Lei da Proteção de Dados Pessoais

Personal Data Protection Law

PORTUGUÊS | ENGLISH

DALAN
DIGITAL
A NEW PATH FOR
DIGITAL CITIZENSHIP

REPÚBLICA DEMOCRÁTICA DE TIMOR-LESTE
UNIDADE ACÇÃO PROGRESSO
RDTL

UNDP

Lei da Proteção de Dados Pessoais

PORTUGUÊS

DALAN DIGITAL
A NEW PATH FOR DIGITAL CITIZENSHIP

REPÚBLICA DEMOCRÁTICA DE TIMOR-LESTE
UNIDADE ACÇÃO PROGRESSO
RDTL

UNDP

REPÚBLICA DEMOCRÁTICA DE TIMOR-LESTE

PROPOSTA DE LEI

N.º _____ /_____

LEI DA PROTEÇÃO DE DADOS PESSOAIS

EXPOSIÇÃO DE MOTIVOS

A Lei Fundamental, que entrou em vigor em 20 de maio de 2002, proclama a República Democrática de Timor-Leste como um Estado de Direito democrático, que se baseia na vontade popular e no respeito pela dignidade da pessoa humana. No catálogo dos direitos fundamentais previsto na Constituição, o artigo 38.º estabelece, em linhas gerais, o direito à proteção de dados pessoais, deixando ao legislador ordinário a definição do respetivo conceito, bem como das condições aplicáveis ao seu tratamento.

Todavia, passados mais de 20 anos desde a aprovação da Constituição, falta ainda aprovar um adequado e eficaz regime de proteção dos dados pessoais, ajustável à realidade do país, sendo essa uma necessidade por demais evidente e sentida por todos.

A presente iniciativa legislativa pretende estabelecer o enquadramento normativo geral da proteção de dados pessoais. Esta Lei da Proteção de Dados Pessoais foi concebida para garantir a proteção das liberdades e dos direitos fundamentais das pessoas singulares, sem prejuízo do concomitante reconhecimento do interesse nacional em possibilitar a utilização adequada e eficaz dessa informação para a criação de novas oportunidades económicas, a prestação de serviços públicos mais eficientes, o incremento da participação de Timor-Leste na economia global e a melhoria da qualidade de vida do Povo Timorense.

A presente Proposta de Lei corporiza os princípios fundamentais internacionalmente acolhidos sobre proteção de dados, cujas raízes assentam em convenções multilaterais, regimes normativos e melhores práticas reconhecidas, que foram, entretanto, integrados nos instrumentos legislativos e regulamentares de vários ordenamentos jurídicos, incluindo os de países lusófonos com os quais Timor-Leste tem maior proximidade.

Considerando que algumas das medidas, cuja adoção se afigura como necessária, integram reserva de competência do Parlamento Nacional, nomeadamente atento o disposto na alínea e) do n.º 2 do artigo 95.º, da Constituição da República Democrática de Timor-Leste, o Governo apresenta ao Parlamento Nacional a presente Proposta de Lei.

Nos termos ora propostos, o tratamento de dados pessoais ao qual se aplique a Lei da Proteção de Dados Pessoais deve ser realizado no estrito respeito pelos direitos de personalidade das pessoas singulares, com observância das regras da boa fé, e sujeito às seguintes linhas mestras:

1. (Finalidade) - O tratamento deve ser realizado com finalidades lícitas, legítimas, específicas e explícitas, atempadamente comunicadas ao titular dos dados, sem lugar a tratamento subsequente que seja incompatível com as mesmas;
2. (Necessidade, adequação e proporcionalidade) - O tratamento deve ser limitado, na medida do necessário, adequado e proporcional para cumprir as respetivas finalidades, e incluir apenas os dados que sejam relevantes, proporcionais e não excessivos em relação às finalidades do tratamento;
3. (Informação livre) - Os titulares dos dados têm o direito de obter uma confirmação por parte do responsável pelo tratamento sobre se os seus dados são (ou não) objeto de tratamento, bem como informação relativa às categorias de dados submetidos a tratamento e às finalidades do tratamento;
4. (Qualidade e exatidão dos dados) - Tendo em consideração a finalidade do tratamento, os responsáveis pelo tratamento e os subcontratados devem tomar medidas adequadas para garantir que os dados pessoais são exatos, incluindo a sua atualização, se necessário;
5. (Transparência) - Os titulares dos dados têm o direito de receber informação, num formato inteligível, sobre o tratamento e a identidade dos respetivos responsáveis pelo tratamento e subcontratados, e tal informação deve ser prestada num formato que seja compatível com a forma regular de interação com o titular dos dados, sem prejuízo de eventuais restrições necessárias para salvaguardar segredos comerciais e industriais;

6. (Segurança) - Os responsáveis pelo tratamento e os subcontratados devem tomar medidas técnicas e organizativas para proteger os dados pessoais contra acessos não autorizados, bem como contra a sua destruição, perda, alteração, comunicação ou disseminação acidental ou ilegítima;
7. (Não discriminação) - Os dados pessoais não podem ser submetidos a tratamento com uma finalidade que seja ilegítima, abusiva ou discriminatória;
8. (Responsabilidade) - Os responsáveis pelo tratamento e os subcontratados devem adotar medidas técnicas e organizativas com vista ao cumprimento das regras de proteção de dados pessoais e serão responsabilizados em caso de incumprimento;
9. (Privacidade e Segurança Desde a Conceção) - Os responsáveis pelo tratamento e os subcontratados devem cumprir as disposições do artigo 11.º da presente lei e quaisquer outros requisitos de segurança aplicáveis, desde a fase de conceção e desenvolvimento de um qualquer produto ou serviço.

Considerando a necessidade de assegurar a efetividade imediata do regime, a presente lei cria diretamente a Autoridade Nacional de Proteção de Dados, enquanto entidade administrativa independente, dotada de independência funcional, autonomia administrativa e financeira, sem sujeição a instruções do poder político, do Governo, de entidades reguladas ou de quaisquer outras entidades públicas ou privadas.

A implementação da lei deve ser progressiva e ajustada à realidade institucional de Timor-Leste, mas sem suspender a proteção essencial dos direitos dos titulares. Assim, a lei estabelece uma fase inicial de instalação, socialização, capacitação e orientação, mantendo, desde o início, mecanismos de fiscalização e resposta a situações de risco grave, tratamentos ilícitos, violações de segurança, interconexões indevidas, tratamento abusivo de dados sensíveis ou biométricos e transferências internacionais ilegais.

A experiência comparada demonstra que a adaptação institucional pode coexistir com uma aplicação efetiva da lei. A presente proposta procura, por isso, conciliar simplicidade legislativa, proteção dos direitos fundamentais, confiança na transformação digital, compatibilidade com padrões internacionais e capacidade prática de execução no contexto timorense.

Destarte,

O Governo apresenta ao Parlamento Nacional, nos termos da alínea c) do n.º 1 do artigo 97.º e da alínea a) do número 2 do artigo 115.º da Constituição, a seguinte Proposta de Lei:

REPÚBLICA DEMOCRÁTICA DE TIMOR-LESTE

PROPOSTA DE LEI

N.º _____ /_____

LEI DA PROTEÇÃO DE DADOS PESSOAIS

A Constituição da República Democrática de Timor-Leste, em vigor desde 20 de maio de 2002, proclama Timor-Leste como um Estado de Direito democrático, assente na vontade popular, no respeito pela dignidade da pessoa humana e na garantia dos direitos, liberdades e garantias fundamentais.

No catálogo constitucional dos direitos fundamentais, o artigo 38.º consagra o direito à proteção dos dados pessoais, remetendo para a lei a definição do respetivo conceito, bem como das condições aplicáveis ao seu tratamento. Decorridas mais de duas décadas desde a entrada em vigor da Constituição, a ausência de um regime legal geral e eficaz de proteção de dados pessoais tornou-se uma lacuna normativa particularmente relevante, tanto do ponto de vista constitucional como do ponto de vista institucional, económico e tecnológico.

A necessidade de legislar nesta matéria assume hoje uma relevância acrescida. Por um lado, impõe-se dar cumprimento efetivo ao artigo 38.º da Constituição. Por outro lado, a transformação digital do Estado, a modernização da Administração Pública, a interoperabilidade entre instituições, o desenvolvimento de sistemas de identidade digital, a digitalização dos registos públicos e a crescente utilização de tecnologias digitais exigem um quadro jurídico claro, seguro e adequado à realidade nacional.

A presente lei estabelece, assim, o regime jurídico geral da proteção de dados pessoais, tendo por finalidade garantir a proteção das liberdades, dos direitos fundamentais e da dignidade das pessoas singulares, sem prejuízo da utilização legítima, responsável e segura da informação para a prestação de serviços públicos mais eficientes, a criação de novas oportunidades económicas, o reforço da confiança digital, a participação de Timor-Leste na economia regional e global e a melhoria da qualidade de vida do Povo Timorense.

A proteção de dados pessoais não deve ser entendida como obstáculo à inovação ou à transformação digital. Pelo contrário, constitui uma condição essencial para que essa transformação ocorra com confiança, transparência, segurança e respeito pelos cidadãos. Sem garantias adequadas de privacidade, segurança e responsabilidade, torna-se mais difícil promover a partilha legítima de informação entre instituições, desenvolver serviços públicos digitais integrados, assegurar a adesão dos cidadãos às novas soluções tecnológicas e consolidar uma Administração Pública centrada na pessoa.

A presente lei inspira-se em princípios internacionalmente reconhecidos em matéria de proteção de dados pessoais, acolhidos em convenções multilaterais, instrumentos regionais, regimes legislativos comparados e boas práticas internacionais, incluindo experiências de países lusófonos, da União Europeia e da ASEAN. A adesão de Timor-Leste à ASEAN reforça, igualmente, a importância de um regime nacional compatível com padrões regionais de confiança digital, comércio eletrónico, proteção da informação pessoal e fluxos transfronteiriços seguros de dados.

O tratamento de dados pessoais abrangido pela presente lei deve obedecer a princípios fundamentais de licitude, lealdade, boa-fé, transparência, finalidade determinada, minimização, necessidade, adequação, proporcionalidade, exatidão, limitação da conservação, segurança, não discriminação e responsabilidade. Estes princípios constituem a base de uma cultura de proteção de dados orientada para a prevenção de riscos, a proteção dos titulares e a responsabilização das entidades públicas e privadas que tratam dados pessoais.

A lei reconhece direitos essenciais aos titulares dos dados, incluindo o direito à informação, ao acesso, à retificação, ao apagamento, à não sujeição a decisões exclusivamente automatizadas e à apresentação de reclamação perante a autoridade competente. Ao mesmo tempo, estabelece deveres para os responsáveis pelo tratamento e subcontratados, nomeadamente em matéria de segurança, documentação, confidencialidade, tratamento de dados sensíveis, proteção de menores, videovigilância, transferências internacionais e adoção de medidas de proteção de dados desde a conceção e por defeito.

Considerando a necessidade de assegurar a efetividade do regime, a presente lei cria a Autoridade Nacional de Proteção de Dados, enquanto entidade administrativa independente, dotada de independência funcional,

autonomia administrativa e financeira, sem sujeição a instruções do Governo, do poder político, das entidades reguladas ou de quaisquer outras entidades públicas ou privadas. A criação desta autoridade constitui uma condição essencial para garantir a fiscalização, a orientação, a aplicação coerente da lei e a proteção efetiva dos direitos dos titulares.

A presente lei prevê ainda mecanismos de fiscalização, medidas corretivas e um regime próprio de contraordenações, de modo a assegurar que a proteção de dados pessoais não se limita a uma declaração de princípios. A existência de consequências jurídicas proporcionais em caso de incumprimento reforça a segurança jurídica, incentiva a conformidade das entidades públicas e privadas e contribui para consolidar a confiança dos cidadãos no tratamento dos seus dados pessoais.

Reconhecendo, contudo, a realidade institucional de Timor-Leste, a implementação da lei deve ser progressiva, proporcional e acompanhada de ações de socialização, capacitação e orientação técnica. Tal implementação gradual não deve, porém, suspender a proteção essencial dos direitos dos titulares, especialmente perante situações de risco grave, tratamento ilícito de dados sensíveis ou biométricos, violações de segurança, interconexões indevidas, utilização abusiva de identificadores únicos ou transferências internacionais ilegais.

A experiência comparada demonstra que a adaptação institucional pode coexistir com uma aplicação efetiva da lei. A presente lei procura, por isso, conciliar simplicidade legislativa, proteção dos direitos fundamentais, confiança na transformação digital, compatibilidade com padrões internacionais e capacidade prática de execução no contexto timorense.

Assim, o Parlamento Nacional decreta, nos termos do artigo 38.º e do n.º 1 do artigo 95.º da Constituição da República, para valer como lei, o seguinte:

CAPÍTULO I
DISPOSIÇÕES GERAIS

Artigo 1.º
Objeto

1. A presente lei estabelece o regime geral da proteção de dados pessoais das pessoas singulares.

Artigo 2.º
Princípios gerais

1. O tratamento de dados pessoais deve realizar-se de forma a respeitar os princípios relativos ao tratamento de dados pessoais, os direitos do titular dos dados e as obrigações previstas neste diploma.
2. O titular dos dados deve dispor de mecanismos claros, de fácil compreensão e acesso, e de baixo custo, que permitam o exercício dos seus direitos nos termos legais.

Artigo 3.º
Definições

1. Para os efeitos da presente lei, entende-se por:
   a) "Anonimização", o processo de retirar elementos aos dados pessoais para que o titular dos dados deixe de ser identificado ou identificável;
   b) "Dados anonimizados", os dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado ou identificável;
   c) "ANPD", a Autoridade Nacional de Proteção de Dados, uma entidade administrativa independente responsável por fiscalizar a aplicação da presente lei;
   d) "Base de dados" ou "Ficheiro", qualquer conjunto estruturado de informação, em suporte físico ou eletrónico, que compreenda dados pessoais organizados de forma sistemática, permitindo a pesquisa de informação pessoal específica;
   e) "Dados pessoais", qualquer informação, de qualquer natureza, independentemente do respetivo suporte, incluindo cópias físicas e eletrónicas, som e imagem, referente a uma pessoa singular («titular dos dados»), e que torne essa pessoa identificável.

f) “Dados sensíveis”, os dados pessoais que revelem convicções ou posições religiosas ou filosóficas, opiniões políticas, filiação partidária ou sindical, origem racial ou étnica, vida privada, informação relativa à saúde, vida ou orientação sexual, assim como os dados genéticos, biométricos e dados relativos a deficiências de natureza física, intelectual, mental, de desenvolvimento ou funcional;

g) “Dados biométricos”, os dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos;

h) “Destinatário”, a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo ou entidade, a quem sejam comunicados dados pessoais, ou a quem os dados pessoais sejam acessíveis;

i) “Estabelecimento”, uma instalação estável com base na qual o responsável pelo tratamento ou o subcontratado exercem, de forma efetiva e real, uma atividade. A forma jurídica de tal estabelecimento, quer se trate de sucursal, quer de uma filial, não é fator determinante neste contexto;

j) “Identificável”, uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome ou número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da sua identidade física, fisiológica, genética, mental, económica, cultural ou social;

k) “Menor”, a pessoa singular com idade inferior a 17 anos, sem prejuízo dos efeitos da emancipação nos termos da lei civil;

l) “Pseudonimização”, o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de 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 identificada e identificável;

m) “Responsável pelo tratamento”, a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo ou entidade, que, individualmente ou em conjunto com outrem, tome decisões em matéria de tratamento de dados pessoais;

n) “Subcontratado”, a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo ou entidade, que trata os dados pessoais por conta do responsável pelo tratamento e segundo as instruções deste;

o) “Titular dos dados”, uma pessoa singular identificada ou identificável;

p) “Tratamento de dados pessoais” ou “tratamento”, qualquer operação realizada com os dados pessoais, por meios automatizados ou não automatizados, tais como o acesso, a consulta, a recolha, a receção, a extração, o registo, a organização, a estruturação, a classificação, a avaliação, a utilização, a reprodução, a comparação, a interconexão, a transmissão, a distribuição, a comunicação, a transferência, a divulgação, a disseminação, o processamento, o arquivamento, o armazenamento, a conservação, a eliminação, a destruição, a recuperação e a modificação da informação;

q) “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 sujeitos a qualquer tipo de tratamento.

