de dados pessoais deve ser feita de forma a permitir a identificação de seus titulares apenas durante o período necessário para a prossecução das finalidades para as quais são tratadas.

CAPÍTULO IV

Direitos do titular dos dados pessoais

ARTIGO 24
(Direito de Informação)

1. Sem prejuízo do disposto na legislação aplicável ao direito à informação, o responsável pelo tratamento de dados pessoais deve disponibilizar aos titulares dos dados pessoais, de forma clara e acessível, pelo menos as seguintes informações:
 - a) a identidade e endereço do responsável pelo tratamento dos dados e na falta destes o seu representante;
 - b) as finalidades do tratamento dos dados pessoais e a eventual criação de um ficheiro;
 - c) as categorias de dados pessoais sobre que incide;
 - d) com quais agentes de tratamento os dados pessoais são partilhados;
 - e) possíveis consequências de omissão de resposta;
 - f) as consequências da recolha de dados pessoais sem o consentimento do titular ou, em caso de incapacidade, pelo seu representante legal;
 - g) a existência ou não de tratamento de dados pessoais que lhe digam respeito;
 - h) as finalidades específicas do tratamento dos dados pessoais;
 - i) as categorias de dados pessoais objecto de tratamento;
 - j) os destinatários ou categorias de destinatários aos quais os dados pessoais são comunicados;
 - k) que os dados pessoais específicos são objecto de tratamento;
 - l) quaisquer informações disponíveis sobre a origem dos dados pessoais, quando estes não forem obtidos directamente do titular.
2. Quando os dados pessoais forem recolhidos directamente do titular, as informações relativas à finalidade do tratamento devem ser fornecidas no momento da recolha.
3. Nos casos em que os dados pessoais não forem recolhidos directamente do titular dos dados pessoais, o agente de tratamento deve fornecer as informações descritas no número 1, do presente artigo:
 - a) no momento do registo dos dados pessoais, ou;
 - b) o mais tardar no prazo de 15 (quinze) dias após a recolha, salvo se as informações já forem do conhecimento do titular.
4. A prestação de informações deve ser feita de maneira clara, precisa e objectiva, especialmente quando destinada a menores de idade ou pessoas com necessidades especiais.

ARTIGO 25
(Direito de Acesso)

1. O titular de dados pessoais tem o direito de obter do responsável pelo tratamento, livremente, sem restrições, demoras ou custos excessivos, informação sobre:
 - a) a confirmação de serem ou não tratados dados pessoais que lhe digam respeito;
 - b) as finalidades desse tratamento;
 - c) as categorias de dados pessoais sobre que incide;
 - d) os destinatários ou categorias de destinatários a quem são comunicados os dados pessoais.
2. O responsável pelo tratamento deve ainda, comunicar ao titular os dados específicos objecto de tratamento, bem como quaisquer informações disponíveis sobre a origem desses dados.
3. O direito de acesso aos dados pessoais pode ser limitado nas seguintes situações:
 - a) quando o tratamento de dados pessoais envolver a segurança do Estado;
 - b) durante a prevenção ou investigação criminal;
 - c) nos casos abrangidos pelo segredo de justiça;
 - d) quando os dados forem utilizados exclusivamente para fins de investigação científica;
 - e) quando não houver risco de violação dos direitos fundamentais do titular, especialmente quanto à privacidade e protecção da vida privada.
4. Nessas situações, o direito de acesso é exercido através da ANPD, que pode informar apenas as diligências realizadas.
5. O direito de acesso à informação relativa aos dados da saúde incluindo os dados genéticos, é exercido por intermédio do médico escolhido pelo titular dos dados.

ARTIGO 26
(Direito de oposição)

O titular dos dados pessoais tem o direito de oposição, salvo disposição legal em contrário, e pelo menos nas seguintes situações:

- a) se opor em qualquer altura a que os dados que lhe digam respeito sejam objecto de tratamento quando existam razões ponderosas e legítimas relacionadas com a sua situação particular, devendo neste caso o responsável excluir do tratamento tais dados;
- b) se opor ao tratamento dos seus dados em outras circunstâncias previstas na presente Lei e em outra legislação específica.

ARTIGO 27

(Direito de rectificação, actualização e eliminação)

1. Ao titular dos dados pessoais é assegurado o exercício dos direitos de rectificar, actualizar e eliminar os seus dados pessoais, quando os mesmos estiverem incompletos, inexactos, desactualizados ou utilizados de forma incompatível com a finalidade declarada.
2. Ao titular dos dados é assegurado o exercício de eliminação dos seus dados pessoais, após a finalidade para a qual é solicitada.
3. O responsável pelo tratamento de dados pessoais é obrigado a assegurar esses direitos no prazo máximo de vinte dias úteis, a contar da recepção formal do pedido apresentado pelo titular, nos termos previstos pela legislação aplicável.
4. Caso os dados sujeitos a rectificação, actualização ou eliminação tenham sido previamente partilhados ou comunicados a terceiros, o responsável pelo tratamento deve, no mesmo prazo, informar os agentes de tratamento sobre as alterações efectuadas.
5. Os agentes de tratamento têm o dever de proceder em conformidade com as orientações recebidas, garantindo a coerência e actualização dos seus registos.

ARTIGO 28

(Direito dos incapazes)

Quando os titulares dos dados pessoais forem incapazes, os direitos previstos em legislação específica e nos artigos anteriores são exercidos por intermédio de um dos pais ou representante legal.

ARTIGO 29

(Direitos do titular dos dados pessoais em casos especiais)

Os direitos de informação, de acesso, de rectificação, eliminação e de limitação do tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, detecção, investigação ou repressão de infracções penais ou de execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública são exercidos nos termos da legislação específica e da presente Lei.

ARTIGO 30

(Direito de portabilidade dos dados)

1. O titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir, se tratamento se basear no consentimento dado nos termos do artigo 14 da presente Lei.
2. No exercício do direito de portabilidade dos dados nos termos do número 1 do presente artigo, o titular dos dados tem o direito a que os dados pessoais sejam transmitidos directamente entre os responsáveis pelo tratamento, sempre que tal seja tecnicamente possível.
3. O exercício do direito de portabilidade não se aplica ao tratamento necessário para o exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento.
4. O direito de portabilidade não prejudica os direitos e as liberdades de terceiros.

