

MORAIS LEITÃO
LEGAL CIRCLE

VPQ
ADVOGADOS

Guia Prático

Regime Jurídico Geral de Proteção de Dados Pessoais em Cabo-Verde

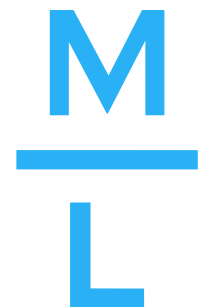
As mais recentes alterações
(2021)



Guia Prático

Regime Jurídico Geral de Proteção de Dados Pessoais em Cabo-Verde

As mais recentes alterações
(2021)



NOTA INTRODUTÓRIA

Foram diversas e extensas as transformações em matéria de proteção de dados pessoais desde a publicação da Lei n.º 133/V/2001, de 22 de janeiro, que aprovou o regime jurídico geral de proteção de dados pessoais em Cabo-Verde (Lei da Proteção de Dados Pessoais Cabo-Verdiana ou Lei da Proteção de Dados) e mesmo desde a publicação das alterações introduzidas àquele regime pela Lei n.º 41/VIII/2013, de 17 de setembro.

Neste sentido, veio a Comissão Nacional de Proteção de Dados Cabo-Verdiana (CNPd) alertar, nos últimos relatórios anuais de atividades, para a necessidade de ajustar a Lei da Proteção de Dados à realidade deste país.

Inspirado pelo disposto no Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados – RGPD) há pouco mais de um ano foi concretizada, em Cabo-Verde, uma alteração significativa da Lei da Proteção de Dados através da publicação da Lei n.º 121/IX/2021, de 17 de março (Lei n.º 121/IX/2021 ou Lei).

A nova Lei implica profundas mudanças no paradigma legal e regulatório da proteção de dados pessoais, com impactos significativos na atividade económica de Cabo Verde.

Atenta a experiência acumulada nas mais diversas vertentes da interpretação e aplicação do RGPD, a Morais Leitão Legal Circle conta com uma equipa especificamente dedicada ao estudo e ao

acompanhamento dos impactos que a alteração da Lei da Proteção de Dados Cabo-Verdiana implica para operadores públicos e privados em Cabo Verde e para as suas atividades, visando encontrar soluções que permitam, em cada caso, compatibilizar os valores inerentes à garantia de privacidade e da proteção dos dados pessoais com níveis adequados de *compliance*.

Com este guia prático pretendemos partilhar a nossa visão sobre os principais aspetos que as organizações públicas e privadas terão de considerar para cumprir com as alterações introduzidas à Lei da Proteção de Dados Cabo-Verdiana.

Glossário	11
<hr/>	
1. Necessidade de adaptar as organizações para cumprir as novas disposições da Lei da Proteção de Dados Pessoais Cabo-Verdiana	15
<hr/>	
2. As principais alterações introduzidas na Lei da Proteção de Dados Pessoais Cabo-Verdiana	17
<hr/>	
3. A Lei da Proteção de Dados Cabo-Verdiana: entrada em vigor e âmbito de aplicação	19
<hr/>	
4. Direitos dos titulares de dados pessoais ao abrigo da Lei da Proteção de Dados Pessoais Cabo-Verdiana	21
<hr/>	
5. Condições aplicáveis ao consentimento	22
<hr/>	
6. Consagração das figuras de <i>privacy by design</i> e <i>privacy by default</i>	23
<hr/>	
7. <i>Data Breach</i>	25
<hr/>	
8. Avaliação de impacto sobre a proteção de dados	26
<hr/>	
9. Introdução da figura do encarregado da proteção de dados	28
<hr/>	
10. Tipificação de novos crimes	30
<hr/>	
11. Por onde começar? Seis passos fundamentais	31
<hr/>	
Autores	35
<hr/>	

GLOSSÁRIO

CONSENTIMENTO (DO TITULAR DOS DADOS)

Qualquer 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.