Artigo 4.º

Âmbito de aplicação

1. A presente lei aplica-se ao tratamento de dados pessoais realizado:

a) No contexto das atividades de um estabelecimento situado no território nacional, independentemente de o tratamento ocorrer dentro ou fora desse território;

b) Fora do território nacional, em locais onde a legislação timorense seja aplicável por força do direito internacional público;

c) Por responsável pelo tratamento ou subcontratado, sem estabelecimento no território nacional, em relação ao tratamento de dados pessoais de titular de dados que se encontre naquele território e que esteja relacionado com:

i) A oferta de bens ou serviços ao titular dos dados, independentemente de estarem associados a uma contraprestação ou pagamento; ou

ii) O controlo do comportamento do titular dos dados, desde que esse comportamento tenha lugar no território nacional.

2. Nos casos referidos na alínea c) do número anterior, o responsável pelo tratamento deve designar, mediante comunicação à ANPD, um representante estabelecido em território nacional, que se lhe substitua no exercício dos seus direitos e cumprimento das suas obrigações, sem prejuízo da sua própria responsabilidade.

Artigo 5.º

Exclusões

1. A presente lei não se aplica ao tratamento de dados pessoais efetuado em qualquer das seguintes situações:

a) Por pessoa singular no âmbito de atividades exclusivamente pessoais ou domésticas;

b) Para fins exclusivamente jornalísticos ou de expressão artística ou literária;

c) Por autoridade competente para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de penas, sem prejuízo do disposto no artigo 24.º.

d) Por autoridade competente para efeitos de defesa nacional e de segurança do Estado.

2. O tratamento de dados pessoais a que se referem as alíneas c) e d) do número anterior está sujeito a regras específicas constantes de diploma próprio; essas regras devem incluir as medidas necessárias, proporcionais e adequadas para satisfação do interesse público, tendo em consideração a gravidade do risco para o titular dos dados, o respeito pelas garantias processuais e direitos fundamentais do titular dos dados, bem como as normas contidas em instrumentos de direito internacional público a que Timor-Leste se encontre vinculado.

3. Os dados anonimizados não são considerados dados pessoais para efeitos da presente lei, exceto quando o processo de anonimização a que os dados sejam submetidos tenha sido revertido, ou quando os dados possam ser revertidos mediante a aplicação de esforços razoáveis por parte do responsável pelo tratamento ou por terceiro.

Artigo 6.º

Autoridade Nacional de Proteção de Dados

1. A autoridade de controlo responsável pela promoção, fiscalização e garantia do cumprimento da presente lei é a Autoridade Nacional de Proteção de Dados, adiante designada por ANPD.

2. A criação, natureza jurídica, composição, atribuições, competências, poderes, garantias de independência, regime financeiro e regras essenciais de funcionamento da ANPD são regulados no Capítulo IV da presente lei.

CAPÍTULO II

TRATAMENTO DE DADOS PESSOAIS EM GERAL

Secção I

Princípios e obrigações

Artigo 7.º

Princípios relativos ao tratamento de dados pessoais

1. Os dados pessoais devem ser:

a) Tratados de forma lícita, legítima, leal e transparente («princípio da licitude, lealdade e transparência»);

b) Recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser tratados posteriormente de forma incompatível com essas finalidades («princípio da limitação das finalidades»);

c) Adequados, pertinentes e limitados ao mínimo necessário às finalidades para que são tratados («princípio da minimização»);

d) Exatos e atualizados sempre que necessário, devendo ser tomadas as medidas adequadas para assegurar que sejam apagados ou retificados sem demora os dados inexatos ou incompletos, tendo em conta as finalidades para que são tratados («princípio da exatidão»);

e) Conservados de forma a permitir a identificação do titular dos dados apenas durante o período necessário para a prossecução das finalidades para as quais são tratados («princípio da limitação da conservação»).

2. Cabe ao responsável pelo tratamento assegurar a observância do disposto nos números anteriores («princípio da responsabilidade»).

Artigo 8.º

Condições de licitude do tratamento

1. O tratamento de dados pessoais só pode ser efetuado se se verificar pelo menos uma das seguintes condições:

a) Se o titular tiver dado de forma válida o seu consentimento;

b) Se o tratamento for necessário para o cumprimento de uma obrigação legal ou regulamentar a que o responsável pelo tratamento esteja sujeito;

c) Se o tratamento for necessário para execução de um contrato do qual o titular dos dados seja parte ou de diligências pré-contratuais efetuadas a seu pedido;

d) Se o tratamento for necessário para evitar situações de fraude ou proteger a segurança do titular dos dados, no âmbito da confirmação da identidade do titular dos dados antes de responder a um pedido deste;

e) Se o tratamento for necessário para o regular exercício de direitos em procedimentos judiciais, administrativos, de arbitragem ou outros meios de resolução alternativa de litígios;

f) Se o tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;

g) Se o tratamento for necessário para propósitos médicos ou de saúde, sendo realizado por profissional de saúde ou entidade prestadora de cuidados de saúde;

h) Se o tratamento for necessário para defesa dos interesses legítimos do responsável pelo tratamento ou de terceiro, exceto se prevalecerem os direitos e liberdades fundamentais do titular dos dados que exijam a proteção dos dados pessoais; ou

i) Se o tratamento for necessário para a execução de uma missão de interesse público ou para o exercício de autoridade pública da qual esteja investido o responsável pelo tratamento.

2. O tratamento de dados pessoais efetuado nos termos da alínea i) do número anterior é regido por legislação própria, que deve prever medidas de defesa do interesse público, com observância das garantias processuais e dos direitos fundamentais do titular dos dados, devendo para esse efeito a ANPD emitir recomendações ou pareceres técnicos.

Artigo 9.º

Consentimento

1. O consentimento do titular dos dados pessoais é válido se existir uma manifestação de vontade, livre, específica e informada, nos termos da qual o titular aceita, mediante declaração ou ato positivo inequívoco, que os seus dados pessoais sejam objeto de tratamento.

2. Considera-se que o consentimento é informado, se o titular tiver recebido a seguinte informação, num formato prontamente inteligível e compatível com o modo de interação com o responsável, incluindo, se for caso disso, por meios eletrónicos:

a) A identidade, a morada ou endereço de correio eletrónico do responsável pelo tratamento e, caso exista, do representante designado por este;

b) As categorias dos dados pessoais tratados;

c) As finalidades específicas do tratamento, sendo consideradas nulas e de nenhum valor as manifestações de vontade genéricas de tratamento de dados pessoais;

d) Os métodos de recolha da informação;

e) Os destinatários, ou categorias de destinatários pretendidos, se a informação for transmitida a terceiro; e

f) A existência e as condições de exercício dos direitos de acesso, de retificação e de apagamento, salvo se se aplicar exceção prevista nos termos legais.

3. A informação referida no número anterior é prestada ao titular dos dados no momento da recolha dos dados pessoais, podendo ainda ser prestada, num prazo razoável, em momento posterior, caso se comprove que:

a) Os demais requisitos do consentimento, em especial a liberdade de decidir, estão reunidos; e

b) A prestação da informação no momento da recolha é impossível ou exige um esforço desproporcionado.

4. O consentimento é prestado por escrito, ou através de outros meios que sejam suscetíveis de demonstrar a manifestação inequívoca da vontade do titular dos dados.

5. Se o consentimento do titular dos dados for prestado no contexto de uma declaração escrita que diga também respeito a outros assuntos, o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente desses outros assuntos.

6. O consentimento não constitui fundamento válido para o tratamento de dados pessoais por entidade pública quando, pela natureza da relação entre o titular dos dados e a entidade pública, não exista verdadeira liberdade de escolha ou quando o tratamento seja necessário ao cumprimento de obrigação legal, missão de interesse público ou exercício de autoridade pública.

Artigo 10.º

Revogação do consentimento

1. O consentimento pode ser livremente revogado pelo titular dos dados, mediante comunicação dirigida ao responsável pelo tratamento, permanecendo no entanto válido o tratamento entretanto efetuado com base no consentimento anteriormente prestado.

2. A revogação de consentimento não deve implicar custos para o titular dos dados, não podendo o responsável pelo tratamento cobrar qualquer quantia para satisfazer a pretensão daquele.

3. Ocorrendo alteração na finalidade do tratamento que não seja compatível com a finalidade referida na alínea c) do n.º 2 do artigo 9.º, o responsável pelo tratamento deve informar o titular dos dados sobre essa alteração, antes do tratamento subsequente, e o titular dos dados pode recusar-se a prestar consentimento para a nova finalidade.

Artigo 11.º

Medidas gerais de proteção de dados

1. O responsável pelo tratamento e o subcontratado devem pôr em prática medidas técnicas e organizativas como, por exemplo, a pseudonimização, que assegurem um nível de proteção dos dados pessoais adequado, tendo por referência a probabilidade e gravidade dos riscos do tratamento dos dados pessoais, bem como o contexto em que é realizado.

2. As medidas previstas no número anterior devem:

a) Proteger os dados pessoais contra qualquer acesso não autorizado, ou a sua destruição, perda, alteração, comunicação acidental ou ilegítima, ou qualquer tipo de tratamento impróprio ou ilegítimo, e em particular quando o tratamento implicar a transmissão de dados em rede;

b) Ter em conta a segurança física dos dados;

c) Assegurar que, desde a conceção e por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento, tendo em atenção, designadamente, a quantidade de dados pessoais recolhidos, a extensão do seu tratamento, o seu prazo de conservação e a sua acessibilidade; e

d) Prever mecanismos que permitam ao responsável pelo tratamento ou ao subcontratado detetar, prevenir e responder a ataques, intrusões, e outras falhas de segurança.

3. Tratando-se de oferta ou prestação de um produto ou serviço, o responsável pelo tratamento e o subcontratado devem cumprir o disposto nos números anteriores logo a partir da fase de conceção do produto ou serviço.
4. O responsável pelo tratamento deve exigir ao subcontratado e a quaisquer terceiros para quem transfira dados pessoais, que lhe comuniquem imediatamente sempre que tenham conhecimento da ocorrência de uma violação de dados pessoais, e que tomem medidas imediatas para corrigir, ou de outra forma responder à falha de segurança que provocou a violação de dados pessoais.
5. A ANPD pode estabelecer padrões técnicos mínimos para as medidas previstas no presente artigo, tendo em consideração a natureza dos dados pessoais, as características do tratamento, bem como o estado atual da tecnologia, podendo esses padrões incluir medidas específicas para o tratamento de dados pessoais sensíveis.
6. Tendo em conta a natureza das entidades responsáveis pelo tratamento, bem como das instalações em que o tratamento é realizado, a ANPD pode dispensar a existência de certas medidas técnicas e organizativas, garantindo que se mostre o respeito pelos direitos fundamentais do titular dos dados.
7. O cumprimento de códigos de conduta e certificações aprovados pela ANPD pode ser utilizado como elemento para demonstrar o cumprimento das obrigações previstas no presente artigo.

Artigo 12.º

Medidas específicas para o armazenamento, apagamento e conservação

1. Os dados pessoais devem ser conservados apenas durante o tempo necessário para as finalidades subjacentes à sua recolha e tratamento, sem prejuízo do disposto em outras disposições legais ou autorização conferida pela ANPD.
2. Os dados pessoais devem ser apagados de forma segura.
3. Ao determinar o método de apagamento seguro, o responsável pelo tratamento deve ter em consideração, pelo menos, a natureza, a sensibilidade dos dados e o contexto em que os mesmos são tratados.
4. Dentro do âmbito e limites técnicos das atividades de tratamento, os dados pessoais são apagados depois de concluído o seu tratamento, sem prejuízo do disposto no número seguinte.
5. O armazenamento dos dados após a conclusão do tratamento é autorizado para as seguintes finalidades:

a) Cumprimento de uma obrigação legal ou regulamentar imposta ao responsável pelo tratamento;

b) Fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, nos termos definidos pela ANPD;

c) Propósito de transferência para terceiro, desde que sejam cumpridos os requisitos aplicáveis ao tratamento de dados, na forma prevista na presente lei; ou

d) Utilização exclusiva do responsável pelo tratamento, sendo proibido o acesso por terceiros, e desde que tenham sido adotadas medidas técnicas e organizativas de restrição ao acesso aos dados, designadamente, a sua anonimização.

Artigo 13.º

Regime de subcontratação

1. O responsável pelo tratamento tem a obrigação de zelar pelo cumprimento da presente lei.
2. Sempre que o tratamento seja realizado por conta do responsável pelo tratamento, este deve escolher um subcontratado que ofereça garantias suficientes de execução de medidas técnicas e organizativas adequadas, devendo o responsável pelo tratamento monitorizar o cumprimento dessas medidas.

3. A realização de operações de tratamento em regime de subcontratação rege-se por um contrato reduzido a escrito, ou por outro instrumento jurídico equivalente, que obrigue o subcontratado perante o responsável pelo tratamento e estipule, designadamente, que o subcontratado atua exclusivamente mediante instruções do responsável pelo tratamento, o objeto e a duração do tratamento, a natureza e a finalidade do tratamento, as categorias de dados pessoais tratados, as obrigações e os direitos do responsável pelo tratamento, as condições de sub-subcontratação, o procedimento a adotar no caso de violação de dados pessoais, bem como a obrigação que incumbe ao subcontratado de adotar as medidas técnicas e organizativas adequadas.
4. O responsável pelo tratamento deve exigir de qualquer subcontratado ou terceiro que atue por sua conta que o informe de quaisquer dados inexatos ou incompletos de que tome conhecimento.
5. Qualquer pessoa que, agindo sob a autoridade do responsável pelo tratamento ou do subcontratado, incluindo o próprio subcontratado, tenha acesso a dados pessoais, não pode proceder ao seu tratamento sem instruções do responsável pelo tratamento, salvo por força de obrigação legal.
6. O responsável pelo tratamento pode delegar no subcontratado o cumprimento das obrigações emergentes dos Capítulos II e III da presente lei, sem prejuízo da sua própria responsabilidade.

Artigo 14.º

Transferências de dados para países terceiros ou organizações internacionais

1. Para além de outros requisitos aplicáveis ao tratamento de dados pessoais nos termos da presente lei, o responsável pelo tratamento só pode transferir dados pessoais para um país terceiro ou organização internacional:
   a) Quando a ANPD tenha declarado, mediante decisão, que o país terceiro ou organização internacional asseguram um nível de proteção adequado;
   b) Com o consentimento explícito do titular dos dados;
   c) Nos termos de cláusulas contratuais que estipulem medidas técnicas e organizativas que garantam um nível de proteção adequado dos dados pessoais transferidos;
   d) Com base em regras vinculativas aplicáveis a grupos empresariais multinacionais, que estipulem medidas técnicas e organizativas a implementar por todas as entidades do grupo, de modo a garantir um nível de proteção adequado dos dados pessoais, e que devem ser respeitadas por todas aquelas entidades; ou
   e) De acordo com códigos de conduta, certificações, marcas, selos ou normas de proteção de dados pessoais, alusivos a mecanismos de transferência, que estabeleçam níveis de proteção adequados.
2. Sem prejuízo de orientações específicas emitidas pela ANPD, a adequação do nível de proteção é apreciada em função de todas as circunstâncias que rodeiem a transferência de dados, em especial, a natureza dos dados, a finalidade e a duração do tratamento ou tratamentos pretendidos, as regras de direito, gerais ou sectoriais, em vigor nos países de origem e destino final, bem como as normas profissionais e as medidas de segurança que são respeitadas no país ou organização internacional em causa.