CAPÍTULO V

Tratamento de dados pessoais pelas Instituições Públicas

ARTIGO 31
(Procedimentos)

O tratamento de dados pessoais pelas pessoas colectivas de direito público, deve ser realizado para o cumprimento da sua finalidade pública, na persecução do interesse público, com o objectivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

- a) sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e actualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas actividades;
- b) os prazos e procedimentos para exercício dos direitos do titular perante a instituição pública observam o disposto em legislação específica, em especial as disposições constantes na Lei do processo administrativo e na Lei do direito à informação;
- c) os dados devem ser mantidos em formato interoperável e estruturado para o uso partilhado, com vista à execução de políticas públicas, à prestação de serviços públicos, à descentralização da actividade pública e à disseminação e ao acesso das informações pelo público em geral;
- d) o uso partilhado de dados pessoais pela instituição pública deve atender a finalidade específica de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de protecção de dados pessoais elencados no artigo 5 da presente Lei;
- e) a instituição pública pode transferir para entidades privadas dados pessoais constantes na base de dados a que tenha acesso nos casos em que os dados forem acessíveis publicamente, ou em casos de cumprimento de política pública ou ainda sistemas interoperáveis, observadas as disposições da presente Lei;
- f) seja indicado um encarregado de dados pessoais quando realizarem operações de tratamento de dados pessoais, nos termos da presente Lei;
- g) as empresas públicas e as sociedades de economia mista que actuam em regime de concorrência, sujeitas ao disposto da Constituição da República de Moçambique, tem o mesmo tratamento dispensado às pessoas colectivas de direito privado, nos termos da presente Lei;

- h) a ANPD pode solicitar, a qualquer momento, aos órgãos e as entidades públicas a realização de operações de tratamento de dados pessoais, informações específicas sobre o âmbito e a natureza dos dados, e outros detalhes do tratamento realizado, e pode emitir parecer técnico complementar para garantir o cumprimento da presente Lei;
- i) a ANPD pode estabelecer normas complementares para as actividades de comunicação e de uso partilhada e dados pessoais.

ARTIGO 32

(Tratamento de dados pessoais sensíveis pelas Instituições Públicas)

1. A lei salvaguarda o tratamento de dados pessoais sobre a origem racial ou étnica, ascendência, as opiniões políticas, as convicções religiosas ou filosóficas, ou filiação a sindicato, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos a vida sexual ou orientação sexual.
2. O disposto no número 1 do presente artigo não se aplica aos seguintes casos:
 - a) o titular dos dados tiver dado o seu consentimento explícito para o tratamento desses dados pessoais para uma ou mais finalidades específicas;
 - b) o tratamento seja necessário para efeitos do cumprimento de obrigações de exercícios de direitos específicos do responsável pelo tratamento ou de titular de dados em matéria de legislação laboral, de segurança social e de protecção social ou ainda por uma convenção colectiva;
 - c) tratamento seja necessário para proteger os interesses vitais do titular dos dados ou de outra forma singular, no caso do titular dos dados estar física ou legalmente incapacitado de dar o seu consentimento;
 - d) o tratamento for realizado por motivo de interesse público com autorização da ANPD;
 - e) tratamento seja efectuado, no âmbito das suas actividades legítimas e mediante as garantias adequadas, por uma fundação, associação ou qualquer outro organismo sem fins políticos, filosóficos, religiosos ou sindicais, e desde que esse tratamento se refira exclusivamente aos membros ou antigos membros desse organismo ou a pessoas com os quais eles tenham mantido contactos regulares relacionados com os seus

objectivos, e que os dados pessoais não sejam divulgados a terceiros sem o consentimento dos seus titulares;

- f) o tratamento se referir a dados pessoais que tenham sido manifestamente tornados públicos pelo seu titular;
- g) o tratamento for necessário a declaração, ao exercício ou a defesa de um direito num processo judicial ou sempre que os tribunais actuem no exercício das suas funções jurisdicionais;
- h) o tratamento seja necessário por motivo de interesse público, que deve ser proporcional ao objectivo visado, respeitar a essência do direito à protecção de dados pessoais e prever medidas adequadas e específicas que salvaguardam os direitos fundamentais e os interesses do titular dos dados;
- i) o tratamento seja necessário para efeitos de medicina preventiva, para avaliação da capacidade de trabalho do funcionário, diagnóstico médico, prestação de cuidados ou tratamento de saúde, acção social, gestão de sistema e serviços de saúde ou por força de um contrato com um profissional de saúde;
- j) o processamento for necessário por motivo de interesse público, especialmente para fins históricos, artísticos, estatísticos, científicos, jornalísticos e de investigação;
- k) para a execução de uma missão no interesse público, realizada pelo responsável pelo tratamento ou por terceiros devidamente autorizados;
- l) o tratamento seja necessário por motivos de interesse público no domínio da saúde pública, tais como a protecção contra ameaças transfronteiriças graves para a saúde ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde, e dos medicamentos, dispositivos médicos que preveja medidas adequadas e específicas que salvaguardam os direitos e liberdade do titular dos dados, em particular o sigilo profissional.

3. Os dados pessoais referidos no número 1 do presente artigo podem ser tratados para os fins referidos no número 2, se forem tratados por ou sob a responsabilidade de um profissional sujeito a obrigação de sigilo profissional, nos termos de regulamentação estabelecida pelas autoridades nacionais competentes, ou por outra pessoa igualmente sujeita a uma obrigação de confidencialidade ou de regulamentação estabelecida pelas mesmas autoridades.

4. A ANPD pode manter ou impor novas condições, incluindo limitações, no que respeita ao tratamento de dados genéticos, dados biométricos ou dados relativos à saúde.

ARTIGO 33

(Tratamento de dados pessoais relacionados com condenações penais e infracções)

1. O tratamento de dados pessoais relacionados a condenações penais e infracções ou com medidas de segurança conexas com base no número 1 do artigo 20, só é efectuado sob o controle de uma autoridade pública.
2. Os registos completos das condenações só são conservados sob o controle das autoridades públicas.