DADOS BIOMÉTRICOS

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

DADOS GENÉTICOS

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

DADOS PESSOAIS

Qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável, o “titular dos dados”.

DADOS RELATIVOS À SAÚDE

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

DEFINIÇÃO DE PERFIS

Qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, a sua saúde, as suas preferências pessoais, os seus interesses, a sua fiabilidade, o seu comportamento, a sua localização ou as suas deslocações.

DESTINATÁRIO

A pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo a quem sejam comunicados dados pessoais ou a quem os dados pessoais sejam acessíveis, independentemente de se ser ou não de um terceiro, com exceção das autoridades públicas que recebem dados pessoais no âmbito de inquéritos específicos nos termos da lei, as quais não sendo destinatários, observam as regras de proteção de dados pessoais em função das finalidades do tratamento.

FICHEIRO (DE DADOS PESSOAIS)

Qualquer conjunto estruturado de dados pessoais, acessível segundo critérios determinados, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico.

INTERCONEXÃO DE DADOS

Forma de tratamento que consiste na possibilidade de relacionamento dos dados de um ficheiro com os dados de outro ou outros ficheiros mantidos pelo mesmo responsável ou por outro ou outros responsáveis com outra finalidade.

PSEUDONIMIZAÇÃO

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

RESPONSÁVEL PELO TRATAMENTO

A pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determina as finalidades e os meios de tratamentos dos dados pessoais.

SUBCONTRATANTE

A pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que trata os dados pessoais por conta do responsável pelo tratamento.

TERCEIRO

A pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que, não sendo o titular dos dados, o responsável pelo tratamento, o subcontratante ou outra pessoa sob autoridade direta do responsável pelo tratamento ou do subcontratante, esteja habilitado a tratar os dados.

TITULAR DOS DADOS

Pessoa singular identificada ou identificável a quem respeita a informação (os dados pessoais).

TRATAMENTO

Qualquer operação ou conjunto de operações sobre dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, por difusão ou por qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição, bem como a realização de operações lógicas e/ou aritméticas sobre esses dados.

VIOLAÇÃO DE DADOS PESSOAIS

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

1. NECESSIDADE DE ADAPTAR AS ORGANIZAÇÕES PARA CUMPRIR AS NOVAS DISPOSIÇÕES DA LEI DA PROTEÇÃO DE DADOS PESSOAIS CABO-VERDIANA

As alterações introduzidas pela Lei n.º 121/IX/2021 à Lei da Proteção de Dados Cabo-Verdiana são significativas e requerem, por isso, uma ponderação criteriosa acerca da gestão de níveis de risco pelas organizações públicas e privadas em matéria de proteção de dados pessoais.

É um facto que, em geral, os níveis de *compliance* de proteção de dados pessoais que se verificam nas organizações públicas e privadas que atuam em Cabo Verde carecem de amadurecimento, pelo que urge iniciar um processo para garantir a sua robustez, assegurando a adoção das melhores práticas em matéria de tratamento de dados pessoais que contribua para a operacionalização de Cabo Verde Digital de modo conciliado com um elevado nível de salvaguarda dos direitos e das garantias fundamentais de cada uma das pessoas a quem os dados respeitam.

Importa ainda ter em consideração que os conceitos normativos da proteção de dados são relativamente genéricos e abrangentes (e também abstratos), havendo um número muito elevado de atividades que, no seio de cada organização, envolvem operações de tratamento de dados pessoais

e que, considerando as exigências e os impactos da Lei da Proteção de Dados Pessoais Cabo-Verdiana, deverão passar a estar sob controlo.