Secção II

Direitos do titular dos dados

Artigo 15.º

Direito de acesso

1. O titular dos dados tem o direito de obter do responsável pelo tratamento, a título gratuito, a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento, bem como, quando se confirmar esse tratamento, o acesso aos dados pessoais e a prestação de informação sobre:
   a) As finalidades específicas do tratamento;
   b) As categorias de dados pessoais em causa;
   c) O tipo e a duração do tratamento;
   d) Os destinatários ou categorias de destinatários dos dados;

e) A identificação do responsável pelo tratamento;

f) A informação de contacto do responsável pelo tratamento e do representante designado por este, caso exista; e

g) A existência e condições de exercício dos direitos do titular dos dados previstos na presente lei, com menção explícita ao direito de apresentar reclamação à ANPD e aos direitos de acesso, retificação e apagamento dos dados;

2. Com periodicidade razoável, o titular dos dados pode enviar um pedido de confirmação e de prestação de informações ao responsável pelo tratamento, por meio de uma solicitação de acesso aos dados.
3. Depois de receber um pedido do titular dos dados, o responsável pelo tratamento deve confirmar a identidade do requerente e de seguida responder, sem constrangimentos ou demora injustificados.
4. Caso nem o responsável pelo tratamento nem os seus subcontratados detenham dados pessoais do titular dos dados, o responsável pelo tratamento informa-o sobre a identidade do responsável pelo tratamento e/ou do subcontratado corretos, sempre que possível.
5. Sem prejuízo do disposto no número anterior, o responsável pelo tratamento pode recusar o pedido do titular dos dados sempre que:
   a) A divulgação da informação viole a lei ou uma ordem judicial;
   b) Tendo em conta a sensibilidade dos dados, o ónus ou encargo suportado com a divulgação da informação seja irrazoável ou desproporcional face aos riscos para o titular dos dados;
   c) O pedido seja apresentado de modo repetitivo ou com má fé; ou
   d) A divulgação da informação comprometa direitos e interesses de terceiros que não o titular dos dados, nomeadamente, comprometendo a segurança dos dados ou segredos comerciais e industriais.
6. O responsável pelo tratamento deve garantir que o titular dos dados é informado, sem demora injustificada, sobre os motivos de qualquer recusa, bem como sobre a possibilidade de reclamar para a ANPD.

Artigo 16.º

Direito de retificação

1. Tendo em consideração as finalidades do tratamento, o responsável pelo tratamento e o subcontratado devem tomar todas as medidas adequadas para assegurar a exatidão dos dados, sendo retificados ou atualizados os dados inexatos ou incompletos, se necessário.
2. Com periodicidade razoável, o titular dos dados pode solicitar ao responsável pelo tratamento a correção de inexatidões e, tendo em conta as finalidades do tratamento, pode pedir que os seus dados pessoais incompletos sejam completados.
3. Quando a informação inexata ou incompleta afetar a finalidade do tratamento, o responsável pelo tratamento deve comunicar a cada subcontratado e terceiro a quem os dados pessoais tenham sido transmitidos qualquer retificação dos dados pessoais a que se tenha procedido.
4. O subcontratado deve informar o responsável pelo tratamento sobre quaisquer inexatidões e correções de que tenha conhecimento.
5. Depois de receber o pedido de retificação, o responsável pelo tratamento deve confirmar a identidade do requerente, e responder de forma atempada e sem encargos para o titular dos dados.
6. Caso o responsável pelo tratamento ou os seus subcontratados tratem dados do titular dos dados, o responsável pelo tratamento garante que as eventuais inexatidões são corrigidas, exceto quando:
   a) Os benefícios resultantes de uma não alteração dos dados pessoais se sobreponham à probabilidade e à gravidade dos riscos colocados ao titular dos dados, tendo em consideração a sensibilidade dos dados tratados;
   b) A retificação viole a lei ou uma ordem judicial; ou
   c) O ónus ou encargo suportado com a correção seja irrazoável ou desproporcional face aos riscos para o titular dos dados.

Artigo 17.º

Direito ao apagamento

1. O titular dos dados tem o direito de exigir ao responsável pelo tratamento, a título gratuito e sem demora injustificada, o apagamento dos dados pessoais que lhe digam respeito, verificando-se um dos seguintes casos:
   a) Os dados pessoais deixem de ser necessários para a finalidade que motivou a sua recolha ou tratamento posterior;
   b) O titular dos dados retire o seu consentimento, nos termos da presente lei, conquanto não exista outra condição de licitude para o tratamento desses dados;
   c) Os dados pessoais tenham sido tratados ilicitamente; ou
   d) Os dados pessoais devam ser apagados nos termos de uma norma legal ou regulamentar a que o responsável pelo tratamento esteja sujeito.
2. Após o recebimento de um pedido de apagamento, o responsável pelo tratamento deve apagar os dados, sem demora injustificada, exceto na medida em que o tratamento seja necessário para:
   a) Exercer o direito à liberdade de expressão e de informação;
   b) Cumprimento de norma legal ou regulamentar a que o responsável pelo tratamento esteja sujeito;
   c) Execução de uma missão de interesse público, designadamente, na área de saúde pública, conforme seja permitido nos termos da presente lei ou outra norma legal ou regulamentar;
   d) Fins de arquivo de interesse público, de investigação científica ou histórica ou fins estatísticos, caso o apagamento possa tornar impossível ou prejudicar seriamente a realização dos objetivos desse tratamento; ou
   e) A declaração, exercício ou defesa de direitos em processo judicial.

Artigo 18.º

Não sujeição a decisões individuais automatizadas

1. Qualquer pessoa tem o direito de não ficar sujeita a uma decisão que produza efeitos na sua esfera jurídica ou que a afete de modo significativo, tomada exclusivamente com base num tratamento automatizado de dados destinado a avaliar determinados aspetos da sua personalidade, designadamente a sua capacidade profissional, o seu crédito, a confiança de que é merecedora ou o seu comportamento.
2. Sem prejuízo do cumprimento das restantes disposições da presente lei, o n.º 1 não se aplica se a decisão:
   a) For baseada no consentimento do titular dos dados;
   b) For necessária para a celebração ou para a execução de um contrato entre o titular dos dados e um responsável pelo tratamento; ou
   c) For autorizada por lei.
3. Nos casos previstos no n.º 2 devem ser adotadas medidas adequadas que garantam a defesa dos direitos e interesses legítimos do titular dos dados e que permitam que o seu ponto de vista seja exposto e considerado.
4. Pode ainda ser permitida a tomada de uma decisão nos termos do n.º 1, quando autorizada pela ANPD e desde que sejam tomadas medidas adequadas para a defesa dos direitos e interesses legítimos do titular dos dados.

Artigo 19.º

Direito de apresentar reclamação à ANPD

1. Sem prejuízo de qualquer outra via de recurso, todos os titulares de dados têm o direito de apresentar uma reclamação à ANPD sempre que considerarem que o tratamento dos seus dados pessoais viola a presente lei.
2. Os mecanismos para o exercício do direito referido no número anterior são definidos por regulamento, deliberação ou modelo aprovado pela ANPD.

CAPÍTULO III

DISPOSIÇÕES RELATIVAS A SITUAÇÕES ESPECÍFICAS DE TRATAMENTO

Artigo 20.º

Tratamento de dados pessoais sensíveis

1. É proibido o tratamento de dados pessoais sensíveis, salvo mediante consentimento explícito do titular dos dados, ou quando o tratamento for considerado necessário:
   a) Para cumprimento de uma obrigação legal ou regulamentar a que o responsável pelo tratamento esteja sujeito;
   b) Para execução de contrato de que o titular dos dados seja parte ou de diligências pré-contratuais efetuadas a seu pedido;
   c) Para evitar situações de fraude ou proteger a segurança do titular dos dados, no âmbito da confirmação da identidade do titular dos dados antes de responder a um pedido deste;
   d) Para o regular exercício de direitos em procedimentos judiciais, administrativos, de arbitragem ou outros meios de resolução alternativa de litígios;
   e) Para proteção de interesses vitais do titular dos dados ou de terceiro, estando o titular dos dados física ou legalmente incapaz de dar o seu consentimento;
   f) Para propósitos médicos ou de saúde, sendo realizado por profissional de saúde obrigado ao segredo profissional ou entidade prestadora de cuidados de saúde;
   g) Para defesa dos interesses legítimos do responsável pelo tratamento ou de terceiro, exceto se prevalecerem os direitos e liberdades fundamentais do titular dos dados que exijam a proteção dos dados pessoais; ou
   h) Por motivos de interesse público importante, designadamente, em matéria de proteção da segurança do Estado, da defesa da segurança pública, bem como no domínio da saúde pública, incluindo a proteção 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 ou dispositivos médicos.
2. O tratamento de dados pessoais efetuado nos termos da alínea h) do número anterior é regido por legislação própria, que deve identificar e prever medidas de defesa do interesse público considerado importante, com observância das garantias processuais e dos direitos fundamentais do titular dos dados, devendo para esse efeito a ANPD emitir recomendações ou pareceres técnicos.
3. O tratamento dos dados sensíveis é ainda permitido quando for referente a dados manifestamente tornados públicos pelo seu titular, desde que tenha dado consentimento explícito para o tratamento dos mesmos.
4. Em qualquer caso, o tratamento de dados sensíveis deve observar garantias de não discriminação de pessoas singulares, bem como incorporar as medidas adequadas e específicas que salvaguardem os direitos fundamentais do titular dos dados.

Artigo 21.º

Tratamento de dados pessoais de menor

1. O tratamento de dados pessoais cujo titular seja menor deve ter em conta o seu melhor interesse, nos termos da legislação nacional sobre proteção de menores.
2. Quando o tratamento de dados pessoais de menor não emancipado se baseie no consentimento, este só é válido se for prestado pelo respetivo representante legal ou por quem exerça responsabilidades parentais, sem prejuízo da audição do menor sempre que, atendendo à sua idade e maturidade, tal se revele adequado.
3. Nos casos a que se refere o n.º 2, o responsável pelo tratamento deve empreender esforços razoáveis, atendendo aos meios disponíveis, para confirmar a idade, identidade e legitimidade do prestador do consentimento.
4. A informação prevista no n.º 2 do artigo 9.º, quando referente a tratamento de dados pessoais de menor, deve ser prestada ao respetivo titular das responsabilidades parentais, de uma forma simples, compreensível e acessível, tendo igualmente em consideração as características físico-motoras,

percetivas, sensoriais, intelectuais e mentais do menor, com uso de recursos audiovisuais sempre que apropriado.

5. O responsável que proceda ao tratamento de dados pessoais de menores deve divulgar publicamente informação referente ao tipo de dados recolhidos, ao modo como são utilizados e aos procedimentos para exercício dos direitos do titular dos dados previstos na presente lei.

Artigo 22.º

Videovigilância

1. Sem prejuízo das disposições legais específicas que regulem a sua utilização, nomeadamente por razões de segurança pública, os sistemas de videovigilância cuja finalidade seja a proteção de pessoas e bens devem cumprir os requisitos e os limites definidos no número seguinte.
2. As câmaras não podem incidir sobre:
   a) Vias públicas, propriedades limítrofes ou outros locais que não sejam do domínio exclusivo do responsável, exceto no que seja estritamente necessário para cobrir os acessos ao imóvel;
   b) A zona de introdução do código pessoal ou PIN em caixas automáticas, terminais de pagamento eletrónico ou equipamentos equivalentes;
   c) O interior de áreas reservadas a clientes ou utentes onde deva ser respeitada a sua intimidade e privacidade, designadamente instalações sanitárias, zonas de espera e provadores de vestuário;
   d) O interior de áreas reservadas aos trabalhadores, designadamente, vestiários, instalações sanitárias e zonas exclusivamente afetas ao seu descanso.
3. Nos estabelecimentos de ensino e aprendizagem, as câmaras de videovigilância só podem incidir sobre os perímetros externos e locais de acesso, e ainda sobre espaços cujos bens e equipamentos requeiram especial proteção, como laboratórios ou salas de informática.
4. No âmbito das relações laborais, as imagens gravadas e outros dados pessoais registados através da utilização de sistemas de vídeo ou outros meios tecnológicos de vigilância à distância só podem ser utilizados no âmbito do processo penal ou contraordenacional ou para efeitos de apuramento de responsabilidade disciplinar.
5. Nos casos em que é admitida a videovigilância, é proibida a captação de som, exceto no período em que as instalações vigiadas estejam encerradas ou mediante autorização da ANPD.
6. As imagens recolhidas através de sistemas de videovigilância devem ser conservadas apenas pelo período estritamente necessário à finalidade que justificou a sua recolha, sem prejuízo da sua conservação quando sejam necessárias para efeitos probatórios em processo criminal, contraordenacional, disciplinar, administrativo ou judicial.
7. A ANPD pode definir, por regulamento, deliberação ou orientação geral, os prazos máximos de conservação das imagens, os requisitos de acesso, extração, comunicação, registo de operações e destruição segura, tendo em conta a finalidade do sistema, o risco para os titulares e a natureza do local vigiado.
8. O acesso às imagens deve ser limitado a pessoas expressamente autorizadas, em número estritamente necessário, ficando sujeito a dever de confidencialidade, registo de acessos e medidas técnicas e organizativas adequadas.

Artigo 23.º

Tratamento de dados pessoais para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos

1. Sem prejuízo das disposições da presente lei, as regras aplicáveis ao tratamento dos dados para fins de arquivo de interesse público, de investigação científica ou histórica ou para fins estatísticos, bem como a sua conservação para os mesmos fins, são desenvolvidas em orientações da ANPD.

Artigo 24.º

Registo de atividades ilícitas, condenações penais, medidas de segurança, infrações e contraordenações

1. A criação e a manutenção de registos centrais relativos a pessoas suspeitas, acusadas ou condenadas pela prática de atividades ilícitas, infrações penais, contraordenações, e sujeitas a decisões que apliquem penas, multas, medidas de segurança, coimas e sanções acessórias, só podem ser realizadas por entidades públicas com essa competência legal, e com observância das normas procedimentais, de segurança e de proteção de dados previstas na presente lei e consagradas em diploma próprio, sujeito a parecer prévio da ANPD.
2. O tratamento de dados pessoais relativos a pessoas suspeitas, acusadas ou condenadas pela prática de atividades ilícitas, infrações penais ou contraordenações, ou sujeitas a decisões que apliquem penas, multas, medidas de segurança, coimas e sanções acessórias, é permitido, desde que:
   a) Tal tratamento seja necessário à execução de finalidades legítimas do seu responsável;
   b) Sejam respeitados os direitos fundamentais do titular dos dados; e
   c) Sejam observadas as normas de proteção de dados e de segurança da informação previstas na presente lei e consagradas em diploma próprio, sujeito a parecer prévio da ANPD.

CAPÍTULO IV

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

Artigo 25.º

Criação e natureza

1. É criada a Autoridade Nacional de Proteção de Dados, adiante designada por ANPD, entidade administrativa independente responsável pela promoção, fiscalização e garantia do cumprimento da presente lei.
2. A ANPD é pessoa coletiva de direito público, dotada de poderes de autoridade, independência funcional, autonomia administrativa, financeira e patrimonial, património próprio e orçamento próprio.
3. A ANPD tem sede em Díli e exerce as suas funções em todo o território nacional, com sujeição exclusiva à Constituição e à lei.
4. A ANPD tem a natureza, composição, atribuições, competências, poderes, garantias de independência, organização básica, regime financeiro e mecanismos de funcionamento previstos na presente lei.
5. A ANPD pode aprovar regulamentos, deliberações, orientações, recomendações, modelos e códigos de boas práticas destinados a concretizar a aplicação da presente lei, nos termos nela previstos.
6. A criação e funcionamento da ANPD não dependem de diploma posterior, sem prejuízo da aprovação do respetivo regulamento interno e dos atos necessários à sua instalação administrativa e financeira.

Artigo 26.º

Independência

1. A ANPD exerce as suas atribuições com independência, imparcialidade e sujeição exclusiva à Constituição e à lei.
2. Os membros dos seus órgãos, trabalhadores, consultores e colaboradores não podem solicitar nem receber instruções de qualquer entidade pública ou privada quanto ao mérito das decisões, recomendações, pareceres, fiscalizações ou processos em curso.
3. Os regulamentos, deliberações, decisões e demais atos da ANPD que produzam efeitos externos são impugnáveis nos termos gerais perante os tribunais competentes.