ARTIGO 34

(Tratamento dos dados pessoais por subcontratante)

1. O responsável pelo tratamento dos dados pessoais pode recorrer a subcontratantes que apresentem garantias suficientes de adopção de medidas técnicas e organizativas adequadas de modo a que o tratamento satisfaça os requisitos estabelecidos na presente Lei e assegure a protecção dos direitos do titular dos dados pessoais.
2. O subcontratante não pode recorrer a outro subcontratante sem a autorização prévia específica ou geral, por escrito, do responsável pelo tratamento, com excepção dos casos em que a subcontratação constar nos contratos formais entre os agentes de tratamento.
3. Em caso de autorização geral, o subcontratante informa ao responsável pelo tratamento de dados pessoais sobre todas as alterações pretendidas quanto à contratação de outros subcontratantes, podendo o responsável pelo tratamento opor-se a essas alterações.
4. O tratamento de dados pessoais em subcontratação é regulado pela legislação específica ou contrato escrito que estabeleça o objecto, a duração, a natureza e a finalidade do tratamento, o tipo de dados pessoais e as categorias de titulares de dados a tratar, bem como as obrigações e os direitos do responsável pelo tratamento.
5. A Lei ou contrato referido no número anterior prevê, designadamente, que o subcontratante:
 - a) só proceda de acordo com as instruções do responsável pelo tratamento de dados pessoais;
 - b) assegure que as pessoas autorizadas a tratar os dados pessoais assumem um compromisso de confidencialidade ou se encontram sujeitas a obrigações legais de confidencialidade;
 - c) preste assistência ao responsável pelo tratamento por todos os meios adequados de modo a assegurar o cumprimento das disposições relativas aos direitos do titular dos dados;

- d) após concluir os serviços de tratamento, apague de forma definitiva ou devolva os dados ao responsável pelo tratamento, consoante a escolha deste, e apague as cópias existentes, a menos que a sua conservação seja exigida por lei;
- e) disponibilize ao responsável pelo tratamento as informações necessárias para demonstrar o cumprimento do disposto no presente artigo;
- f) respeite as condições referidas nos números 2 e 3 do presente artigo no que respeita à contratação de outro subcontratante;
- g) adopte as medidas técnicas e organizativas adequadas que assegurem a protecção dos dados pessoais, em conformidade com o exigido na presente Lei, devendo considerar o princípio da protecção de dados pessoais desde a concepção e por defeito.

ARTIGO 35

(Responsabilidade das entidades públicas)

1. Quando houver infracção à presente Lei em decorrência do tratamento de dados pessoais por órgãos públicos, a ANPD deve enviar a notificação formal com as medidas necessárias para cessar a violação.
2. A ANPD deve exigir a publicação de relatórios de impacto à protecção de dados pessoais.
3. A ANPD deve exigir adopção de padrões e boas práticas para o tratamento de dados pessoais pelas instituições públicas.

CAPÍTULO VI

Transferência Internacional de dados pessoais

ARTIGO 36

(Transferência Internacional de dados pessoais para países que asseguram um nível de protecção adequada)

1. A transferência internacional de dados pessoais somente é admissível para países, territórios ou organismos internacionais que comprovam, de forma objectiva e documental, a capacidade de assegurar o nível de protecção substancialmente equivalente ou superior ao previsto na presente Lei e nas normas complementares emitidas pela Autoridade Nacional de Protecção de Dados (ANPD).

2. A realização de tal transferência pode estar condicionada à notificação prévia e circunstanciada à ANPD, instruída com relatório técnico de impacto à protecção de dados pessoais, descrição detalhada das categorias de dados, finalidades e hipóteses de tratamento, identificação completa das partes envolvidas, medidas de segurança aplicadas, e política de eliminação dos dados transferidos quando atingido a finalidade.

3. Entende-se que um país, território ou organismo internacional assegura nível de protecção adequado quando demonstrar, de forma contínua e verificável, que adota princípios, direitos e garantias de protecção de dados pessoais compatíveis com os previstos na presente Lei, incluindo, no mínimo:

a) existência de autoridade de controle independente e dotada de poderes sancionatórios efectivos;

b) previsão legal de direitos equivalentes aos dos titulares previstos nesta Lei;

c) mecanismos administrativos e judiciais acessíveis para reparação de danos e exercício de direitos;

d) salvaguardas técnicas e organizacionais capazes de prevenir o tratamento ilícito, discriminatório ou desproporcional; e

e) instrumentos de cooperação internacional que permitam à ANPD a verificação e auditoria das práticas de tratamento.

4. A adequação reconhecida pode ser revista, suspensa ou revogada pela ANPD a qualquer momento, sempre que verificado o redução do nível de protecção, a inexistência de garantias efectivas ou o descumprimento das condições de notificação e salvaguarda.

5. Durante o período de reavaliação, e conseqüente redução do nível de adequação a ANPD deve notificar os controladores, para solicitarem a respectiva autorização sempre que aplicável, não sendo aplicável o regime da autorização a transferência deve ser suspensa.

6. Nenhum contrato, política interna ou instrumento internacional pode ser interpretado de forma a eximir o agente de tratamento de suas obrigações legais perante os titulares dos dados, nem limitar o exercício de competência fiscalizatória da ANPD.

7. O prazo para a transferência internacional de dados pessoais é matéria a regulamentar pela ANPD.

ARTIGO 37

(Transferência de dados pessoais para Países que não asseguram um nível de protecção adequada)

1. A transferência internacional de dados para um país que não assegure um nível de protecção adequado está sujeita a autorização da ANPD, a qual só pode ser concedida verificada uma das seguintes circunstâncias constantes de legislação específica:

- a) se o titular de dados tiver dado o seu consentimento inequívoco, expresso e escrito;
- b) se a transferência internacional de dados decorrer da aplicação de tratados ou acordos internacionais em que a República de Moçambique seja parte;
- c) se a transferência de dados tiver como finalidade exclusiva a resposta ou pedido de ajuda humanitária;
- d) se a transferência de dados for necessária para a execução de um contrato entre titulares de dados e o responsável pelo tratamento ou de diligências prévias à formação do contrato decididas a pedido titular dos dados;
- e) se a transferência dos dados for necessária para a execução ou celebração de um contrato do titular dos dados, entre o responsável pelo tratamento e um terceiro;
- f) se a transferência de dados for necessária ou legalmente exigida para a protecção de um interesse público ou para a declaração, o exercício ou a defesa de um direito num processo judicial;
- g) se a transferência de dados for necessária para proteger os interesses vitais do titular dos dados para a prevenção, diagnóstico ou tratamento médico, e o titular estiver física ou legalmente incapaz de dar o seu consentimento;
- h) se o destinatário dos dados assegurar contratualmente, perante o responsável pelo tratamento, o nível de protecção adequado aos dados pessoais transferidos.