A amplitude de algumas das principais alterações exige que cada organização – tanto no setor público como no privado – tenha posto em marcha e continue a desenvolver um processo de adaptação interna de procedimentos, rotinas e regulamentação (que, em grande número de casos, pressupõe, ainda, um trabalho prévio de identificação dos pontos críticos e das necessidades específicas de adaptação). Nalguns casos, pode estar em causa o redesenho de soluções e, em todos eles, a necessidade de planeamento e execução de ajustamentos que exigem tempo. As mais recentes alterações à Lei da Proteção de Dados Pessoais Cabo-Verdiana contam já com um ano de aplicação, tendo entrado em vigor em abril de 2021, pelo que é urgente rever a conformidade das organizações de hoje com um quadro legal já em aplicação.

2. AS PRINCIPAIS ALTERAÇÕES INTRODUZIDAS NA LEI DA PROTEÇÃO DE DADOS PESSOAIS CABO-VERDIANA

- Proteção dos dados pessoais respeitantes às pessoas (singulares) que se encontrem em Cabo Verde, independentemente do local em que os dados são tratados, com a consequente aplicação da Lei da Proteção de Dados aos responsáveis pelo tratamento (ou às entidades que tratem os dados por conta daqueles) estabelecidos fora do território nacional que recorram a dados pessoais daquelas pessoas, sempre que a atividade de tratamento respeite à oferta de bens ou serviços a esses titulares (mesmo que gratuitamente) ou ao controlo do seu comportamento que ocorra em território cabo-verdiano;
- Relevância legal da técnica de “pseudonimização” enquanto medida a adotar para segurança acrescida dos dados;
- Alargamento de conceitos: dados biométricos, violação de dados pessoais, dados relativos à saúde e definição de perfis;
- Alteração da designação de dados sensíveis para dados pessoais especiais e correspondente alargamento do seu elenco legal com a inclusão explícita de dados biométricos e orientação sexual;
- Consagração de um dispositivo legal que regula de forma clara e precisa as condições aplicáveis ao consentimento, obrigando os responsáveis pelo

tratamento à adoção de medidas apropriadas para garantir a sua validade e subsistência;

- Atribuição de competência à CNPD para autorizar o tratamento de dados especiais quando esteja em causa um interesse público ou o tratamento seja necessário para a prossecução de um interesse legítimo do responsável pelo tratamento;
- Alargamento da informação a fornecer ao titular de dados pessoais, pelas organizações (responsável pelo tratamento) que tratam dados pessoais sobre aspetos desse tratamento (*e.g.*, dever de informar o seu endereço, categorias de dados objeto de tratamento e fundamento para o tratamento);
- Introdução de deveres de notificação que incumbem aos responsáveis pelo tratamento, em caso de violações de dados pessoais (*data breach*) à CNPD e, em certos casos, de comunicações aos próprios titulares de dados pessoais;
- Consagração das figuras de *privacy by design* e *privacy by default*;
- Introdução da figura do encarregado da proteção de dados, vulgo DPO (*Data Protection Officer*) e dos casos em que a sua designação é obrigatória;
- Tipificação de novos crimes (*e.g.*, desvio de dados, utilização de dados de forma incompatível com a finalidade da recolha, interconexão ilegal de dados e inserção de dados falsos) e introdução de alguns aspetos processuais relativos à contraordenação.

3. A LEI DA PROTEÇÃO DE DADOS CABO-VERDIANA: ENTRADA EM VIGOR E ÂMBITO DE APLICAÇÃO

A Lei n.º 121/IX/2021 está em vigor desde 17 de abril de 2021, data a partir da qual todas as organizações públicas e privadas deveriam ter em curso planos de adaptação interna às novas regras em matéria de proteção de dados.

No que respeita ao âmbito de aplicação subjetivo do novo regime jurídico, cumpre dar nota de que uma das alterações introduzidas é o facto de, agora, todas as pessoas que se encontrem em Cabo Verde, independentemente do local onde os dados são tratados, estarem abrangidas pela Lei da Proteção de Dados Cabo-Verdiana pelo menos quando esteja em causa determinados tratamentos.