Artigo 27.º

Atribuições e poderes

1. Compete à ANPD, designadamente:
   a) Fiscalizar e promover o cumprimento da presente lei;

b) Receber, apreciar e decidir reclamações apresentadas pelos titulares dos dados;

c) Emitir pareceres, recomendações, orientações, deliberações e códigos de boas práticas;

d) Aprovar modelos de informação aos titulares, modelos de notificação de violações de dados e outros instrumentos de aplicação prática da presente lei;

e) Realizar inspeções, auditorias e pedidos de informação às entidades públicas e privadas;

f) Ordenar medidas corretivas necessárias à conformidade dos tratamentos com a presente lei;

g) Determinar a limitação, suspensão ou cessação de tratamentos ilícitos;

h) Ordenar a retificação, apagamento, limitação ou bloqueio de dados pessoais, quando legalmente devido;

i) Suspender transferências internacionais de dados que violem a presente lei;

j) Aplicar coimas e sanções acessórias, nos termos da presente lei;

k) Emitir parecer prévio sobre tratamentos de elevado risco, interoperabilidade pública, identificadores únicos, biometria, videovigilância e plataformas digitais públicas;

l) Cooperar com autoridades estrangeiras e organizações internacionais em matéria de proteção de dados;

m) Promover ações de formação, socialização e sensibilização junto de entidades públicas, entidades privadas e cidadãos;

n) Apresentar ao Parlamento Nacional relatório anual sobre a sua atividade, o estado da proteção de dados pessoais em Timor-Leste e as recomendações legislativas ou administrativas necessárias.

2. No exercício dos seus poderes, a ANPD deve atuar com proporcionalidade, privilegiando, quando adequado, medidas de orientação, recomendação e correção antes da aplicação de sanções mais gravosas, sem prejuízo da repressão efetiva das infrações graves e muito graves.

Artigo 28.º

Competência regulamentar da ANPD

1. A ANPD pode aprovar regulamentos, deliberações, orientações, recomendações, modelos e códigos de boas práticas destinados a concretizar a aplicação da presente lei, em especial quanto a matérias técnicas, procedimentais, setoriais ou de elevado risco.
2. A competência prevista no número anterior abrange, designadamente, segurança do tratamento, prazos de conservação, videovigilância, exercício dos direitos dos titulares, notificação de violações de dados, avaliações de impacto, subcontratação, transferências internacionais, interoperabilidade pública, identificadores únicos e tratamentos de dados em setores específicos.
3. Os atos da ANPD não podem criar restrições novas aos direitos fundamentais, nem estabelecer infrações, sanções ou obrigações essenciais sem base legal suficiente, devendo limitar-se à concretização e boa execução da presente lei.
4. Os regulamentos e deliberações de caráter geral da ANPD são publicados oficialmente e, sempre que adequado, precedidos de consulta pública.

Artigo 29.º

Composição

1. A ANPD é dirigida por um Conselho Diretivo composto por três membros, incluindo um Presidente.
2. Dois membros do Conselho Diretivo, incluindo o Presidente, são eleitos pelo Parlamento Nacional, por maioria absoluta dos Deputados em efetividade de funções.
3. Um membro do Conselho Diretivo é designado pelo Governo, mediante resolução do Conselho de Ministros.
4. Os membros do Conselho Diretivo são escolhidos de entre pessoas de reconhecida idoneidade, independência e competência técnica, jurídica ou institucional em matéria de direitos fundamentais, proteção de dados, tecnologias digitais, administração pública, regulação ou governação.
5. O mandato dos membros do Conselho Diretivo tem a duração de cinco anos, renovável uma única vez.

6. Os membros do Conselho Diretivo exercem funções com independência, imparcialidade e dedicação adequada à natureza das suas funções, não estando sujeitos a instruções do Parlamento Nacional, do Governo, de entidades reguladas ou de quaisquer outras entidades públicas ou privadas.
7. O Presidente representa a ANPD, convoca e dirige as reuniões do Conselho Diretivo, assegura a coordenação dos seus trabalhos e exerce as demais competências previstas na presente lei e no regulamento interno.

Artigo 30.º

Incompatibilidades, impedimentos e cessação de mandato

1. Os membros do Conselho Diretivo não podem exercer funções governativas, cargos dirigentes em partidos políticos, funções de direção em entidades sujeitas à fiscalização da ANPD, nem qualquer atividade suscetível de comprometer a sua independência ou imparcialidade.
2. Os membros do Conselho Diretivo estão sujeitos a deveres de sigilo, reserva, imparcialidade, independência e prevenção de conflitos de interesses.
3. Os membros do Conselho Diretivo não podem ser destituídos antes do termo do mandato, salvo em caso de renúncia, morte, incapacidade permanente, incompatibilidade superveniente, condenação por crime doloso ou violação grave dos deveres do cargo.
4. A cessação antecipada do mandato deve ser fundamentada e decidida pela entidade competente para a respetiva eleição ou designação, nos termos da presente lei.

Artigo 31.º

Regulamento interno da ANPD

1. O regulamento interno estabelece, designadamente:
   a) A organização interna dos serviços;
   b) As regras de funcionamento do Conselho Diretivo;
   c) A distribuição interna de processos;
   d) Os procedimentos de atendimento, reclamação, fiscalização, parecer, orientação, deliberação e contraordenação;
   e) As regras de expediente, arquivo, tramitação eletrónica e notificações;
   f) As regras internas de segurança da informação, confidencialidade, sigilo e controlo de acessos;
   g) Os mecanismos de prevenção de conflitos de interesses;
   h) Os modelos internos de gestão processual, reclamação, notificação de violações de dados e comunicação com os titulares dos dados e entidades responsáveis pelo tratamento.
2. O regulamento interno não pode limitar os direitos dos titulares dos dados, restringir os poderes da ANPD, criar infrações ou sanções, alterar prazos legais, modificar garantias de defesa ou impugnação judicial, nem estabelecer obrigações essenciais sem base na presente lei.
3. O regulamento interno é publicado oficialmente e disponibilizado ao público em formato acessível.

Artigo 32.º

Serviços, pessoal e orçamento

1. A ANPD dispõe de serviços próprios, compostos por pessoal técnico, jurídico, administrativo e informático necessário ao exercício das suas funções.
2. Até à aprovação do seu quadro de pessoal, a ANPD pode funcionar com trabalhadores recrutados por contrato, mobilidade, destacamento, requisição ou cedência temporária de entidades públicas, sem prejuízo da sua independência funcional.
3. O pessoal da ANPD está sujeito a dever especial de sigilo, confidencialidade, imparcialidade e proteção da informação a que tenha acesso.
4. A ANPD dispõe de orçamento próprio, inscrito no Orçamento Geral do Estado, em dotação que assegure a sua independência funcional e capacidade efetiva de atuação.

5. A ANPD pode beneficiar de apoio técnico, formação, cooperação internacional e assistência de parceiros de desenvolvimento, desde que tal apoio não comprometa a sua independência.

Artigo 33.º

Dever de cooperação

1. As entidades públicas e privadas devem cooperar com a ANPD, prestando as informações, documentos, esclarecimentos e acesso necessários ao exercício das suas competências.
2. O dever de cooperação não prejudica o segredo profissional legalmente protegido, o segredo de justiça, a confidencialidade das comunicações entre advogado e cliente e demais garantias processuais aplicáveis.
3. A recusa injustificada de cooperação com a ANPD constitui infração nos termos da presente lei.

Artigo 34.º

Relatório anual

1. A ANPD apresenta ao Parlamento Nacional, até 31 de março de cada ano, relatório sobre a sua atividade no ano anterior.
2. O relatório deve incluir, designadamente, reclamações recebidas, decisões adotadas, pareceres emitidos, principais riscos identificados, medidas de fiscalização realizadas, recomendações legislativas ou administrativas e avaliação do estado da proteção de dados pessoais em Timor-Leste.
3. O relatório é publicado e disponibilizado em formato acessível ao público, sem prejuízo da proteção de informação confidencial, segredo legalmente protegido ou dados pessoais.

CAPÍTULO V

FISCALIZAÇÃO, RESPONSABILIDADE E CONTRAORDENAÇÕES

Artigo 35.º

Competência da ANPD

1. Compete à ANPD fiscalizar o cumprimento da presente lei, bem como instaurar, instruir e decidir os processos de contraordenação relativos às infrações nela previstas.
2. A decisão do processo de contraordenação cabe ao órgão diretivo da ANPD.
3. No exercício das suas competências, a ANPD pode solicitar às entidades públicas ou privadas as informações, documentos, registos e esclarecimentos necessários.
4. As entidades públicas e privadas devem cooperar com a ANPD, sem prejuízo do segredo profissional legalmente protegido, do segredo de justiça, da confidencialidade das comunicações entre advogado e cliente e das demais garantias legalmente aplicáveis.
5. Sempre que os factos apurados possam constituir crime, a ANPD comunica-os ao Ministério Público, remetendo os elementos relevantes de que disponha, sem prejuízo da continuação do processo de contraordenação quando legalmente admissível.

Artigo 36.º

Medidas corretivas

1. Sem prejuízo da aplicação de coima ou de outras consequências legais, a ANPD pode ordenar as medidas necessárias para assegurar a conformidade do tratamento de dados com a presente lei.
2. A ANPD pode, designadamente:
   a) Emitir advertência ou recomendação;
   b) Dirigir repreensão ao responsável pelo tratamento ou ao subcontratado;
   c) Ordenar a conformação do tratamento com a lei, em prazo determinado;
   d) Ordenar a retificação, apagamento, limitação ou bloqueio de dados pessoais;
   e) Ordenar a suspensão temporária ou definitiva de determinado tratamento;
   f) Suspender transferências internacionais de dados;

g) Suspender interconexão, interoperabilidade ou partilha de dados;

h) Determinar a adoção de medidas técnicas e organizativas adequadas;

i) Ordenar a comunicação de violação de dados pessoais ao titular, quando legalmente exigida.

3. As medidas corretivas devem ser adequadas e proporcionais à gravidade da situação, ao risco para os titulares dos dados, ao número de pessoas afetadas, ao tipo de dados envolvidos e à conduta da entidade responsável.
4. Em caso de risco grave e iminente para os direitos dos titulares, a ANPD pode determinar medidas urgentes antes da decisão final, devendo fundamentar a urgência e limitar a medida ao estritamente necessário.

Artigo 37.º

Contraordenações leves

1. Constitui contraordenação leve:

a) A prestação de informação incompleta, pouco clara ou insuficientemente acessível ao titular dos dados, quando não esteja em causa a omissão de elementos essenciais nem resulte risco relevante para os seus direitos;

b) A resposta tardia a pedido de exercício de direitos do titular, quando o atraso não seja significativo, não constitua recusa injustificada e não cause prejuízo relevante ao titular;

c) A falta de atualização de contactos, avisos de privacidade, registos internos ou outros elementos formais exigidos pela presente lei, quando dessa omissão não resulte risco relevante para os titulares;

d) A falta de conservação organizada de documentação demonstrativa do cumprimento da presente lei, quando a omissão seja meramente formal e não impeça a fiscalização pela ANPD.

Artigo 38.º

Contraordenações graves

1. Constitui contraordenação grave:

a) O tratamento de dados pessoais sem fundamento de licitude previsto na presente lei;

b) A recolha de dados pessoais para finalidades não determinadas, não explícitas ou incompatíveis com as finalidades comunicadas ao titular;

c) A recolha ou conservação de dados pessoais manifestamente excessivos, desnecessários ou desproporcionados face à finalidade do tratamento;

d) A conservação de dados pessoais por período superior ao necessário ou ao legalmente permitido, sem fundamento legítimo de conservação;

e) A utilização de dados pessoais inexatos, incompletos ou desatualizados, quando o responsável pelo tratamento conheça ou deva conhecer essa inexatidão e dela possa resultar prejuízo relevante para o titular;

f) A omissão de informação essencial ao titular dos dados sobre a identidade do responsável pelo tratamento, as finalidades do tratamento, os destinatários dos dados ou os direitos que lhe assistem;

g) A recusa injustificada ou reiterada do exercício dos direitos de acesso, retificação, apagamento, oposição, limitação ou demais direitos reconhecidos na presente lei;

h) A violação do dever de segurança do tratamento, quando resulte risco relevante de acesso não autorizado, perda, alteração, divulgação indevida ou utilização abusiva dos dados pessoais;

i) A falta de notificação de violação de dados pessoais à ANPD, quando legalmente exigida;

j) A falta de comunicação de violação de dados pessoais ao titular, quando legalmente exigida;

k) A realização de tratamento por subcontratado sem contrato escrito ou instrumento jurídico equivalente que defina as instruções, responsabilidades e garantias exigidas pela presente lei;

l) A transferência internacional de dados pessoais sem decisão de adequação, consentimento válido, cláusulas contratuais adequadas, regras vinculativas, certificação, código de conduta ou outro mecanismo admitido pela presente lei;

m) A utilização de sistema de videovigilância em violação dos limites previstos na presente lei, designadamente quanto aos locais abrangidos, acesso às imagens, captação de som, conservação ou comunicação das gravações;

n) A falta de realização de avaliação de impacto ou de consulta prévia à ANPD, quando legalmente exigidas para tratamentos de risco elevado;

o) A falta de designação de encarregado ou ponto focal de proteção de dados, quando legalmente exigida;

p) A recusa injustificada de prestação de informações, documentos, registos ou esclarecimentos solicitados pela ANPD no exercício das suas competências;

q) O incumprimento de medida corretiva, ordem ou decisão da ANPD emitida nos termos da presente lei.

Artigo 39.º

Contraordenações muito graves

1. Constitui contraordenação muito grave:

a) O tratamento de dados sensíveis fora dos casos permitidos pela presente lei, quando dele resulte risco elevado para os direitos, liberdades e garantias dos titulares;

b) O tratamento de dados biométricos para identificação única de pessoa singular sem habilitação legal bastante, consentimento válido quando exigido ou garantias técnicas e organizativas adequadas, quando dele resulte risco elevado para os titulares;

c) O tratamento de dados pessoais relativos a menores em violação das regras previstas na presente lei, quando dele resulte risco elevado para os seus direitos, liberdades e garantias;

d) A criação, interconexão ou utilização de bases de dados públicas ou privadas sem fundamento legal ou sem garantias adequadas, quando permita o acesso, cruzamento ou perfilagem de dados pessoais em larga escala;

e) A utilização de identificador único como chave universal de acesso, cruzamento ou interconexão indiscriminada de bases de dados, fora dos casos legalmente admitidos;

f) A comunicação, divulgação, venda, disponibilização ou cedência ilícita de dados pessoais a terceiros, quando praticada com dolo ou quando envolva dados sensíveis, dados biométricos, dados de menores ou dados em larga escala;

g) A violação de dados pessoais resultante da falta grave de medidas de segurança, quando cause ou seja suscetível de causar risco elevado para os direitos, liberdades e garantias dos titulares;

h) A ocultação dolosa de violação de dados pessoais, de tratamento ilícito ou de comunicação indevida de dados, quando exista dever legal de comunicação à ANPD ou ao titular;

i) A transferência internacional ilícita de dados sensíveis, dados biométricos, dados relativos a menores ou dados pessoais em larga escala, sem qualquer garantia adequada nos termos da presente lei;

j) A utilização de dados pessoais para finalidades discriminatórias, persecutórias, abusivas ou incompatíveis com a dignidade da pessoa humana;

k) A destruição, alteração, ocultação ou falsificação de documentos, registos, logs, contratos, autorizações ou outros elementos relevantes para a fiscalização da ANPD;

l) A obstrução grave das funções de fiscalização da ANPD, designadamente através de recusa reiterada de cooperação, impedimento de acesso a informação legalmente exigível ou incumprimento reiterado de ordens da Autoridade;

m) O incumprimento de medida urgente ou cautelar determinada pela ANPD para prevenir risco grave e iminente para os direitos dos titulares.

2. Para efeitos do presente artigo, considera-se existir risco elevado, designadamente, quando o tratamento seja suscetível de causar discriminação, usurpação de identidade, prejuízo patrimonial ou não patrimonial relevante, exposição pública ilegítima, violação da confidencialidade de dados sensíveis, afetação significativa de menores, limitação indevida de direitos ou outro impacto grave nos direitos, liberdades e garantias dos titulares.