2. Cabe à ANPD determinar as condições específicas que devem constar no contrato no número anterior;

3. No caso de transferência internacional de dados entre empresas do mesmo grupo empresarial, a garantia de cumprimento de um nível de protecção adequado pode ser alcançada através da adopção de regras internas relativas à privacidade e protecção de dados cujo cumprimento seja obrigatório.

CAPÍTULO VII

Atribuições e responsabilidades do Encarregado de protecção de dados pessoais

ARTIGO 38

(Encarregado de protecção de dados pessoais)

1. Todas as entidades públicas e privadas que actuam no território nacional devem indicar um Encarregado de protecção de dados pessoais.
2. A indicação do Encarregado de protecção de dados pessoais deve ser realizada por acto formal através de um documento escrito, datado e assinado, informando as formas de actuação e as actividades a serem desempenhadas.
3. O documento de indicação do Encarregado de protecção de dados pessoais deve ser apresentado a ANPD, quando solicitado.
4. Nas ausências, impedimentos e férias do encarregado de dados pessoais, um substituto deve ser formalmente designado.
5. As situações referidas no número 4 do presente artigo não podem ser obstáculo para o exercício dos direitos dos titulares ou para o atendimento às comunicações da ANPD.
6. O encarregado de dados pessoais deve ser capaz de comunicar-se com os titulares e com a ANPD, de forma clara e precisa e em língua portuguesa.
7. Cabe ao agente de tratamento estabelecer as qualificações profissionais necessárias para o desempenho das atribuições do encarregado, considerando seus conhecimentos sobre a legislação de protecção de dados pessoais.
8. O Encarregado de protecção de dados pessoais exerce suas funções com total autonomia técnica e operacional perante a entidade responsável, sem subordinação hierárquica no desempenho de suas atribuições, garantindo a imparcialidade na supervisão das actividades de tratamento de dados pessoais e na orientação sobre a conformidade com a legislação aplicável.
9. A identidade e as informações de contacto do encarregado devem estar actualizadas e serem divulgadas publicamente, de forma clara e objectiva, preferencialmente no sítio electrónico do controlador.
10. A divulgação da identidade do encarregado abrange, no mínimo:
 - a) o nome completo, se for pessoa singular;
 - b) no caso de pessoa colectiva, deve constar o nome completo da pessoa singular responsável.

11. O agente de tratamento que não possuir sítio electrónico deve realizar a divulgação da identidade e das informações de contacto do encarregado por quaisquer outros meios de comunicação disponíveis, especialmente aqueles geralmente são utilizados para contacto com os titulares.
12. O perfil do Encarregado de dados pessoais é matéria de regulamentação específica pela ANDP.

ARTIGO 39

(Obrigações do Agente de Tratamento com o Encarregado de protecção de dados pessoais)

1. O agente de tratamento deve:
 - a) proporcionar os meios necessários para o exercício das funções do encarregado, incluindo, entre outros, recursos humanos, técnicos e administrativos;
 - b) solicitar assistência e orientação do encarregado na realização de actividades e na tomada de decisões estratégicas relacionadas com o tratamento de dados pessoais;
 - c) garantir ao encarregado a autonomia técnica necessária para o desempenho das suas funções, livre de interferências indevidas, especialmente no que diz respeito à orientação sobre as práticas a serem adoptadas em relação à protecção de dados pessoais;
 - d) assegurar aos titulares meios céleres, eficazes e adequados para viabilizar a comunicação com o encarregado e o exercício dos seus direitos;
 - e) garantir ao encarregado acesso directo às pessoas de maior nível hierárquico dentro da organização, aos responsáveis pela tomada de decisões estratégicas que afectem ou envolvam o tratamento de dados pessoais, bem como às demais áreas da organização.

ARTIGO 40

(Encarregados de Protecção de dados pessoais em Entidades Públicas)

1. É obrigatório a indicação de encarregados de protecção de dados pessoais nas entidades públicas, de acordo com o disposto nos números seguintes.
2. Para efeitos do número anterior, entende-se por entidades públicas:
 - a) os órgãos de soberania;
 - b) instituições públicas;
 - c) as autarquias locais;
 - d) o Banco de Moçambique;
 - e) as instituições de ensino superior públicas, independentemente da sua natureza;
 - f) as empresas do sector empresarial do estado;
 - g) as associações públicas.
3. Independentemente de quem seja responsável pelo tratamento, existe pelo menos um encarregado de protecção de dados pessoais:
 - a) por cada Ministério ou área governativa, no caso do Estado, sendo indicado pelo respectivo Ministro;
 - b) por cada autarquia, sendo indicado pelo Presidente do Conselho Autárquico.
4. A indicação deve ser publicada no Boletim da República.

ARTIGO 41

(Funções e Obrigações do Encarregado de protecção de dados pessoais em Entidades Públicas)

1. São funções do Encarregado de protecção de dados pessoais:
 - a) registar e comunicar incidentes de segurança à autoridade competente;
 - b) apoiar o agente de tratamento no registo das operações de tratamento de dados pessoais;
 - c) auxiliar o agente de tratamento na elaboração de relatórios de impacto à protecção de dados pessoais, obrigatórios para operações de alto risco;
 - d) implementar mecanismos internos de supervisão e mitigação de riscos relacionados ao tratamento de dados pessoais;
 - e) auxiliar o agente de tratamento, quando necessário, na criação e publicação da política de privacidade interna e externa bem como nas demais políticas que forem necessárias para atender as demandas do agente de tratamento;