Neste sentido, os responsáveis pelo tratamento de dados, assim como os subcontratantes, estabelecidos fora do território nacional que tratem dados pessoais respeitantes a pessoas singulares que se encontrem em Cabo Verde, devem também cumprir o disposto na Lei da Proteção de Dados Cabo-Verdiana, sempre que a atividade de tratamento respeite à oferta de bens ou serviços a esses mesmos titulares (independentemente dessa prestação pressupor, ou não, um pagamento) ou ao controlo do seu comportamento, quando estejam em causa comportamentos ocorridos em território cabo-verdiano.

Ademais, e sem prejuízo de legislação específica, a Lei da Proteção de Dados Pessoais Cabo-Verdiana aplica-se transversalmente a todos os

setores de atividade e ainda à videovigilância e a outras formas de captação, tratamento e difusão de sons e imagens que permitam identificar pessoas sempre que o responsável pelo tratamento esteja domiciliado ou sediado em território nacional ou recorra a um fornecedor de acesso a redes informáticas e telemáticas aí estabelecido.

4. DIREITOS DOS TITULARES DE DADOS PESSOAIS AO ABRIGO DA LEI DA PROTEÇÃO DE DADOS PESSOAIS CABO-VERDIANA

São vários os direitos conferidos pela Lei da Proteção de Dados Pessoais Cabo-Verdiana aos titulares de dados com vista a reforçar a sua posição e a proteger os valores fundamentais que se impõem na recolha, no uso, na conservação e nas demais operações de tratamento de dados pessoais. É absolutamente essencial que o responsável pelo tratamento esteja preparado para assegurar o exercício desses direitos pelos titulares e satisfazer esse exercício, sempre que fundamentado, de modo tempestivo, devendo dispor de sistemas e de procedimentos que garantam isso mesmo, sob pena de incorrer em infrações ao abrigo da Lei da Proteção de Dados.

Indicamos, em seguida, os direitos que sofreram alterações ou que foram introduzidos (ou explicitados) pelas alterações legislativas mais recentes ao regime jurídico existente:

- (alargamento de) Direitos de informação e acesso;
- Direito de retificação;
- Direito ao apagamento;
- Direito à limitação do tratamento;
- Direito de portabilidade dos dados;
- Direitos do titular dos dados em casos especiais; e
- Direitos de titulares de dados que já faleceram.

5. CONDIÇÕES APLICÁVEIS AO CONSENTIMENTO

A alteração da Lei da Proteção de Dados Pessoais Cabo-Verdiana veio prever condições aplicáveis ao consentimento, exigindo-se ainda que, quando o tratamento for realizado com base no consentimento, o responsável pelo tratamento possa demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais.

Exige-se que o consentimento do titular dos dados seja prestado de forma livre, inequívoca e específica pois, quando 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 de modo inteligível e de fácil acesso e numa linguagem clara e simples.

Nesta senda, importa ainda referir que o titular dos dados tem o direito de retirar o seu consentimento a qualquer momento, de forma fácil e sem ser prejudicado, independentemente da licitude do tratamento já realizado com base no consentimento previamente dado, outro requisito que acentua o requisito do consentimento livre.

O consentimento deve ainda ser informado, pelo que, previamente à obtenção do consentimento, o responsável pelo tratamento deve facultar ao titular dos dados as informações previstas na Lei da Proteção de Dados Pessoais Cabo-Verdiana.

A Lei da Proteção de Dados foi ainda alterada no sentido de prever a forma como o consentimento de incapazes deve ser obtido.

6. CONSAGRAÇÃO DAS FIGURAS DE *PRIVACY BY DESIGN* E *PRIVACY BY DEFAULT*

Privacy by design e *privacy by default* são dois conceitos que, tal como no RGPD, encontram também consagração expressa na Lei de Proteção de Dados e que se relacionam com um modelo de tratamento/proteção de dados por predefinição e desde a conceção, permitindo que sejam criadas de raiz medidas de minimização de impacto e medidas de segurança nos produtos e serviços oferecidos desde a fase mais embrionária do seu desenvolvimento, passando as definições de proteção da privacidade a ser a norma, por defeito (*e.g.*, em redes sociais ou em aplicações móveis).