Artigo 40.º

Coimas

1. As contraordenações leves são puníveis com coima de 100 a 2 500 dólares americanos, tratando-se de pessoa singular, e de 250 a 10 000 dólares americanos, tratando-se de pessoa coletiva.
2. As contraordenações graves são puníveis com coima de 500 a 10 000 dólares americanos, tratando-se de pessoa singular, e de 1 000 a 50 000 dólares americanos, tratando-se de pessoa coletiva.
3. As contraordenações muito graves são puníveis com coima de 1 000 a 25 000 dólares americanos, tratando-se de pessoa singular, e de 5 000 a 150 000 dólares americanos, tratando-se de pessoa coletiva.
4. A negligência é punível, sendo os limites mínimos e máximos das coimas reduzidos a metade.
5. Quando o infrator seja microempresa, pequena entidade, associação sem fins lucrativos ou entidade pública de reduzida dimensão, e a infração seja leve ou resulte de negligência sem dano relevante para os titulares, a ANPD deve privilegiar advertência, recomendação ou ordem de conformação antes da aplicação de coima, salvo em caso de reincidência, dolo, recusa de cooperação ou risco significativo para os direitos dos titulares.
6. O pagamento da coima não dispensa o infrator do cumprimento dos deveres omitidos nem da adoção das medidas corretivas determinadas pela ANPD.

Artigo 41.º

Sanções acessórias

1. Em função da gravidade da infração, podem ser aplicadas as seguintes sanções acessórias:
   a) Publicidade da decisão sancionatória;
   b) Suspensão temporária de tratamento, operação, sistema ou transferência internacional;
   c) Proibição temporária de tratamento de determinadas categorias de dados;
   d) Obrigação de adotar plano de conformidade;
   e) Obrigação de realizar auditoria independente;
   f) Suspensão de certificação, autorização, selo, código de conduta ou instrumento reconhecido pela ANPD.
2. As sanções acessórias devem ser adequadas e proporcionais à gravidade da infração e ao risco para os titulares dos dados.
3. A publicidade da decisão sancionatória deve proteger dados pessoais de terceiros, segredo profissional, segredo comercial e demais informação legalmente protegida.

Artigo 42.º

Critérios de aplicação das sanções

1. Na determinação da coima e das sanções acessórias, a ANPD atende, designadamente:
   a) À natureza, gravidade e duração da infração;
   b) Ao número de titulares afetados;
   c) Ao tipo, volume e sensibilidade dos dados envolvidos;
   d) Ao caráter doloso ou negligente da infração;
   e) À capacidade económica do infrator;
   f) À cooperação prestada à ANPD;
   g) À reincidência;
   h) Às medidas adotadas para prevenir, cessar ou reparar os danos;
   i) Ao benefício económico obtido ou esperado com a infração;
   j) Ao grau de afetação da confiança pública e dos direitos dos titulares.

Artigo 43.º

Direito de audição e defesa

1. Nenhuma coima ou sanção acessória pode ser aplicada sem que o arguido seja previamente notificado da imputação da infração e lhe seja concedida a possibilidade de exercer o direito de defesa.
2. A notificação deve conter:
   a) A identificação do arguido;
   b) A descrição dos factos imputados;
   c) A indicação das normas violadas;
   d) A qualificação da infração como leve, grave ou muito grave;
   e) As sanções abstratamente aplicáveis;
   f) Os meios de prova constantes do processo;
   g) O prazo para apresentação de defesa.
3. O arguido dispõe do prazo de 30 dias úteis para apresentar defesa escrita, juntar documentos e requerer diligências de prova.
4. Em casos de especial complexidade, o prazo referido no número anterior pode ser prorrogado pela ANPD, mediante requerimento fundamentado, por período não superior a 30 dias úteis.
5. O arguido pode fazer-se assistir por advogado ou defensor e consultar o processo, sem prejuízo da proteção de dados pessoais de terceiros, informação confidencial, segredo profissional, segredo comercial, segredo de justiça e demais interesses legalmente protegidos.

Artigo 44.º

Prova e decisão

1. A ANPD pode realizar as diligências de prova necessárias à descoberta da verdade e à boa decisão do processo.
2. O arguido pode requerer diligências de prova relevantes para a sua defesa.
3. A ANPD pode indeferir, por decisão fundamentada, as diligências manifestamente impertinentes, desnecessárias, dilatórias ou repetitivas.
4. A decisão final deve ser fundamentada e conter:
   a) A identificação do arguido;
   b) A descrição dos factos provados;
   c) A indicação das normas violadas;
   d) A qualificação jurídica da infração;
   e) A coima e sanções acessórias aplicadas, quando existam;
   f) As medidas corretivas determinadas, quando existam;
   g) O prazo e modo de cumprimento;
   h) A indicação dos meios de impugnação judicial.
5. A falta de apresentação de defesa não impede a decisão final, sem prejuízo do dever da ANPD de apreciar os factos relevantes.

Artigo 45.º

Impugnação judicial

1. As decisões da ANPD que apliquem coimas, sanções acessórias ou medidas corretivas são impugnáveis judicialmente perante o tribunal competente.
2. A impugnação deve ser apresentada no prazo de 30 dias úteis a contar da notificação da decisão.
3. Recebida a impugnação, a ANPD pode, no prazo de 15 dias úteis, revogar total ou parcialmente a decisão impugnada.
4. Caso não revogue integralmente a decisão, a ANPD remete os autos ao tribunal competente, podendo juntar alegações, elementos ou informações que considere relevantes.

5. A impugnação judicial suspende a execução da coima e das sanções acessórias, salvo decisão judicial em contrário.
6. A impugnação judicial não suspende medidas corretivas ou urgentes destinadas a prevenir risco grave ou iminente para os direitos dos titulares, salvo decisão judicial em contrário.

Artigo 46.º

Responsabilidade civil e tutela judicial

1. Qualquer pessoa que tenha sofrido dano patrimonial ou não patrimonial em virtude de violação da presente lei tem direito a obter indemnização do responsável pelo tratamento ou do subcontratado, nos termos gerais.
2. O exercício de direitos perante a ANPD não prejudica o recurso aos tribunais competentes.
3. A responsabilidade civil não prejudica a aplicação de coimas, sanções acessórias, medidas corretivas ou responsabilidade criminal que ao caso couber.

Artigo 47.º

Aplicação subsidiária

1. Ao procedimento contraordenacional previsto na presente lei são subsidiariamente aplicáveis, em tudo o que não contrarie as suas disposições, as normas gerais do procedimento administrativo.
2. Na falta de regime legal especialmente aplicável, e com as necessárias adaptações, são subsidiariamente aplicáveis os princípios gerais do direito sancionatório, o Código Penal e o Código de Processo Penal, na medida em que sejam compatíveis com a natureza administrativa do processo de contraordenação.
3. A aplicação subsidiária não pode prejudicar os direitos de defesa do arguido, a proteção dos titulares dos dados, a confidencialidade de informação legalmente protegida, nem a eficácia das medidas urgentes necessárias à proteção de direitos fundamentais.

CAPÍTULO VI

DISPOSIÇÕES TRANSITÓRIAS E FINAIS

Artigo 48.º

Instalação da ANPD

1. A ANPD considera-se criada na data da entrada em vigor da presente lei.
2. O Parlamento Nacional procede à eleição dos membros do Conselho Diretivo que lhe cabe eleger e o Governo designa o membro que lhe cabe designar, no prazo de 120 dias após a entrada em vigor da presente lei.
3. Até à instalação efetiva dos órgãos da ANPD, o Ministro responsável pela área da justiça, assegura os atos preparatórios necessários à sua instalação, designadamente a identificação de instalações, a previsão orçamental inicial, o apoio administrativo, a abertura de procedimentos de recrutamento e a preparação dos instrumentos de funcionamento.
4. A ANPD inicia funções com a tomada de posse dos membros do seu Conselho Diretivo.
5. No prazo de 90 dias após a tomada de posse, o Conselho Diretivo aprova o regulamento interno da ANPD, o plano inicial de atividades, os modelos provisórios de reclamação e os procedimentos básicos de contacto com os titulares dos dados e entidades responsáveis pelo tratamento.

Artigo 49.º

Fase inicial de implementação

1. Durante os primeiros 18 meses de funcionamento, a ANPD deve privilegiar atividades de orientação, formação, socialização, aprovação de modelos práticos, identificação de tratamentos de maior risco e apoio à conformidade das entidades públicas e privadas.
2. O disposto no número anterior não prejudica a adoção imediata de medidas corretivas ou sancionatórias quando estejam em causa tratamentos ilícitos de dados sensíveis, dados biométricos, interconexões

ilegais de bases de dados, violações graves de segurança, transferências internacionais ilícitas, recusa de cooperação ou risco significativo para os direitos dos titulares.

3. A aplicação de coimas por infrações leves praticadas por negligência só se inicia 18 meses após a entrada em vigor da presente lei, salvo em caso de reincidência, recusa de cooperação, incumprimento de ordem da ANPD ou risco relevante para os titulares.

Artigo 50.º

Legislação anterior

1. Após a entrada em vigor da presente lei, sempre que se justifique, os regimes jurídicos em Timor-Leste que necessitem compatibilização com a presente Lei devem ser progressivamente adequados ao disposto na presente lei, de modo a assegurar um enquadramento legislativo coerente e harmonioso.
2. A falta de adequação legislativa no prazo referido no número anterior não prejudica a aplicação imediata dos princípios, direitos e deveres essenciais previstos na presente lei.

Artigo 51.º

Entrada em vigor

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

Visto e aprovado em Conselho de Ministros em [dia] de [mês] de 2026.

O Primeiro-Ministro,

_____

O Ministro da Justiça,

_____

Personal Data Protection Law

ENGLISH

DALAN
DIGITAL
A NEW PATH FOR
DIGITAL CITIZENSHIP

DEMOCRATIC REPUBLIC OF TIMOR-LESTE

DRAFT LAW

No. _____ /_____

PERSONAL DATA PROTECTION LAW

EXPLANATORY MEMORANDUM

The Fundamental Law, which entered into force on 20 May 2002, proclaims the Democratic Republic of Timor-Leste to be a democratic State governed by the rule of law, based on the will of the people and respect for the dignity of the human person. Within the catalogue of fundamental rights laid down in the Constitution, Article 38 establishes, in general terms, the right to the protection of personal data, leaving it to the ordinary legislature to define the relevant concepts and the conditions applicable to its processing.

Nevertheless, more than 20 years after the adoption of the Constitution, an adequate and effective personal data protection regime, suited to the country's circumstances, has yet to be implemented, despite this being a need that is widely felt and more than evident.

This legislative initiative seeks to establish the general legal framework for the protection of personal data. This Personal Data Protection Law was designed to safeguard the freedoms and fundamental rights of natural persons, while at the same time recognising the national interest in enabling the appropriate and effective use of such information to create new economic opportunities, provide more efficient public services, increase Timor-Leste's participation in the global economy and improve the quality of life of the Timorese people.

This Draft Law embodies the fundamental principles on data protection recognised internationally, rooted in multilateral conventions, regulatory frameworks and acknowledged best practices, which have since been incorporated into the legislative and regulatory instruments of various legal systems, including those of Portuguese-speaking countries with which Timor-Leste has close ties.

Considering that some of the measures whose adoption is deemed necessary fall within the reserved legislative competence of the National Parliament, notably in view of Article 95(2)(e) of the Constitution of the Democratic Republic of Timor-Leste, the Government submits this Draft Law to the National Parliament.

Under the proposed terms, the processing of personal data to which the Personal Data Protection Law applies must be carried out in strict respect for the personality rights of natural persons, in accordance with the requirements of good faith, and subject to the following guiding principles:

1. (Purpose) - Processing must be carried out for lawful, legitimate, specific and explicit purposes, communicated to the data subject in a timely manner, and no subsequent processing may be undertaken that is incompatible with those purposes;
2. (Necessity, suitability and proportionality) - Processing must be limited to what is necessary, suitable and proportionate to achieve its purposes, and must include only data that are relevant, proportionate and not excessive in relation to the purposes of the processing;
3. (Free access to information) - Data subjects have the right to obtain confirmation from the controller as to whether or not their data are being processed, as well as information concerning the categories of data processed and the purposes of the processing;
4. (Data quality and accuracy) - Having regard to the purpose of the processing, controllers and processors must take appropriate measures to ensure that personal data are accurate, including updating them where necessary;
5. (Transparency) - Data subjects have the right to receive, in an intelligible format, information about the processing and the identity of the respective controllers and processors, and such information must be provided in a format compatible with the usual manner of interaction with the data subject, without prejudice to any restrictions necessary to safeguard trade and industrial secrets;
6. (Security) - Controllers and processors must take technical and organisational measures to protect personal data against unauthorised access and against accidental or unlawful destruction, loss, alteration, disclosure or dissemination;

7. (Non-discrimination) - Personal data may not be processed for a purpose that is unlawful, abusive or discriminatory;
8. (Accountability) - Controllers and processors must adopt technical and organisational measures to ensure compliance with personal data protection rules and shall be held accountable in the event of non-compliance;
9. (Privacy and Security by Design) - Controllers and processors must comply with Article 11 of this Law and any other applicable security requirements from the design and development stage of any product or service.

Considering the need to ensure the immediate effectiveness of the framework, this Law directly establishes the National Data Protection Authority as an independent administrative body, endowed with functional independence and administrative and financial autonomy, and not subject to instructions from political authorities, the Government, regulated entities or any other public or private entity.

Implementation of the Law must be progressive and adapted to Timor-Leste's institutional circumstances, without suspending the essential protection of data subjects' rights. Accordingly, the Law establishes an initial phase of institutional establishment, public awareness, capacity-building and guidance, while maintaining from the outset mechanisms for supervision and response to situations of serious risk, unlawful processing, security breaches, improper interconnections, abusive processing of sensitive or biometric data, and unlawful international transfers.

Comparative experience shows that institutional adaptation can coexist with effective enforcement of the Law. This proposal therefore seeks to reconcile legislative simplicity, the protection of fundamental rights, trust in digital transformation, compatibility with international standards and practical implementation capacity in the Timorese context.

Accordingly, the Government submits to the National Parliament, pursuant to Article 97(1)(c) and Article 115(2)(a) of the Constitution, the following Draft Law:

S

DEMOCRATIC REPUBLIC OF TIMOR-LESTE

DRAFT LAW

No. _____ /_____

PERSONAL DATA PROTECTION LAW

The Constitution of the Democratic Republic of Timor-Leste, in force since 20 May 2002, proclaims Timor-Leste to be a democratic State governed by the rule of law, founded on the will of the people, respect for the dignity of the human person and the guarantee of fundamental rights, freedoms and safeguards.

Within the constitutional catalogue of fundamental rights, Article 38 enshrines the right to the protection of personal data, leaving to legislation the definition of the relevant concepts and the conditions applicable to its processing. More than two decades after the Constitution entered into force, the absence of a general and effective statutory framework for personal data protection has become a particularly significant regulatory gap from constitutional, institutional, economic and technological perspectives.

The need to legislate in this area is now of heightened importance. On the one hand, Article 38 of the Constitution must be given effective implementation. On the other hand, the digital transformation of the State, the modernisation of the Public Administration, interoperability between institutions, the development of digital identity systems, the digitisation of public records and the growing use of digital technologies require a clear and secure legal framework suited to national circumstances.

This Law therefore establishes the general legal framework for the protection of personal data, with the purpose of safeguarding the freedoms, fundamental rights and dignity of natural persons, without prejudice to the legitimate, responsible and secure use of information to provide more efficient public services, create new economic opportunities, strengthen digital trust, support Timor-Leste's participation in the regional and global economy and improve the quality of life of the Timorese people.

The protection of personal data should not be understood as an obstacle to innovation or digital transformation. On the contrary, it is an essential condition for such transformation to take place with trust, transparency, security and respect for citizens. Without adequate guarantees of privacy, security and accountability, it becomes more difficult to promote the legitimate sharing of information between institutions, develop integrated digital public services, secure citizens' acceptance of new technological solutions and consolidate a person-centred Public Administration.

This Law draws on internationally recognised principles of personal data protection embodied in multilateral conventions, regional instruments, comparative legislative frameworks and international best practices, including the experience of Portuguese-speaking countries, the European Union and ASEAN. Timor-Leste's accession to ASEAN also reinforces the importance of a national framework compatible with regional standards for digital trust, electronic commerce, personal data protection and secure cross-border data flows.