- f) auxiliar o agente de tratamento na correção dos instrumentos contratuais que disciplinem questões relacionadas ao tratamento de dados pessoais;
- g) sensibilizar os utilizadores para a importância e prevenção de possíveis incidentes de segurança e para a necessidade de informar imediatamente ao responsável;
- h) assegurar as relações com os titulares dos dados nas matérias abrangidas pela legislação nacional em matéria de protecção de dados pessoais;
- i) aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adoptar providências cabíveis;
- j) receber comunicações da ANPD e adoptar providências;
- k) orientar aos funcionários e colaboradores a respeito das práticas a serem tomadas em relação à protecção de dados pessoais;
- l) auxiliar o agente de tratamento a criar o registo das operações de actividades com dados pessoais quando necessário, conforme exigido pela legislação;
- m) auxiliar na implementação de mecanismos internos de supervisão e mitigação de riscos relacionados ao tratamento de dados pessoais, para que as medidas adequadas sejam adoptadas com a finalidade de prevenir incidentes de segurança;
- n) colaborar com a entidade na definição de estratégias e decisões referentes ao tratamento de dados pessoais, garantindo que todos os aspectos do tratamento estejam em conformidade com as normas de protecção de dados pessoais;
- o) fornecer treinamentos e orientações aos funcionários e colaboradores do agente de tratamento sobre as práticas adequadas em relação à protecção de dados pessoais, promovendo o cumprimento das políticas de privacidade e segurança;
- p) ao receber comunicações da ANPD, deve junto com o agente de tratamento seguir com a resposta solicitada, com todas as provas assim que solicitado pela Autoridade;
- q) fornecer a orientação e a assistência necessárias ao agente de tratamento;
- r) executar as demais atribuições determinadas pelo controlador.

2. O agente de tratamento deve:

- a) proporcionar os meios necessários para o exercício das funções do encarregado, incluindo, entre outros, recursos humanos, técnicos e administrativos;
- b) solicitar assistência e orientação do encarregado na realização de actividades e na tomada de decisões estratégicas relacionadas com o tratamento de dados pessoais;
- c) garantir ao encarregado a autonomia técnica necessária para o desempenho das suas funções, livre de interferências indevidas, especialmente no que diz respeito à

orientação sobre as práticas a serem adoptadas em relação à protecção de dados pessoais;

- d) assegurar aos titulares meios céleres, eficazes e adequados para viabilizar a comunicação com o encarregado e o exercício dos seus direitos;
- e) garantir ao encarregado acesso directo às pessoas de maior nível hierárquico dentro da organização, aos responsáveis pela tomada de decisões estratégicas que afectem ou envolvam o tratamento de dados pessoais, bem como às demais áreas da organização.

CAPÍTULO VIII

Responsabilidade e Ressarcimento de Danos

ARTIGO 42

(Responsabilidade dos Agentes de tratamento de dados pessoais)

1. O agente de tratamento que no exercício de actividades de tratamento de dados pessoais, causar dano patrimonial, moral, individual ou colectivo ao titular de dados e a terceiros em violação à legislação de protecção de dados pessoais, comete uma contravenção muito grave.
2. O operador ou sub-operador é responsável solidariamente pelos danos causados pelo tratamento de dados pessoais nas seguintes hipóteses:
 - a) incumprimento das obrigações estabelecidas na legislação de protecção de dados pessoais;
 - b) não observância das instruções lícitas do controlador, equiparando-se ao controlador nestes casos.
3. Os controladores conjuntos, directamente envolvidos no tratamento que causou dano ao titular dos dados, respondem solidariamente.
4. O juiz, no processo judicial, pode inverter o ônus da prova a favor do titular dos dados quando:
 - a) a alegação for verdadeira do titular;
 - b) o titular apresentar insuficiência de meios para produzir prova; ou
 - c) a produção de prova for excessivamente onerosa ao titular.
5. As acções de reparação por danos colectivos decorrentes do tratamento de dados pessoais podem ser exercidas colectivamente em juízo, observando-se a legislação aplicável.

6. Aquele que reparar o dano ao titular dos dados pessoais pode exercer direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.
7. Os agentes de tratamento (controlador, controlador conjunto, operador e sub-operador) não são responsabilizados se comprovarem:
 - a) não terem realizado o tratamento de dados que lhes foi atribuído;
 - b) que o tratamento realizado estava em conformidade com a legislação de protecção de dados pessoais;
 - c) que o dano foi causado exclusivamente por culpa do titular dos dados ou de terceiros.
8. O tratamento de dados pessoais é considerado irregular se:
 - a) não observar a legislação de protecção de dados pessoais;
 - b) não fornecer a segurança esperada pelo titular, considerando:
 - i. o modo como o tratamento foi realizado;
 - ii. os riscos e resultados esperados;
 - iii. as medidas técnicas necessárias para a protecção dos dados pessoais.
9. O agente de tratamento de dados pessoais é responsabilizado, quando deixar de adoptar as medidas de segurança previstas na presente Lei e causar danos por violação da segurança dos dados pessoais.
10. As hipóteses de violação de direitos dos titulares no âmbito das relações de consumo continuam sujeitas às regras de responsabilidade previstas na legislação específica.

CAPÍTULO IX

Segurança e boas práticas

SECÇÃO I

Segurança e sigilo de dados pessoais

ARTIGO 43

(Medidas de segurança)

1. Os agentes de tratamento de dados pessoais devem adoptar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

2. A ANPD deve dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no presente artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado actual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no artigo 5 da presente Lei.
3. As medidas a que se refere o presente artigo devem ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.
4. Os agentes de tratamento de dados pessoais ou qualquer outra pessoa que intervenha em uma das fases do tratamento obrigam-se a garantir a segurança da informação prevista na presente Lei em relação aos dados pessoais, mesmo após o seu término.
5. O controlador deve comunicar a ANPD e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
6. A comunicação é feita 5 dias, após ter conhecimento da situação, e deve mencionar no mínimo:
 - a) a descrição da natureza dos dados pessoais afectados;
 - b) as informações sobre os titulares envolvidos;
 - c) a indicação das medidas técnicas e de segurança utilizadas para a protecção dos dados pessoais, observados os segredos comercial e industrial;
 - d) os riscos relacionados ao incidente;
 - e) os motivos da demora, no caso de a comunicação não ter sido imediata;
 - f) as medidas que foram ou que são adoptadas para reverter ou mitigar os efeitos do prejuízo;
 - g) o nome e os contactos do Encarregado de protecção de dados pessoais ou de outro ponto de contacto, para efeitos de prestação de informações adicionais.
7. A ANPD verifica a gravidade do incidente e pode, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao agente de tratamento a adopção de providências, tais como, a ampla divulgação do facto em meios de comunicação e medidas para reverter ou mitigar os efeitos do incidente.
8. No juízo de gravidade do incidente, é avaliada eventual confirmação de que foram adoptadas medidas técnicas adequadas que tornem os dados pessoais afectados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.
9. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governação e aos princípios gerais previstos na presente Lei e às demais normas regulamentares.