Os responsáveis pelo tratamento ficam obrigados a tratar os dados numa lógica de *privacy by design* e de minimização, de acordo com o contexto, o âmbito, as finalidades e o risco do tratamento.

A aplicação prática de medidas que preservem os dados pessoais requer esforços por parte das empresas, que terão de desenvolver mecanismos, ideias e tecnologias que assegurem – de raiz e logo desde a conceção e desenvolvimento de produtos, serviços ou atividades que envolvem tratamento de dados pessoais –, elevados níveis de proteção dos dados pessoais e uma minimização do impacto dos mesmos sobre a privacidade dos titulares.

O respeito por estes princípios de proteção da privacidade assume especial relevância na conceção e no controlo dos sistemas e dos recursos tecnológicos, designadamente no que respeita ao número e aos perfis de acesso à informação pessoal, ao número de utilizadores e políticas de *need-to-know*, às opções de minimização de impacto na privacidade

vs. necessidades de tratamento, aos registos de acesso à informação pessoal (*logs*) e às medidas de segurança específicas consoante o impacto ou os riscos para os dados pessoais.

7. DATA BREACH

Caso se verifique uma violação de dados pessoais, o responsável pelo tratamento deve notificar a CNPD no prazo de 72 horas, a menos que a violação não seja suscetível de resultar num risco para os direitos, liberdades e garantias das pessoas singulares cujos dados viram a sua disponibilidade, confidencialidade e/ou integridade comprometidas.

Quando não seja possível efetuar a notificação no prazo indicado acima, o responsável pelo tratamento deve indicar os motivos do atraso.

Além do referido, é agora obrigatório que o responsável pelo tratamento comunique a violação ao próprio titular de dados – o que deverá fazer sem demora injustificada –, caso essa violação seja suscetível de resultar num elevado risco para os direitos, liberdades e garantias do mesmo.

Salientamos ainda o facto de estas comunicações terem de ser documentadas e devidamente sustentadas.

Mostra-se crítico que as organizações disponham de planos e de procedimentos que garantam a deteção, a avaliação e as medidas de reação adequadas a dar resposta às ocorrências de *data breach*.

8. AVALIAÇÃO DE IMPACTO SOBRE A PROTEÇÃO DE DADOS

O responsável pelo tratamento deve notificar a CNPD sempre que pretenda iniciar um tratamento que utilize novas tecnologias e que, tendo em conta a sua natureza, âmbito, contexto e finalidade, seja suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares.

Além da referida notificação, o responsável pelo tratamento é obrigado a realizar uma avaliação de impacto, nomeadamente quando o tratamento tenha por base:

- a) A avaliação sistemática e completa de aspetos pessoais relacionados com pessoas singulares e que seja baseada no tratamento automatizado (incluindo a definição de perfis);
- b) As operações de tratamento em grande escala de categorias especiais de dados ou de dados pessoais relacionados com condenações penais e infrações; e
- c) O controlo sistemático de zonas acessíveis ao público em grande escala.

Acrescente-se ainda que, ao efetuar esta avaliação de impacto sobre a proteção de dados, o responsável pelo tratamento deve solicitar parecer do encarregado da proteção de dados, nos casos em que este tenha sido designado.

Notamos ainda que a lei estabelece que, sempre que necessário e, pelo menos, sempre que se verifique uma alteração dos riscos que as operações

de tratamento representam, o responsável pelo tratamento deve proceder a um controlo para avaliar se o tratamento é realizado em conformidade com a avaliação de impacto sobre a proteção de dados.