The processing of personal data covered by this Law must comply with the fundamental principles of lawfulness, fairness, good faith, transparency, specified purpose, minimisation, necessity, suitability, proportionality, accuracy, storage limitation, security, non-discrimination and accountability. These principles form the basis of a data protection culture focused on risk prevention, the protection of data subjects and the accountability of public and private entities that process personal data.

The Law recognises essential rights of data subjects, including the rights to information, access, rectification, erasure, not to be subject to decisions based solely on automated processing, and to lodge a complaint with the competent authority. At the same time, it establishes duties for controllers and processors, particularly in relation to security, documentation, confidentiality, the processing of sensitive data, the protection of minors, video surveillance, international transfers and the adoption of data protection measures by design and by default.

Considering the need to ensure the effectiveness of the framework, this Law establishes the National Data Protection Authority as an independent administrative body, endowed with functional independence and administrative and financial autonomy, and not subject to instructions from the Government, political

authorities, regulated entities or any other public or private entity. The establishment of this Authority is an essential condition for ensuring supervision, guidance, consistent application of the Law and the effective protection of data subjects' rights.

This Law also provides for supervisory mechanisms, corrective measures and a specific administrative offence regime, thereby ensuring that personal data protection is not confined to a statement of principles. The existence of proportionate legal consequences for non-compliance strengthens legal certainty, encourages compliance by public and private entities and helps consolidate citizens' trust in the processing of their personal data.

While recognising Timor-Leste's institutional circumstances, implementation of the Law must be progressive, proportionate and accompanied by public-awareness, capacity-building and technical-guidance measures. Such gradual implementation must not, however, suspend the essential protection of data subjects' rights, particularly in situations involving serious risk, the unlawful processing of sensitive or biometric data, security breaches, improper interconnections, abusive use of unique identifiers or unlawful international transfers.

Comparative experience shows that institutional adaptation can coexist with effective enforcement of the Law. This Law therefore seeks to reconcile legislative simplicity, the protection of fundamental rights, trust in digital transformation, compatibility with international standards and practical implementation capacity in the Timorese context.

Accordingly, the National Parliament enacts, pursuant to Article 38 and Article 95(1) of the Constitution of the Republic, to have the force of law, the following:

CHAPTER I
GENERAL PROVISIONS

Article 1
Purpose

1. This Law establishes the general framework for the protection of the personal data of natural persons.

Article 2
General principles

1. Personal data processing must be carried out in a manner that respects the principles governing the processing of personal data, the rights of the data subject and the obligations laid down in this Law.
2. The data subject must have access to clear, easily understandable, accessible and low-cost mechanisms enabling the exercise of his or her rights in accordance with the law.

Article 3
Definitions

1. For the purposes of this Law, the following definitions apply:
   a) ‘Anonymisation’ means the process of removing elements from personal data so that the data subject is no longer identified or identifiable
   b) ‘Anonymised data’ means personal data rendered anonymous in such a manner that the data subject is not or is no longer identified or identifiable;
   c) ‘NDPA’ means the National Data Protection Authority, an independent administrative body responsible for supervising the application of this Law;
   d) ‘Database’ or ‘Filing system’ means any structured set of information, in physical or electronic form, comprising personal data organised systematically so as to permit the retrieval of specific personal information;
   e) ‘Personal data’ means any information of any kind, irrespective of the medium in which it is held, including physical and electronic copies, sound and images, relating to a natural person (‘data subject’) and rendering that person identifiable;

f) ‘Sensitive data’ means personal data revealing religious or philosophical beliefs or positions, political opinions, political-party or trade-union membership, racial or ethnic origin, private life, information concerning health, sex life or sexual orientation, as well as genetic data, biometric data and data concerning disabilities of a physical, intellectual, mental, developmental or functional nature;

g) ‘Biometric data’ means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person which allow or confirm the unique identification of that natural person, including facial images or fingerprint data;

h) ‘Recipient’ means a natural or legal person, public authority, service or any other body or entity to which personal data are disclosed or made accessible;

i) ‘Establishment’ means a stable arrangement through which the controller or processor effectively and genuinely carries out an activity. The legal form of such an establishment, whether a branch or a subsidiary, is not decisive in this context;

j) ‘Identifiable’ means a natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name or identification number, location data, online identifiers, or one or more factors specific to his or her physical, physiological, genetic, mental, economic, cultural or social identity;

k) ‘Minor’ means a natural person under 17 years of age, without prejudice to the effects of emancipation under civil law;

l) ‘Pseudonymisation’ means the processing of personal data in such a manner that the data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures ensuring that the personal data cannot be attributed to an identified or identifiable natural person;

m) ‘Controller’ means a natural or legal person, public authority, service or any other body or entity which, alone or jointly with others, makes decisions concerning the processing of personal data;

n) ‘Processor’ means a natural or legal person, public authority, service or any other body or entity which processes personal data on behalf of and in accordance with the instructions of the controller;

o) ‘Data subject’ means an identified or identifiable natural person;

p) ‘Processing of personal data’ or ‘processing’ means any operation performed on personal data, by automated or non-automated means, such as access, consultation, collection, receipt, extraction, recording, organisation, structuring, classification, assessment, use, reproduction, comparison, interconnection, transmission, distribution, disclosure, transfer, publication, dissemination, processing, archiving, storage, retention, erasure, destruction, retrieval and alteration of information;

q) ‘Personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data subject to any form of processing.

Article 4

Scope of application

1. This Law applies to the processing of personal data carried out:

a) In the context of the activities of an establishment located within the national territory, regardless of whether the processing takes place within or outside that territory;

b) Outside the national territory, in places where Timorese law applies by virtue of public international law;

c) By a controller or processor not established within the national territory, in relation to the processing of personal data of a data subject who is in that territory, where the processing relates to:

i) The offering of goods or services to the data subject, irrespective of whether they are associated with consideration or payment; or

ii) The monitoring of the data subject's behaviour, insofar as that behaviour takes place within the national territory.

2. In the cases referred to in paragraph 1(c), the controller must, by notice to the NDPA, designate a representative established within the national territory to act on its behalf in the exercise of its rights and the fulfilment of its obligations, without prejudice to the controller's own responsibility.

Article 5

Exclusions

1. This Law does not apply to the processing of personal data carried out in any of the following situations:
   a) By a natural person in the course of exclusively personal or household activities;
   b) For exclusively journalistic purposes or for the purposes of artistic or literary expression;
   c) By a competent authority for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, without prejudice to Article 24;
   d) By a competent authority for the purposes of national defence and State security.
2. The processing of personal data referred to in paragraph 1(c) and (d) is subject to specific rules laid down in separate legislation; those rules must include the necessary, proportionate and appropriate measures to serve the public interest, having regard to the seriousness of the risk to the data subject, respect for the data subject's procedural safeguards and fundamental rights, and the rules contained in instruments of public international law binding on Timor-Leste.
3. Anonymised data are not considered personal data for the purposes of this Law, except where the anonymisation process to which the data have been subjected has been reversed, or where the data can be reversed through the application of reasonable efforts by the controller or a third party.

Article 6

National Data Protection Authority

1. The supervisory authority responsible for promoting, supervising and ensuring compliance with this Law is the National Data Protection Authority, hereinafter referred to as the NDPA.
2. The establishment, legal nature, composition, functions, competences, powers, guarantees of independence, financial arrangements and essential operating rules of the NDPA are governed by Chapter IV of this Law.

CHAPTER II

PROCESSING OF PERSONAL DATA IN GENERAL

Section I

Principles and obligations

Article 7

Principles relating to the processing of personal data

1. Personal data must be:
   a) Processed lawfully, legitimately, fairly and transparently ('principle of lawfulness, fairness and transparency');
   b) Collected for specified, explicit and legitimate purposes and not subsequently processed in a manner incompatible with those purposes ('principle of purpose limitation');
   c) Adequate, relevant and limited to the minimum necessary for the purposes for which they are processed ('principle of data minimisation');
   d) Accurate and kept up to date where necessary, and appropriate measures must be taken to ensure that inaccurate or incomplete data are erased or rectified without delay, having regard to the purposes for which they are processed ('principle of accuracy');
   e) Kept in a form permitting identification of the data subject only for as long as is necessary for the purposes for which they are processed ('principle of storage limitation').

2. The controller is responsible for ensuring compliance with the preceding paragraphs ('principle of accountability').

Article 8

Conditions for lawful processing

1. Personal data may be processed only where at least one of the following conditions applies:
   a) The data subject has validly given consent;
   b) Processing is necessary for compliance with a legal or regulatory obligation to which the controller is subject;
   c) Processing is necessary for the performance of a contract to which the data subject is party or in order to take pre-contractual steps at the data subject's request;
   d) Processing is necessary to prevent fraud or protect the security of the data subject in the context of verifying the data subject's identity before responding to a request from him or her;
   e) Processing is necessary for the proper exercise of rights in judicial, administrative or arbitration proceedings or other forms of alternative dispute resolution;
   f) Processing is necessary to protect the vital interests of the data subject or another natural person;
   g) Processing is necessary for medical or health purposes and is carried out by a health professional or healthcare provider;
   h) Processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party, except where those interests are overridden by the fundamental rights and freedoms of the data subject requiring the protection of personal data; or
   i) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
2. The processing of personal data pursuant to paragraph 1(i) is governed by specific legislation, which must provide measures to safeguard the public interest while respecting the procedural safeguards and fundamental rights of the data subject; for this purpose, the NDPA shall issue recommendations or technical opinions.

Article 9

Consent

1. The data subject's consent is valid where it consists of a freely given, specific and informed indication of wishes by which the data subject agrees, through a statement or clear affirmative action, to the processing of his or her personal data.
2. Consent is considered informed where the data subject has received the following information in a readily intelligible format compatible with the manner of interaction with the controller, including, where applicable, by electronic means:
   a) The identity and postal or email address of the controller and, where applicable, the representative designated by the controller;
   b) The categories of personal data processed;
   c) The specific purposes of the processing, any general indication of willingness to permit the processing of personal data being null and void;
   d) The methods used to collect the information;
   e) The intended recipients or categories of recipients, where the information is transmitted to a third party; and
   f) The existence of, and conditions for exercising, the rights of access, rectification and erasure, unless an exception provided by law applies.
3. The information referred to in the preceding paragraph shall be provided to the data subject at the time the personal data are collected, but may also be provided within a reasonable period thereafter where it is demonstrated that:
   a) The other requirements for consent, in particular freedom of choice, are satisfied; and

b) Providing the information at the time of collection is impossible or would involve a disproportionate effort.

4. Consent shall be given in writing or by other means capable of demonstrating an unambiguous indication of the data subject's wishes.
5. Where the data subject's consent is given in the context of a written declaration that also concerns other matters, the request for consent must be presented in a manner that clearly distinguishes it from those other matters.
6. Consent does not constitute a valid basis for the processing of personal data by a public entity where, owing to the nature of the relationship between the data subject and the public entity, there is no genuine freedom of choice, or where processing is necessary for compliance with a legal obligation, the performance of a task carried out in the public interest or the exercise of official authority.

Article 10

Withdrawal of consent

1. The data subject may freely withdraw consent by notifying the controller; however, processing carried out in the meantime on the basis of the consent previously given remains valid.
2. Withdrawal of consent must not entail any cost for the data subject, and the controller may not charge any amount for complying with the data subject's request.
3. Where the purpose of processing changes in a manner incompatible with the purpose referred to in Article 9(2)(c), the controller must inform the data subject of that change before further processing, and the data subject may refuse to consent to the new purpose.

Article 11

General data protection measures

1. The controller and processor must implement technical and organisational measures, such as pseudonymisation, ensuring an appropriate level of personal data protection, having regard to the likelihood and severity of the risks posed by the processing of personal data and the context in which it is carried out.
2. The measures referred to in the preceding paragraph must:
   a) Protect personal data against any unauthorised access, destruction, loss, alteration, accidental or unlawful disclosure, or any form of improper or unlawful processing, particularly where processing involves the transmission of data over a network;
   b) Take account of the physical security of the data;
   c) Ensure that, by design and by default, only personal data necessary for each specific purpose of processing are processed, having regard in particular to the amount of personal data collected, the extent of processing, the storage period and accessibility; and
   d) Provide mechanisms enabling the controller or processor to detect, prevent and respond to attacks, intrusions and other security failures.
3. Where a product or service is offered or provided, the controller and processor must comply with the preceding paragraphs from the design stage of the product or service.
4. The controller must require the processor and any third party to which personal data are transferred to notify the controller immediately upon becoming aware of a personal data breach and to take immediate measures to remedy, or otherwise respond to, the security failure that caused the breach.
5. The NDPA may establish minimum technical standards for the measures referred to in this Article, taking into account the nature of the personal data, the characteristics of the processing and the current state of technology; such standards may include specific measures for the processing of sensitive personal data.
6. Having regard to the nature of the entities responsible for processing and the premises in which processing is carried out, the NDPA may waive certain technical and organisational measures, provided that respect for the fundamental rights of the data subject is demonstrated.
7. Compliance with codes of conduct and certifications approved by the NDPA may be used as evidence of compliance with the obligations laid down in this Article.

Article 12

Specific measures for storage, erasure and retention

1. Personal data must be retained only for as long as necessary for the purposes underlying their collection and processing, without prejudice to other statutory provisions or authorisation granted by the NDPA.
2. Personal data must be securely erased.
3. In determining the method of secure erasure, the controller must take into account at least the nature and sensitivity of the data and the context in which they are processed.
4. Within the scope and technical limits of the processing activities, personal data shall be erased once their processing has been completed, without prejudice to the following paragraph.
5. Storage of data after completion of processing is permitted for the following purposes:
   a) Compliance with a legal or regulatory obligation imposed on the controller;
   b) Archiving in the public interest, scientific or historical research purposes, or statistical purposes, under the terms defined by the NDPA;
   c) Transfer to a third party, provided that the requirements applicable to data processing under this Law are met; or
   d) Exclusive use by the controller, with access by third parties prohibited, provided that technical and organisational measures restricting access to the data, including anonymisation, have been adopted.

Article 13

Processing on behalf of a controller

1. The controller is responsible for ensuring compliance with this Law.
2. Where processing is carried out on behalf of the controller, the controller must select a processor providing sufficient guarantees that appropriate technical and organisational measures will be implemented, and must monitor compliance with those measures.
3. Processing operations carried out on behalf of a controller shall be governed by a written contract or other equivalent legal instrument binding the processor in relation to the controller and stipulating, in particular, that the processor acts only on the controller's instructions, the subject matter and duration of the processing, the nature and purpose of the processing, the categories of personal data processed, the obligations and rights of the controller, the conditions governing the engagement of sub-processors, the procedure to be followed in the event of a personal data breach, and the processor's obligation to adopt appropriate technical and organisational measures.
4. The controller must require any processor or third party acting on its behalf to inform it of any inaccurate or incomplete data of which that processor or third party becomes aware.
5. Any person acting under the authority of the controller or processor, including the processor itself, who has access to personal data may not process those data except on instructions from the controller, unless required to do so by law.
6. The controller may delegate to the processor the fulfilment of the obligations arising under Chapters II and III of this Law, without prejudice to the controller's own responsibility.

Article 14

Transfers of data to third countries or international organisations

1. In addition to the other requirements applicable to the processing of personal data under this Law, the controller may transfer personal data to a third country or international organisation only:
   a) Where the NDPA has declared, by decision, that the third country or international organisation ensures an adequate level of protection;
   b) With the explicit consent of the data subject;
   c) Under contractual clauses stipulating technical and organisational measures that ensure an adequate level of protection for the personal data transferred;

d) On the basis of binding rules applicable to multinational corporate groups, stipulating technical and organisational measures to be implemented by all entities within the group so as to ensure an adequate level of protection for personal data, and which must be observed by all those entities; or

e) In accordance with codes of conduct, certifications, marks, seals or personal data protection standards relating to transfer mechanisms that establish adequate levels of protection.

2. Without prejudice to specific guidance issued by the NDPA, the adequacy of the level of protection shall be assessed in light of all the circumstances surrounding the data transfer, in particular the nature of the data, the purpose and duration of the intended processing operation or operations, the general or sector-specific rules of law in force in the countries of origin and final destination, and the professional rules and security measures observed in the country or international organisation concerned.