ARTIGO 44

(Prazos de conservação de dados pessoais)

1. Quando cessa a finalidade que motivou o tratamento, inicial ou posterior, de dados pessoais, o responsável pelo tratamento deve proceder à sua destruição ou anonimização.
2. Quando, pela natureza e finalidade do tratamento, designadamente para fins de arquivo de interesse público, fins de investigação científica ou histórica ou fins estatísticos, não seja possível determinar antecipadamente o momento em que a mesma deixa de ser necessário, é lícita a conservação dos dados pessoais, desde que sejam adoptadas medidas técnicas e organizativas adequadas a garantir os direitos do titular dos dados.
3. Quando os dados pessoais sejam necessários para o responsável pelo tratamento, ou o subcontratante, confirmar o cumprimento de obrigações contratuais ou de outra natureza, os mesmos podem ser conservados enquanto não decorrer o prazo de prescrição dos direitos respectivos.
4. Nos casos em que existe um prazo de conservação de dados imposto por lei, só pode ser exercido o direito a eliminação prevista no artigo 27 da presente Lei findo esse prazo.
5. Os dados relativos a declarações contributivas para efeitos de aposentação ou reforma podem ser conservados sem limite de prazo, a fim de auxiliar o titular na reconstituição das carreiras contributivas, desde que sejam adoptadas medidas técnicas e organizativas adequadas a garantir os direitos do titular dos dados.

SECÇÃO II

Boas práticas e governação

ARTIGO 45

(Boas práticas no tratamento de dados pessoais)

1. O agente de tratamento, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, devem formular regras de boas práticas e de governação que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as acções educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

2. Ao estabelecer regras de boas práticas, o agente de tratamento leva em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade, a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.
3. Na aplicação dos princípios indicados no artigo 5 da presente Lei, o agente de tratamento, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados, a probabilidade e a gravidade dos danos para os titulares dos dados, deve implementar um programa de governação em privacidade que, no mínimo:
 - a) demonstre o comprometimento do agente de tratamento em adoptar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à protecção de dados pessoais;
 - b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua colecta;
 - c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
 - d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
 - e) tenha o objectivo de estabelecer relação de confiança com o titular, por meio de actuação transparente e que assegure mecanismos de participação do titular;
 - f) esteja integrado à sua estrutura geral de governação, estabeleça e aplique mecanismos de supervisão interna e externa;
 - g) conte com planos de resposta a incidentes e mitigação;
 - h) seja actualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;
 - i) demonstre a efectividade de seu programa de governação em privacidade quando apropriado e, em especial, a pedido da ANPD ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.
4. As regras de boas práticas e de governação devem ser publicadas e actualizadas periodicamente, reconhecidas e divulgadas pela ANPD.
5. A ANPD estimula a adopção de padrões técnicos que facilitem o controlo pelos titulares dos seus dados pessoais.

ARTIGO 46

(Avaliação Prévia de Impacto)

1. Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidade, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento e de notificá-lo à ANPD, a uma avaliação de impacto das operações de tratamento previstas sobre a protecção de dados pessoais.
2. A ANPD deve determinar ao controlador que elabore o Relatório de Avaliação prévia de impacto, referente as suas operações de tratamento de dados pessoais que podem gerar alto risco à garantia dos princípios gerais de protecção de dados pessoais, às liberdades civis e aos direitos fundamentais, observados os segredos comercial e industrial.
3. As directrizes para a realização de Avaliação Prévia de Impacto sobre a protecção de dados esta sujeita a regulamentação específica.

ARTIGO 47

(Dever de Colaboração)

1. As entidades públicas e privadas devem colaborar com a ANPD, fornecendo todas as informações solicitadas pela ANPD no exercício das suas competências e atribuições.
2. O dever de colaboração inclui a obrigação de cooperar com a ANPD no acesso aos sistemas informáticos, ficheiros de dados pessoais e toda a documentação relacionada com o tratamento e transmissão de dados pessoais, quando necessário para o cumprimento das suas funções.
3. Os membros da ANPD, bem como os seus trabalhadores, prestadores de serviços ou quaisquer pessoas por ela mandatadas, estão sujeitos a um dever de sigilo profissional em relação aos dados pessoais, segredos profissionais, industriais ou comerciais, e informações confidenciais a que tenham acesso no exercício das suas funções e o dever de sigilo permanece válido mesmo após o término de suas funções.
4. O dever de colaboração e os poderes de fiscalização da ANPD não prejudicam os deveres de segredo legalmente impostos ao responsável pelo tratamento, conforme previsto na presente Lei ou em normas internacionais aplicáveis.

CAPÍTULO X

Notificação de violação de dados pessoais

ARTIGO 48

(Notificações de Violação de dados pessoais à ANDP)

1. Constatada a violação de dados pessoais, o responsável pelo tratamento, deve notificar a autoridade de controlo no prazo de 72 horas, após ter conhecimento da situação, a menos que a violação não seja susceptível de resultar risco para os direitos, liberdades e garantias dos titulares de dados.
2. Nos casos em que não seja possível efectuar a notificação no prazo estabelecido no número 1 do presente artigo, o responsável pelo tratamento deve indicar os motivos do atraso.
3. A notificação a que se refere o número 1 do presente artigo é confidencial e deve, no mínimo, apresentar os requisitos descritos no número 6 do artigo 43.
4. Nos casos em que não seja possível notificar ANPD com as informações referidas no número 3 do presente artigo, elas devem ser fornecidas posteriormente à notificação no prazo de 20 (vinte) dias.
5. O responsável pelo tratamento deve documentar a violação de dados pessoais, incluindo os factos com ela relacionados, os seus efeitos e as medidas de reparação adoptadas, de modo a permitir à ANDP que verifique o cumprimento do disposto no presente artigo.
6. Caso a violação envolva dados pessoais que tenham sido transmitidos para outro Estado, as informações referidas no número 6 do artigo 43 da presente Lei, são-lhe comunicadas, de imediato.
7. Nos casos de subcontratação, o subcontratante notifica o responsável pelo tratamento de qualquer violação de dados pessoais de que tenha conhecimento.
8. Considera-se que o controlador tomou conhecimento do incidente quando este for notificado pelo subcontratante.
9. O conteúdo da notificação esta sujeita a regulamentação específica.