9. INTRODUÇÃO DA FIGURA DO ENCARREGADO DA PROTEÇÃO DE DADOS

O responsável pelo tratamento e o subcontratante designam um encarregado da proteção de dados sempre que:

- a) O tratamento seja efetuado por uma autoridade ou um organismo público, excetuando os Tribunais e o Ministério Público no exercício das suas competências processuais;
- b) As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que, devido à sua natureza, ao seu âmbito e/ou à sua finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala; ou
- c) As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados e de dados relacionados com condenações penais e infrações.

Notamos ainda que os grupos empresariais podem designar um único encarregado da proteção de dados, desde que o mesmo seja facilmente acessível a partir de cada estabelecimento. Também neste sentido, a lei estabelece que quando o responsável pelo tratamento ou o subcontratante seja uma autoridade ou um organismo público, pode ser designado um único encarregado da proteção de dados para várias dessas autoridades ou organismos, tendo em conta a respetiva estrutura organizacional e a dimensão.

Neste contexto, damos ainda conta de que o responsável pelo tratamento deve comunicar à CNPD os contactos do encarregado da proteção de dados, indicando ainda que os titulares dos dados podem contactar o encarregado da proteção de dados sobre todas as questões relacionadas com o tratamento dos seus dados pessoais e com o exercício dos direitos que lhe são conferidos pelo presente diploma.

No que respeita às funções do encarregado da proteção de dados, a lei determina que este deve: *(i)* informar e aconselhar o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratam os dados, a respeito das suas obrigações em matéria de proteção de dados; *(ii)* controlar a conformidade das políticas do responsável pelo tratamento ou do subcontratante relativas à proteção de dados pessoais com a lei; *(iii)* prestar aconselhamento, quando tal for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controlar a sua realização; *(iv)* cooperar e estabelecer a ponte de contacto com a CNPD sempre que tal seja necessário e/ou solicitado.

10. TIPIFICAÇÃO DE NOVOS CRIMES

A alteração à Lei da Proteção de Dados Cabo-Verdiana trouxe consigo a tipificação de novos crimes, a saber:

- Desvio de dados;
- Utilização de dados de forma incompatível com a finalidade da recolha;
- Interconexão ilegal de dados; e
- Inserção de dados falsos.

No que respeita a sanções, prevêem-se penas de prisão de 1 a 2 anos e penas de multa de 120 a 240 dias, consoante o crime em questão. Não obstante, é de notar que todas estas penas podem ser agravadas para o dobro nos seus limites quando se verificar que existiu um prejuízo efetivo.

11. POR ONDE COMEÇAR? SEIS PASSOS FUNDAMENTAIS

O conjunto muito significativo de alterações introduzidas à Lei da Proteção de Dados Pessoais Cabo-Verdiana, mas sobretudo a alteração do paradigma legal e regulatório verificado, designadamente em virtude das exigentes obrigações que ora se estabelecem, de forma transversal e num quadro sancionatório relevante para os responsáveis dos tratamentos, implica uma premente abordagem sistematizada e consciente à aplicação do quadro normativo da proteção de dados pessoais.

Aliás, as principais alterações introduzidas à Lei da Proteção de Dados Cabo-Verdiana indicadas nos pontos anteriores deste Guia Prático são bem elucidativas do esforço e do investimento que as organizações públicas e privadas terão de realizar para alcançarem níveis de *compliance* adequados.

Importa, por isso, responder à pergunta: por onde começar?

Os seis passos que propomos são aqueles que consideramos essenciais para que qualquer organização possa alcançar um desejável grau de *compliance* com a Lei da Proteção de Dados Pessoais Cabo-Verdiana. Não obstante, e salvo melhor opinião, salientamos que os níveis de risco resultantes da sua execução dependem sobretudo do esforço, do investimento e dos recursos que as organizações privadas e públicas lhes possam dedicar.