Section II

Rights of the data subject

Article 15

Right of access

1. The data subject has the right to obtain from the controller, free of charge, confirmation as to whether or not personal data concerning him or her are being processed and, where processing is confirmed, access to the personal data and information concerning:

a) The specific purposes of the processing;

b) The categories of personal data concerned;

c) The type and duration of the processing;

d) The recipients or categories of recipients of the data;

e) The identity of the controller;

f) The contact details of the controller and of the representative designated by it, where applicable;

g) The existence of, and conditions for exercising, the data subject's rights under this Law, with explicit reference to the right to lodge a complaint with the NDPA and the rights of access, rectification and erasure.

2. At reasonable intervals, the data subject may send the controller a request for confirmation and information by submitting a data access request.

3. Upon receiving a request from the data subject, the controller must verify the identity of the applicant and then respond without undue constraint or delay.

4. Where neither the controller nor its processors hold personal data concerning the data subject, the controller shall, where possible, inform the data subject of the identity of the correct controller and/or processor.

5. Without prejudice to the preceding paragraph, the controller may refuse the data subject's request where:

a) Disclosure of the information would violate the law or a court order;

b) Having regard to the sensitivity of the data, the burden or cost of disclosing the information would be unreasonable or disproportionate to the risks to the data subject;

c) The request is made repetitively or in bad faith; or

d) Disclosure of the information would prejudice the rights and interests of third parties other than the data subject, including by compromising data security or trade and industrial secrets.

6. The controller must ensure that the data subject is informed without undue delay of the reasons for any refusal and of the possibility of lodging a complaint with the NDPA.

Article 16

Right to rectification

1. Having regard to the purposes of processing, the controller and processor must take all appropriate measures to ensure the accuracy of the data, and inaccurate or incomplete data shall be rectified or updated where necessary.

2. At reasonable intervals, the data subject may request the controller to correct inaccuracies and, having regard to the purposes of processing, may request that incomplete personal data be completed.
3. Where inaccurate or incomplete information affects the purpose of the processing, the controller must communicate any rectification of personal data to each processor and third party to which the personal data have been transmitted.
4. The processor must inform the controller of any inaccuracies and corrections of which it becomes aware.
5. Upon receiving a request for rectification, the controller must verify the identity of the applicant and respond in a timely manner and free of charge to the data subject.
6. Where the controller or its processors process data concerning the data subject, the controller shall ensure that any inaccuracies are corrected, except where:
   a) The benefits of not altering the personal data outweigh the likelihood and severity of the risks posed to the data subject, having regard to the sensitivity of the data processed;
   b) Rectification would violate the law or a court order; or
   c) The burden or cost of correction would be unreasonable or disproportionate to the risks to the data subject.

Article 17

Right to erasure

1. The data subject has the right to require the controller, free of charge and without undue delay, to erase personal data concerning him or her where one of the following applies:
   a) The personal data are no longer necessary for the purpose for which they were collected or subsequently processed;
   b) The data subject withdraws consent in accordance with this Law and there is no other lawful basis for processing those data;
   c) The personal data have been unlawfully processed; or
   d) The personal data must be erased in compliance with a legal or regulatory provision to which the controller is subject.
2. Upon receipt of a request for erasure, the controller must erase the data without undue delay, except to the extent that processing is necessary for:
   a) Exercising the right to freedom of expression and information;
   b) Compliance with a legal or regulatory provision to which the controller is subject;
   c) Performance of a task carried out in the public interest, particularly in the field of public health, as permitted under this Law or another legal or regulatory provision;
   d) Archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, where erasure is likely to render impossible or seriously impair achievement of the objectives of that processing; or
   e) The establishment, exercise or defence of legal claims.

Article 18

Right not to be subject to individual automated decision-making

1. Every person has the right not to be subject to a decision producing legal effects concerning him or her or similarly significantly affecting him or her, where that decision is based solely on automated processing intended to evaluate certain aspects of his or her personality, including professional capacity, creditworthiness, reliability or behaviour.
2. Without prejudice to compliance with the other provisions of this Law, paragraph 1 does not apply where the decision:
   a) Is based on the data subject's consent;
   b) Is necessary for entering into or performing a contract between the data subject and a controller; or
   c) Is authorised by law.

3. In the cases referred to in paragraph 2, appropriate measures must be adopted to safeguard the data subject's rights and legitimate interests and to enable the data subject's point of view to be expressed and taken into account.
4. A decision referred to in paragraph 1 may also be permitted where authorised by the NDPA, provided that appropriate measures are taken to safeguard the data subject's rights and legitimate interests.

Article 19

Right to lodge a complaint with the NDPA

1. Without prejudice to any other remedy, every data subject has the right to lodge a complaint with the NDPA where he or she considers that the processing of his or her personal data infringes this Law.
2. The mechanisms for exercising the right referred to in the preceding paragraph shall be defined by a regulation, decision or form approved by the NDPA.

CHAPTER III

PROVISIONS RELATING TO SPECIFIC PROCESSING SITUATIONS

Article 20

Processing of sensitive personal data

1. The processing of sensitive personal data is prohibited unless the data subject has given explicit consent or the processing is considered necessary:
   a) For compliance with a legal or regulatory obligation to which the controller is subject;
   b) For the performance of a contract to which the data subject is party or in order to take pre-contractual steps at the data subject's request;
   c) To prevent fraud or protect the security of the data subject in the context of verifying the data subject's identity before responding to a request from him or her;
   d) For the proper exercise of rights in judicial, administrative or arbitration proceedings or other forms of alternative dispute resolution;
   e) To protect the vital interests of the data subject or a third party where the data subject is physically or legally incapable of giving consent;
   f) For medical or health purposes, where carried out by a health professional subject to professional secrecy or by a healthcare provider;
   g) For the purposes of the legitimate interests pursued by the controller or a third party, except where those interests are overridden by the fundamental rights and freedoms of the data subject requiring the protection of personal data; or
   h) For reasons of substantial public interest, in particular the protection of State security, the safeguarding of public security and public health, including protection against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices.
2. The processing of personal data pursuant to paragraph 1(h) is governed by specific legislation, which must identify and provide measures to safeguard the substantial public interest concerned while respecting the procedural safeguards and fundamental rights of the data subject; for this purpose, the NDPA shall issue recommendations or technical opinions.
3. The processing of sensitive data is also permitted where it concerns data manifestly made public by the data subject, provided that the data subject has given explicit consent to their processing.
4. In all cases, the processing of sensitive data must include safeguards against discrimination of natural persons and incorporate appropriate and specific measures to protect the fundamental rights of the data subject.

Article 21

Processing of a minor's personal data

1. The processing of personal data relating to a minor must take the minor's best interests into account, in accordance with national child-protection legislation.
2. Where the processing of personal data relating to a non-emancipated minor is based on consent, that consent is valid only if given by the minor's legal representative or by the person exercising parental responsibility, without prejudice to hearing the minor where this is appropriate having regard to the minor's age and maturity.
3. In the cases referred to in paragraph 2, the controller must make reasonable efforts, having regard to the available means, to verify the age and identity of the person giving consent and that person's authority to do so.
4. The information referred to in Article 9(2), where it concerns the processing of a minor's personal data, must be provided to the person exercising parental responsibility in a simple, comprehensible and accessible manner, also taking into account the minor's physical and motor, perceptual, sensory, intellectual and mental characteristics, and using audiovisual resources where appropriate.
5. A controller processing minors' personal data must make public information concerning the types of data collected, the manner in which they are used and the procedures for exercising the data subject's rights under this Law.

Article 22

Video surveillance

1. Without prejudice to specific legal provisions governing its use, particularly for reasons of public security, video-surveillance systems intended to protect persons and property must comply with the requirements and limits set out in the following paragraph.
2. Cameras may not cover:
   a) Public roads, adjoining properties or other places not under the exclusive control of the controller, except to the extent strictly necessary to cover access points to the premises;
   b) The area used to enter a personal code or PIN at automated teller machines, electronic payment terminals or equivalent equipment;
   c) The interior of areas reserved for customers or users where their intimacy and privacy must be respected, including sanitary facilities, waiting areas and fitting rooms;
   d) The interior of areas reserved for workers, including changing rooms, sanitary facilities and areas used exclusively for rest.
3. In education and training establishments, video-surveillance cameras may cover only external perimeters and access points, as well as areas containing property and equipment requiring special protection, such as laboratories or computer rooms.
4. In employment relationships, recorded images and other personal data captured through video systems or other technological means of remote surveillance may be used only in criminal or administrative offence proceedings or for the purpose of determining disciplinary liability.
5. Where video surveillance is permitted, the recording of sound is prohibited, except during periods when the monitored premises are closed or where authorised by the NDPA.
6. Images collected through video-surveillance systems must be retained only for the period strictly necessary for the purpose justifying their collection, without prejudice to retention where they are required as evidence in criminal, administrative offence, disciplinary, administrative or judicial proceedings.
7. The NDPA may define, by regulation, decision or general guidance, maximum image-retention periods and requirements concerning access, extraction, disclosure, logging of operations and secure destruction, having regard to the purpose of the system, the risk to data subjects and the nature of the monitored location.

8. Access to images must be limited to expressly authorised persons, in the number strictly necessary, and shall be subject to a duty of confidentiality, access logging and appropriate technical and organisational measures.

Article 23

Processing of personal data for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes

1. Without prejudice to the provisions of this Law, the rules applicable to the processing of data for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, and to their retention for those purposes, shall be further developed in guidance issued by the NDPA.

Article 24

Records of unlawful activities, criminal convictions, security measures, offences and administrative offences

1. Central records concerning persons suspected, accused or convicted of unlawful activities, criminal offences or administrative offences, and persons subject to decisions imposing penalties, fines, security measures, administrative fines or ancillary sanctions, may be created and maintained only by public entities vested by law with such competence and in compliance with the procedural, security and data-protection rules laid down in this Law and in specific legislation subject to the prior opinion of the NDPA.
2. The processing of personal data relating to persons suspected, accused or convicted of unlawful activities, criminal offences or administrative offences, or subject to decisions imposing penalties, fines, security measures, administrative fines or ancillary sanctions, is permitted provided that:
   a) The processing is necessary for the pursuit of the controller's legitimate purposes;
   b) The fundamental rights of the data subject are respected; and
   c) The data-protection and information-security rules laid down in this Law and in specific legislation subject to the prior opinion of the NDPA are observed.

CHAPTER IV

NATIONAL DATA PROTECTION AUTHORITY

Article 25

Establishment and legal nature

1. The National Data Protection Authority, hereinafter referred to as the NDPA, is hereby established as an independent administrative body responsible for promoting, supervising and ensuring compliance with this Law.
2. The NDPA is a legal person governed by public law, vested with public-authority powers, functional independence and administrative, financial and asset-management autonomy, and shall have its own assets and budget.
3. The NDPA shall have its headquarters in _____ and shall exercise its functions throughout the national territory, subject exclusively to the Constitution and the law.
4. The NDPA shall have the legal nature, composition, functions, competences, powers, guarantees of independence, basic organisation, financial arrangements and operating mechanisms provided for in this Law.
5. The NDPA may adopt regulations, decisions, guidance, recommendations, forms and codes of good practice intended to give practical effect to this Law, under the terms set out herein.
6. The establishment and operation of the NDPA shall not depend on subsequent legislation, without prejudice to the adoption of its internal rules of procedure and the measures necessary for its administrative and financial installation.

Article 26

Independence

1. The NDPA shall perform its functions independently and impartially and shall be subject exclusively to the Constitution and the law.
2. Members of its bodies, staff, consultants and collaborators may neither seek nor receive instructions from any public or private entity concerning the merits of decisions, recommendations, opinions, inspections or ongoing proceedings.
3. Regulations, decisions and other acts of the NDPA producing external effects may be challenged before the competent courts in accordance with the general rules.

Article 27

Functions and powers

1. The NDPA shall be responsible, in particular, for:
   a) Supervising and promoting compliance with this Law;
   b) Receiving, examining and deciding complaints lodged by data subjects;
   c) Issuing opinions, recommendations, guidance, decisions and codes of good practice;
   d) Approving model notices for data subjects, personal data breach notification forms and other instruments for the practical application of this Law;
   e) Carrying out inspections and audits and requesting information from public and private entities;
   f) Ordering corrective measures necessary to bring processing operations into compliance with this Law;
   g) Ordering the restriction, suspension or cessation of unlawful processing;
   h) Ordering the rectification, erasure, restriction or blocking of personal data where required by law;
   i) Suspending international data transfers that infringe this Law;
   j) Imposing administrative fines and ancillary sanctions in accordance with this Law;
   k) Issuing prior opinions on high-risk processing, public-sector interoperability, unique identifiers, biometrics, video surveillance and public digital platforms;
   l) Cooperating with foreign authorities and international organisations in the field of data protection;
   m) Promoting training, public-awareness and outreach activities for public entities, private entities and citizens;
   n) Submitting an annual report to the National Parliament on its activities, the state of personal data protection in Timor-Leste and any necessary legislative or administrative recommendations.
2. In exercising its powers, the NDPA must act proportionately and, where appropriate, give priority to guidance, recommendations and corrective action before imposing more severe sanctions, without prejudice to the effective punishment of serious and very serious offences.

Article 28

Regulatory powers of the NDPA

1. The NDPA may adopt regulations, decisions, guidance, recommendations, forms and codes of good practice intended to give practical effect to this Law, particularly in technical, procedural, sector-specific or high-risk matters.
2. The power referred to in the preceding paragraph covers, in particular, processing security, retention periods, video surveillance, exercise of data subjects' rights, personal data breach notification, impact assessments, processing on behalf of a controller, international transfers, public-sector interoperability, unique identifiers and data processing in specific sectors.
3. Acts of the NDPA may not create new restrictions on fundamental rights or establish offences, sanctions or essential obligations without a sufficient statutory basis, and must be limited to giving practical effect to and ensuring the proper implementation of this Law.
4. Regulations and decisions of general application adopted by the NDPA shall be officially published and, where appropriate, preceded by public consultation.

Article 29

Composition

1. The NDPA shall be governed by a Governing Board composed of three members, including a Chairperson.
2. Two members of the Governing Board, including the Chairperson, shall be elected by the National Parliament by an absolute majority of the Members of Parliament in office.
3. One member of the Governing Board shall be appointed by the Government by resolution of the Council of Ministers.
4. Members of the Governing Board shall be selected from among persons of recognised integrity, independence and technical, legal or institutional expertise in fundamental rights, data protection, digital technologies, public administration, regulation or governance.
5. Members of the Governing Board shall serve a five-year term, renewable once.
6. Members of the Governing Board shall perform their duties independently and impartially, with a level of commitment appropriate to the nature of their functions, and shall not be subject to instructions from the National Parliament, the Government, regulated entities or any other public or private entity.
7. The Chairperson shall represent the NDPA, convene and chair meetings of the Governing Board, coordinate its work and exercise the other powers provided for in this Law and the internal rules of procedure.

Article 30

Incompatibilities, disqualifications and termination of office

1. Members of the Governing Board may not hold government office, leadership positions in political parties, management positions in entities subject to supervision by the NDPA, or engage in any activity liable to compromise their independence or impartiality.
2. Members of the Governing Board are subject to duties of secrecy, discretion, impartiality, independence and prevention of conflicts of interest.
3. Members of the Governing Board may not be removed before the end of their term except in the event of resignation, death, permanent incapacity, a subsequently arising incompatibility, conviction for an intentional criminal offence, or serious breach of the duties of office.
4. Early termination of office must be reasoned and decided by the entity competent for the relevant election or appointment, in accordance with this Law.

Article 31

Internal rules of procedure of the NDPA

1. The internal rules of procedure shall establish, in particular:
   a) The internal organisation of the services;
   b) The operating rules of the Governing Board;
   c) The internal allocation of cases;
   d) Procedures for public service, complaints, supervision, opinions, guidance, decisions and administrative offence proceedings;
   e) Rules on administrative processing, archives, electronic case management and notifications;
   f) Internal rules on information security, confidentiality, secrecy and access control;
   g) Mechanisms for preventing conflicts of interest;
   h) Internal models for case management, complaints, personal data breach notification and communication with data subjects and controllers.
2. The internal rules of procedure may not limit the rights of data subjects, restrict the powers of the NDPA, create offences or sanctions, alter statutory time limits, modify safeguards for the defence or judicial challenge, or establish essential obligations without a basis in this Law.
3. The internal rules of procedure shall be officially published and made available to the public in an accessible format.