CAPÍTULO XI

Tutela Administrativa e Jurisdicional

ARTIGO 49

(Tutela Administrativa)

Sem prejuízo do Direito de apresentação de queixa à ANPD, qualquer pessoa pode, nos termos da presente Lei, recorrer a meios administrativos para garantir o cumprimento das disposições legais e regulamentares em matéria de protecção de dados pessoais.

ARTIGO 50

(Tutela Jurisdicional)

1. Qualquer pessoa pode nos termos da presente Lei, recorrer judicialmente da violação dos seus direitos.
2. As acções propostas contra ANPD são da competência dos Tribunais Administrativos.
3. O titular de dados pode propor acções contra o responsável pelo tratamento ou o subcontratante, incluindo acções de responsabilidade civil.
4. As acções intentadas contra o responsável pelo tratamento ou um subcontratante são propostas nos tribunais nacionais se o responsável ou subcontratante tiver o estabelecimento em território nacional ou se o titular dos dados residir habitualmente em território nacional.

CAPÍTULO XII

Sanções Administrativas

ARTIGO 51

(Tipos de Sanções Administrativas)

1. Os agentes de tratamento de dados, em razão das infracções cometidas às normas previstas na presente Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela ANPD:
 - a) advertência, com indicação de prazo para adopção de medidas correctivas;
 - b) multa;
 - c) bloqueio dos dados pessoais a que se refere a infracção até a sua regularização;
 - d) eliminação dos dados pessoais a que se refere a infracção;
 - e) suspensão parcial do funcionamento da base de dados;
 - f) suspensão do exercício da actividade de tratamento dos dados pessoais;
 - g) proibição parcial ou total do exercício de actividades relacionadas a tratamento de dados.

2. As sanções são aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradual, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:
- a) a gravidade e a natureza das infrações e dos direitos pessoais afectados;
 - b) a boa-fé do infractor;
 - c) a vantagem auferida ou pretendida pelo infractor;
 - d) a condição económica do infractor;
 - e) a reincidência;
 - f) o grau do dano;
 - g) a cooperação do infractor;
 - h) a adopção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto na presente Lei;
 - i) a adopção de política de boas práticas e governação;
 - j) a pronta adopção de medidas correctivas;
 - k) a proporcionalidade entre a gravidade da falta e a intensidade da sanção.
3. O disposto neste artigo não substitui a aplicação de sanções civis ou penais definidas em legislação específica.
4. No cálculo do valor da multa de que trata a alínea b), número 1 do presente artigo, a ANPD pode considerar a facturação total da empresa ou grupo de empresas, quando não dispuserem do valor da facturação no ramo de actividade empresarial em que ocorreu a infracção, definido pela ANPD, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea.
5. Os vazamentos individuais ou os acessos não autorizados de que trata o artigo 48, podem ser objecto de conciliação directa entre o agente de tratamento e titular, e caso não haja acordo, o agente de tratamento está sujeito à aplicação das penalidades definidas na alínea b) do articulado 1, do presente artigo.
6. O valor das multas, referidos no presente artigo, esta sujeita a regulamentação específica.

CAPÍTULO XIII

Anonimização de dados

ARTIGO 52

(Dados anonimizados)

1. Os dados anonimizados não são considerados dados pessoais para os efeitos da presente Lei.
2. A ANPD deve regulamentar as técnicas e padrões utilizados no processo de anonimização e realizar verificações quanto à segurança desses processos.

CAPÍTULO XIV

Registo Cronológico e Registo das Actividades de Tratamento

ARTIGO 53

(Registo Cronológico e Registo de Actividades de Tratamento)

1. O agente de tratamento deve conservar registos cronológicos das seguintes operações de tratamento:
 - a) recolha;
 - b) alteração;
 - c) consulta;
 - d) divulgação, incluindo transferências;
 - e) interconexão;
 - f) eliminação;
 - g) limitação do tratamento, incluindo as datas de início e de cessação da limitação.
2. Os registos cronológicos das operações de consulta e de divulgação devem permitir determinar o motivo, a data e a hora dessas operações, a identificação da pessoa que consultou ou divulgou dados pessoais e, sempre que possível, a identidade dos destinatários desses dados.
3. Os registos cronológicos são utilizados exclusivamente para efeitos de verificação da licitude do tratamento, autocontrolo, exercício do poder disciplinar e garantia da integridade e segurança dos dados pessoais, bem como no âmbito e para efeitos de processo penal.
4. O agente de tratamento disponibiliza os registos cronológicos à ANPD, a pedido desta.
5. O agente de tratamento deve adoptar medidas técnicas e administrativas que garantam a integridade dos registos cronológicos.

ARTIGO 54

(Registo das actividades de tratamento)

1. Todo o agente de tratamento deve manter um registo de todas as actividades de tratamento de dados pessoais sob a sua responsabilidade.
2. Os elementos de registo das actividades de tratamento é sujeita a regulamentação específica.

ARTIGO 55

(Acreditação e certificação)

1. A autoridade competente para a acreditação dos organismos de certificação em matéria de protecção de dados pessoais é ANPD.
2. A certificação, bem como a emissão de selos e marcas de protecção de dados pessoais, é efectuada por organismos de certificação acreditados nos termos do número 1 do presente artigo, destinando-se a atestar que os procedimentos implementados cumprem o disposto na presente Lei.

CAPÍTULO XV

Disposições Finais e Transitórias

ARTIGO 56

(Regime subsidiário)

É aplicável subsidiariamente a presente Lei, em tudo que se mostra omissa, o regime jurídico aplicável as transacções em meios físico e informático e demais legislação complementar.

ARTIGO 57

(Regulamentação)

Compete ao Governo Regular a presente Lei no prazo de 90 dias a contar da data da sua publicação no Boletim da República.

ARTIGO 58

(Entrada em vigor)

A presente Lei entra em vigor 180 dias após a sua publicação.