Nesta senda, julgamos ser essencial:

- ✓ Ponderar a necessidade de criação da figura do *data protection officer* e, eventualmente, de uma equipa especialmente dedicada à proteção dos dados pessoais;

- ✓ Assegurar a existência de políticas, instrumentos e procedimentos de *compliance* em matéria de proteção de dados pessoais;

- ✓ Identificar o tratamento de dados pessoais sensíveis (ou críticos para o negócio) e elaborar avaliações de impacto de proteção de dados (*data protection impact assessments* – DPIA);

- ✓ Assegurar que os novos conceitos estão incluídos nas políticas e nos procedimentos da organização;

- ✓ Criar modelos de comunicação de violações de dados (*data breaches*) que permitam alcançar um compromisso entre o cumprimento dos deveres legais e a minimização dos riscos e dos danos para a organização e para a reputação da mesma;

- ✓ Formar todos os níveis da organização em proteção de dados e fomentar uma cultura de respeito pela privacidade.

AUTORES

Portugal

MORAIS LEITÃO



**HELENA
TAPP BARROSO**
COORDENADORA
htb@mlgts.pt



**TIAGO
FÉLIX DA COSTA**
COORDENADOR
tfcosta@mlgts.pt



**BÁRBARA
MIRANDA LENCASTRE**
blencastre@mlgts.pt

Cabo-Verde

VPQ ADVOGADOS



**VERA PATRÍCIA
QUERIDO**
vquerido@vpqadvogados.com



OLIVER ARAÚJO
oaraujo@vpqadvogados.com

MORAIS LEITÃO

GALVÃO TELES, SOARES DA SILVA & ASSOCIADOS

MORAIS LEITÃO, GALVÃO TELES, SOARES DA SILVA & ASSOCIADOS

Sede

LISBOA

Rua Castilho, 165
1070-050 Lisboa
T +351 213 817 400
F +351 213 817 499
mlgtslisboa@mlgts.pt

PORTO

Avenida da Boavista, 3265 – 4.2
Edifício Oceanvs
4100-137 Porto
T +351 226 166 950 - 226 052 380
F +351 226 163 810 - 226 052 399
mlgtsporto@mlgts.pt

FUNCHAL

Av. Arriaga, n.º 73, 1.º, Sala 113
Edifício Marina Club
9000-060 Funchal
T +351 291 200 040
F +351 291 200 049
mlgrsmadeira@mlgts.pt
mlgts.pt

ALC ADVOGADOS

LUANDA

Masuika Office Plaza
Edifício MKO A, Piso 5, Escritório A/B
Talatona, Município de Belas
Luanda – Angola
T +244 926 877 476/8/9
T +244 926 877 481
geral@alcadvogados.com
alcadvogados.com

MDR ADVOGADOS

MAPUTO

Avenida Marginal, 141, Torres Rani
Torre de Escritórios, 8.º piso
Maputo – Moçambique
T +258 21 344000
F +258 21 344099
geral@mdradvogados.com
mdradvogados.com

VPQ ADVOGADOS

PRAIA

Edifício BAlcenter, 3.º esq.
Av. Cidade de Lisboa, Chã d'Areia
Praia – Cabo Verde
M +238 972 84 20
M +238 973 23 21
geral@vpqadvogados.com
vpqadvogados.com

membros da **MORAIS LEITÃO LEGAL CIRCLE**

Esta publicação é meramente informativa, não constituindo fonte de aconselhamento jurídico nem contendo uma análise exaustiva de todos os aspetos dos regimes a que se refere. A informação nela contida reporta-se à data da sua divulgação, devendo os leitores procurar aconselhamento jurídico antes de a aplicar em questões ou operações específicas. É vedada a reprodução, divulgação ou distribuição, parcial ou integral, do conteúdo desta publicação sem consentimento prévio. Para mais informações, contacte-nos por favor através do endereço com.pr@mlgts.pt.



9 JURISDIÇÕES
+ 400 PESSOAS