Article 32

Services, staff and budget

1. The NDPA shall have its own services, comprising the technical, legal, administrative and information-technology staff necessary for the performance of its functions.
2. Pending approval of its staffing structure, the NDPA may operate with staff recruited under contract, mobility, secondment, requisition or temporary assignment from public entities, without prejudice to its functional independence.
3. NDPA staff are subject to special duties of secrecy, confidentiality, impartiality and protection of the information to which they have access.
4. The NDPA shall have its own budget, entered as an appropriation in the General State Budget sufficient to ensure its functional independence and effective operational capacity.
5. The NDPA may receive technical support, training, international cooperation and assistance from development partners, provided that such support does not compromise its independence.

Article 33

Duty to cooperate

1. Public and private entities must cooperate with the NDPA by providing the information, documents, explanations and access necessary for the exercise of its powers.
2. The duty to cooperate is without prejudice to legally protected professional secrecy, secrecy of judicial proceedings, the confidentiality of lawyer-client communications and other applicable procedural safeguards.
3. Unjustified refusal to cooperate with the NDPA constitutes an offence under this Law.

Article 34

Annual report

1. By 31 March of each year, the NDPA shall submit to the National Parliament a report on its activities during the preceding year.
2. The report must include, in particular, complaints received, decisions adopted, opinions issued, the principal risks identified, supervisory measures carried out, legislative or administrative recommendations, and an assessment of the state of personal data protection in Timor-Leste.
3. The report shall be published and made available to the public in an accessible format, without prejudice to the protection of confidential information, legally protected secrecy or personal data.

CHAPTER V

SUPERVISION, LIABILITY AND ADMINISTRATIVE OFFENCES

Article 35

Competence of the NDPA

1. The NDPA is responsible for supervising compliance with this Law and for initiating, investigating and deciding administrative offence proceedings concerning the infringements provided for herein.
2. Decisions in administrative offence proceedings shall be taken by the governing body of the NDPA.
3. In exercising its powers, the NDPA may request from public or private entities any necessary information, documents, records and explanations.
4. Public and private entities must cooperate with the NDPA, without prejudice to legally protected professional secrecy, secrecy of judicial proceedings, the confidentiality of lawyer-client communications and other legally applicable safeguards.
5. Whenever the facts established may constitute a criminal offence, the NDPA shall report them to the Public Prosecution Service and transmit the relevant material in its possession, without prejudice to continuation of the administrative offence proceedings where legally permissible.

Article 36

Corrective measures

1. Without prejudice to the imposition of an administrative fine or other legal consequences, the NDPA may order the measures necessary to bring data processing into compliance with this Law.
2. The NDPA may, in particular:
   a) Issue a warning or recommendation;
   b) Issue a reprimand to the controller or processor;
   c) Order processing to be brought into compliance with the Law within a specified period;
   d) Order the rectification, erasure, restriction or blocking of personal data;
   e) Order the temporary or permanent suspension of a particular processing operation;
   f) Suspend international data transfers;
   g) Suspend data interconnection, interoperability or sharing;
   h) Require the adoption of appropriate technical and organisational measures;
   i) Order notification of a personal data breach to the data subject where required by law.
3. Corrective measures must be appropriate and proportionate to the seriousness of the situation, the risk to data subjects, the number of persons affected, the type of data involved and the conduct of the responsible entity.
4. Where there is a serious and imminent risk to data subjects' rights, the NDPA may order urgent measures before the final decision, provided that it states the reasons for the urgency and limits the measure to what is strictly necessary.

Article 37

Minor administrative offences

1. The following constitutes a minor administrative offence:
   a) Providing incomplete, unclear or insufficiently accessible information to the data subject, where no essential information has been omitted and no material risk to the data subject's rights results;
   b) Responding late to a request to exercise the data subject's rights, where the delay is not significant, does not amount to an unjustified refusal and causes no material harm to the data subject;
   c) Failing to update contact details, privacy notices, internal records or other formal information required by this Law, where that omission does not create a material risk for data subjects;
   d) Failing to keep organised documentation demonstrating compliance with this Law, where the omission is merely formal and does not prevent supervision by the NDPA.

Article 38

Serious administrative offences

1. The following constitutes a serious administrative offence:
   a) Processing personal data without a lawful basis provided for in this Law;
   b) Collecting personal data for purposes that are unspecified, not explicit or incompatible with the purposes communicated to the data subject;
   c) Collecting or retaining personal data that are manifestly excessive, unnecessary or disproportionate to the purpose of the processing;
   d) Retaining personal data for longer than necessary or legally permitted, without a legitimate basis for retention;
   e) Using inaccurate, incomplete or outdated personal data where the controller knows or ought to know of the inaccuracy and material harm to the data subject may result;
   f) Omitting essential information to the data subject concerning the identity of the controller, the purposes of processing, the recipients of the data or the rights available to the data subject;

g) Unjustifiably or repeatedly refusing the exercise of the rights of access, rectification, erasure, objection, restriction or any other rights recognised by this Law;

h) Breaching the duty to ensure the security of processing where this creates a material risk of unauthorised access, loss, alteration, improper disclosure or abusive use of personal data;

i) Failing to notify a personal data breach to the NDPA where required by law;

j) Failing to communicate a personal data breach to the data subject where required by law;

k) A processor carrying out processing without a written contract or equivalent legal instrument defining the instructions, responsibilities and safeguards required by this Law;

l) Transferring personal data internationally without an adequacy decision, valid consent, appropriate contractual clauses, binding rules, certification, code of conduct or another mechanism permitted by this Law;

m) Using a video-surveillance system in breach of the limits laid down in this Law, particularly as regards the areas covered, access to images, sound recording, retention or disclosure of recordings;

n) Failing to conduct an impact assessment or prior consultation with the NDPA where required by law for high-risk processing;

o) Failing to designate a data protection officer or focal point where required by law;

p) Unjustifiably refusing to provide information, documents, records or explanations requested by the NDPA in the exercise of its powers;

q) Failing to comply with a corrective measure, order or decision issued by the NDPA under this Law.

Article 39

Very serious administrative offences

1. The following constitutes a very serious administrative offence:

a) Processing sensitive data outside the cases permitted by this Law where that processing creates a high risk to the rights, freedoms and safeguards of data subjects;

b) Processing biometric data for the unique identification of a natural person without a sufficient legal basis, valid consent where required, or appropriate technical and organisational safeguards, where that processing creates a high risk to data subjects;

c) Processing personal data relating to minors in breach of the rules laid down in this Law where that processing creates a high risk to their rights, freedoms and safeguards;

d) Creating, interconnecting or using public or private databases without a legal basis or appropriate safeguards where this enables large-scale access to, matching of or profiling based on personal data;

e) Using a unique identifier as a universal key for indiscriminate access to, matching of or interconnection between databases outside the cases permitted by law;

f) Unlawfully communicating, disclosing, selling, making available or transferring personal data to third parties where done intentionally or where sensitive data, biometric data, minors' data or large-scale data are involved;

g) A personal data breach resulting from a serious failure to implement security measures, where it causes or is likely to cause a high risk to the rights, freedoms and safeguards of data subjects;

h) Intentionally concealing a personal data breach, unlawful processing or improper disclosure of data where there is a legal duty to notify the NDPA or the data subject;

i) Unlawfully transferring sensitive data, biometric data, data relating to minors or large-scale personal data internationally without any appropriate safeguard under this Law;

j) Using personal data for discriminatory, persecutory or abusive purposes, or for purposes incompatible with the dignity of the human person;

k) Destroying, altering, concealing or falsifying documents, records, logs, contracts, authorisations or other material relevant to supervision by the NDPA;

l) Seriously obstructing the NDPA's supervisory functions, particularly through repeated refusal to cooperate, preventing access to information legally required or repeatedly failing to comply with the Authority's orders;

m) Failing to comply with an urgent or interim measure ordered by the NDPA to prevent a serious and imminent risk to data subjects' rights.

2. For the purposes of this Article, a high risk is deemed to exist, in particular, where processing is likely to cause discrimination, identity theft, material pecuniary or non-pecuniary harm, unlawful public exposure, breach of the confidentiality of sensitive data, significant harm to minors, improper restriction of rights or another serious impact on the rights, freedoms and safeguards of data subjects.

Article 40

Administrative fines

1. Minor administrative offences are punishable by a fine of between 100 and 2,500 United States dollars for a natural person and between 250 and 10,000 United States dollars for a legal person.
2. Serious administrative offences are punishable by a fine of between 500 and 10,000 United States dollars for a natural person and between 1,000 and 50,000 United States dollars for a legal person.
3. Very serious administrative offences are punishable by a fine of between 1,000 and 25,000 United States dollars for a natural person and between 5,000 and 150,000 United States dollars for a legal person.
4. Offences committed negligently are punishable, with the minimum and maximum fine amounts reduced by half.
5. Where the offender is a microenterprise, small entity, non-profit association or small public entity, and the offence is minor or results from negligence without material harm to data subjects, the NDPA must give priority to a warning, recommendation or compliance order before imposing a fine, except in cases of repeated offending, intent, refusal to cooperate or significant risk to data subjects' rights.
6. Payment of the fine does not release the offender from compliance with omitted duties or from adopting corrective measures ordered by the NDPA.

Article 41

Ancillary sanctions

1. Depending on the seriousness of the offence, the following ancillary sanctions may be imposed:

a) Publication of the sanctioning decision;

b) Temporary suspension of a processing activity, operation, system or international transfer;

c) Temporary prohibition on processing specified categories of data;

d) An obligation to adopt a compliance plan;

e) An obligation to undergo an independent audit;

f) Suspension of a certification, authorisation, seal, code of conduct or instrument recognised by the NDPA.

2. Ancillary sanctions must be appropriate and proportionate to the seriousness of the offence and the risk to data subjects.
3. Publication of the sanctioning decision must protect third parties' personal data, professional secrecy, trade secrets and other legally protected information.

Article 42

Criteria for imposing sanctions

1. In determining the fine and ancillary sanctions, the NDPA shall take into account, in particular:

a) The nature, seriousness and duration of the offence;

b) The number of data subjects affected;

c) The type, volume and sensitivity of the data involved;

d) Whether the offence was intentional or negligent;

e) The offender's financial capacity;

f) The cooperation provided to the NDPA;

g) Repeated offending;

h) Measures adopted to prevent, stop or remedy the harm;

i) The economic benefit obtained or expected from the offence;

j) The degree to which public trust and data subjects' rights were affected.

Article 43

Right to be heard and right of defence

1. No administrative fine or ancillary sanction may be imposed unless the defendant has first been notified of the alleged offence and given an opportunity to exercise the right of defence.
2. The notification must contain:

   a) The identity of the defendant;

   b) A description of the alleged facts;

   c) Identification of the provisions infringed;

   d) Classification of the offence as minor, serious or very serious;

   e) The sanctions potentially applicable;

   f) The evidence contained in the case file;

   g) The time limit for submitting a defence.
3. The defendant shall have 30 working days to submit a written defence, attach documents and request the taking of evidence.
4. In particularly complex cases, the period referred to in the preceding paragraph may be extended by the NDPA, upon a reasoned request, for no more than 30 working days.
5. The defendant may be assisted by a lawyer or defence counsel and may inspect the case file, without prejudice to the protection of third parties' personal data, confidential information, professional secrecy, trade secrets, secrecy of judicial proceedings and other legally protected interests.

Article 44

Evidence and decision

1. The NDPA may take any evidentiary measures necessary to establish the truth and ensure a proper decision in the proceedings.
2. The defendant may request evidentiary measures relevant to the defence.
3. By reasoned decision, the NDPA may refuse measures that are manifestly irrelevant, unnecessary, dilatory or repetitive.
4. The final decision must state reasons and contain:

   a) The identity of the defendant;

   b) A description of the facts found proved;

   c) Identification of the provisions infringed;

   d) The legal classification of the offence;

   e) The administrative fine and ancillary sanctions imposed, where applicable;

   f) The corrective measures ordered, where applicable;

   g) The time limit and manner of compliance;

   h) An indication of the available means of judicial challenge.
5. Failure to submit a defence does not prevent a final decision, without prejudice to the NDPA's duty to assess the relevant facts.

Article 45

Judicial challenge

1. Decisions of the NDPA imposing administrative fines, ancillary sanctions or corrective measures may be challenged before the competent court.
2. The challenge must be lodged within 30 working days of notification of the decision.
3. Upon receipt of the challenge, the NDPA may, within 15 working days, revoke the challenged decision in whole or in part.
4. Unless it revokes the decision in full, the NDPA shall refer the case file to the competent court and may attach submissions, material or information it considers relevant.
5. A judicial challenge suspends enforcement of the administrative fine and ancillary sanctions, unless the court decides otherwise.
6. A judicial challenge does not suspend corrective or urgent measures intended to prevent a serious or imminent risk to data subjects' rights, unless the court decides otherwise.

Article 46

Civil liability and judicial protection

1. Any person who has suffered pecuniary or non-pecuniary damage as a result of an infringement of this Law has the right to obtain compensation from the controller or processor in accordance with the general rules.
2. The exercise of rights before the NDPA is without prejudice to recourse to the competent courts.
3. Civil liability is without prejudice to the imposition of administrative fines, ancillary sanctions, corrective measures or any applicable criminal liability.

Article 47

Subsidiary application

1. In all matters not contrary to the provisions of this Law, the general rules of administrative procedure shall apply subsidiarily to the administrative offence procedure provided for herein.
2. In the absence of a specifically applicable legal regime, and with the necessary adaptations, the general principles of punitive law, the Criminal Code and the Code of Criminal Procedure shall apply subsidiarily insofar as they are compatible with the administrative nature of the administrative offence proceedings.
3. Subsidiary application may not prejudice the defendant's rights of defence, the protection of data subjects, the confidentiality of legally protected information or the effectiveness of urgent measures necessary to protect fundamental rights.

CHAPTER VI

TRANSITIONAL AND FINAL PROVISIONS

Article 48

Installation of the NDPA

1. The NDPA shall be deemed established on the date this Law enters into force.
2. Within 120 days after this Law enters into force, the National Parliament shall elect the members of the Governing Board whom it is responsible for electing and the Government shall appoint the member whom it is responsible for appointing.
3. Pending the effective installation of the NDPA's bodies, the Minister responsible for justice shall ensure the preparatory measures necessary for its installation, including identifying premises, making the initial budgetary provision, providing administrative support, opening recruitment procedures and preparing its operating instruments.
4. The NDPA shall commence its functions when the members of its Governing Board take office.

5. Within 90 days after taking office, the Governing Board shall approve the NDPA's internal rules of procedure, initial activity plan, provisional complaint forms and basic procedures for contact with data subjects and controllers.

Article 49

Initial implementation phase

1. During its first 18 months of operation, the NDPA must give priority to guidance, training, public awareness, approval of practical forms, identification of higher-risk processing activities and support for compliance by public and private entities.
2. The preceding paragraph is without prejudice to the immediate adoption of corrective or punitive measures where unlawful processing of sensitive data or biometric data, unlawful database interconnections, serious security breaches, unlawful international transfers, refusal to cooperate or a significant risk to data subjects' rights is involved.
3. The imposition of administrative fines for minor offences committed negligently shall begin only 18 months after this Law enters into force, except in cases of repeated offending, refusal to cooperate, failure to comply with an NDPA order or a material risk to data subjects.

Article 50

Previous legislation

1. Following the entry into force of this Law, whenever justified, legal regimes in Timor-Leste requiring alignment with this Law shall be progressively adapted to its provisions so as to ensure a coherent and harmonious legislative framework.
2. Failure to complete legislative adaptation within the period referred to in the preceding paragraph does not prejudice the immediate application of the essential principles, rights and duties laid down in this Law.

Article 51

Entry into force

1. This Law shall enter into force 180 days after its publication.

Considered and approved by the Council of Ministers on [day] [month] 2026.

The Prime Minister,

_____

The Minister of Justice,

_____

DALAN
DIGITAL
A NEW PATH FOR
DIGITAL CITIZENSHIP