Aprovada pela Assembleia da República, aos..... de de 2025

A Presidente da Assembleia da República, *Margarida Adamugi Talapa*.

Promulgada aos de de 2025

Publique-se.

O Presidente da República, *Daniel Francisco Chapo*.

Anexo:

A

Agentes de Processamento - todos os agentes envolvidos na cadeia de tratamento de dados pessoais, incluindo, mas não se limitando a: controlador, co-controlador, operador e sub-operador, bem como quaisquer outros intervenientes que, directa ou indirectamente, realizem actividades de tratamento de dados pessoais, nos termos da presente Lei. Esta definição não inclui os indivíduos que, agindo sob a autoridade ou em nome de um agente de tratamento, realizem tarefas de tratamento de dados.

Avaliação Prévia de Impacto - documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar alto risco à garantia dos princípios gerais de protecção de dados pessoais, às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Anonimização de dados - um processo técnico, realizado por meios razoáveis disponíveis no momento do tratamento, que remove ou modifica elementos de identificação de um conjunto de dados pessoais, de modo a que a pessoa singular a que se referem não possa ser identificada, directa ou indirectamente, por qualquer agente, considerando a utilização combinada de outros dados e meios técnicos razoavelmente acessíveis e disponíveis no momento do tratamento.

B

Base de dados - conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte electrónico ou físico.

Bloqueio - suspensão temporária de qualquer operação de tratamento de dados pessoais, mediante guarda do dado pessoal ou da base de dados.

C

Consentimento do titular dos dados - qualquer manifestação de vontade, livre, específica e informada, nos termos da qual o titular aceita, mediante declaração ou acto positivo inequívoco, que os seus dados pessoais sejam objecto de tratamento.

Controlador - pessoa singular ou colectiva, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

Controlador Conjunto - quando dois ou mais controladores decidem, conjuntamente, sobre o tratamento de dados pessoais.

D

Dado Pessoal Sensível - dado pessoal sobre origem racial ou étnica, ascendência, convicção religiosa, opinião política, filiação a sindicato ou a organização de carácter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, situação económica ou condição social do titular dos dados.

Dados anonimizados - dados relativos a um titular que não possa ser identificado, directa ou indirectamente, considerando a utilização de meios técnicos razoáveis disponíveis no momento do tratamento, de forma a tornar o processo de anonimização irreversível.

Dados biométricos - dados pessoais resultantes de um tratamento técnico específico, relativos às características físicas, fisiológicas ou comportamentais de uma pessoa singular, que permitam ou confirmem a sua identificação única, tais como imagens faciais ou dados dactiloscópicos.

Dados genéticos - dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular, que forneçam informações únicas sobre a sua fisiologia ou sobre a sua saúde que resultem, designadamente, da análise de uma amostra biológica da pessoa singular em causa.

Dados relativos à saúde - dados pessoais relativos à saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde.

Destinatário – uma pessoa singular ou colectiva, uma autoridade pública, uma agência ou outro organismo ao qual os dados pessoais são divulgados, seja um terceiro ou não.

E

Encarregado de protecção de dados pessoais - é pessoa singular, colectiva ou comissão designada pelo agente de tratamento para actuar, de forma independente, como canal de comunicação entre o responsável pelo tratamento e/ou o operador, os titulares dos dados e a Autoridade Nacional de Protecção de Dados (ANPD). O responsável, seja ele pessoa singular ou colectiva, deverá exercer as suas funções sem receber instruções quanto ao desempenho das suas atribuições, preservando a imparcialidade e a autonomia necessárias ao cumprimento das suas responsabilidades, nos termos da lei.

Eliminação - eliminação de um dado pessoal ou de um conjunto de dados pessoais armazenados numa base de dados, independentemente do procedimento utilizado.

O

Operador - pessoa singular ou colectiva, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

P

Processador – uma pessoa singular ou colectiva, de direito público ou privado, que trata os dados pessoais por conta do responsável pelo tratamento.

Processamento de Dados Pessoal - qualquer operação ou conjunto de operações efectuadas sobre os dados pessoais, que através de meios automáticos ou não, tais como recolha, registo, organização, armazenamento, adaptação, alteração, recuperação, suporte, cópia, consulta, utilização, divulgação, ou qualquer outra forma de distribuição, ou doutro modo, fazendo disponibilização, alinhamento ou combinação e bloqueio, encriptação, supressão ou destruição de dados pessoais.

Protecção de dados pessoais - o conjunto de medidas técnicas e administrativas, normas e procedimentos que visam a segurança dos dados pessoais e a privacidade das pessoas singulares.

Pseudominização - o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular dos dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular ou identificável.

R

Relatório de Avaliação de Impacto na Protecção de Dados - é a documentação elaborada pelo responsável pelo tratamento que descreve detalhadamente um processo de tratamento de dados pessoais que possa gerar um elevado risco para as liberdades civis e para os direitos fundamentais dos titulares dos dados. O relatório deve conter, no mínimo, a descrição dos processos de tratamento, a análise da sua necessidade e conformidade, a identificação dos riscos e as medidas, salvaguardas e mecanismos a adotar para os mitigar.

Responsável pelos Dados - qualquer pessoa singular ou colectiva, pública ou privada, qualquer outra organização ou associação que sozinha ou em conjunto com outras pessoas decida recolher e processar dados pessoais e determinar a sua finalidade.

S

Sub Operador - pessoa singular ou colectiva, de direito público ou privado, contratada pelo operador para auxiliar a realizar o tratamento de dados pessoais em nome do controlador.

Sub- processador - uma pessoa singular ou colectiva de direito público ou privado, contratada pelo subcontratante para auxiliar no tratamento de dados pessoais em nome do responsável pelo tratamento.

T

Tratamento de Dados - operação efectuada com dados pessoais, com ou sem meios automatizados, como as que se referem a colecta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extracção.

Transferência Internacional de Dados - partilha de dados pessoais para país estrangeiro ou organismo internacional.

Titular - pessoa singular a quem se referem os dados pessoais que são objecto de tratamento.

U

Uso partilhado de dados - comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento partilhado de bases de dados pessoais por órgãos e entidades públicas no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

V

Violação de dados pessoais - uma violação de segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.