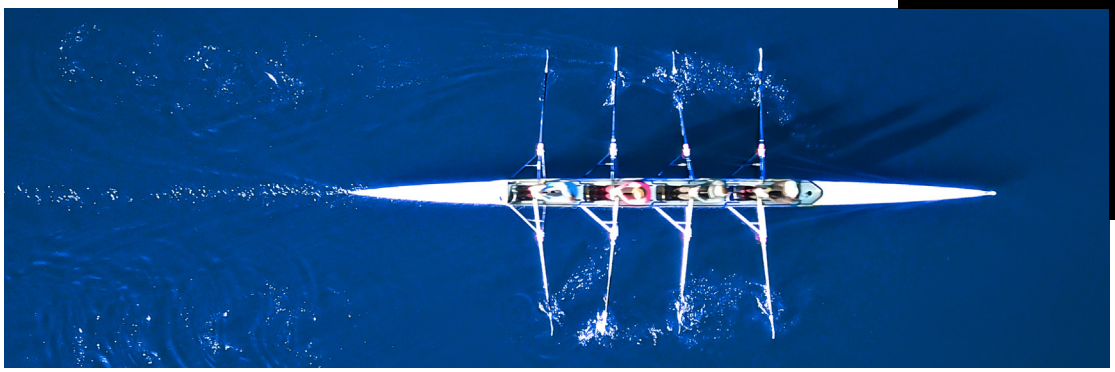
PLMJ



AGO. 24

ANGOLA

NEWS

TECNOLOGIA, MEDIA E TELECOMUNICAÇÕES

Dados Pessoais e Ciber-segurança em Angola:

A Actuação Fiscalizadora da APD, Desafios para as Organizações e Boas Práticas a considerar

Introdução

O quadro legal angolano aplicável à protecção de dados pessoais vigora desde 2011, com a publicação da Lei de Protecção de Dados (Lei n.º 22/11, de 17 de Junho – "LPDP") e da Lei das Comunicações Electrónicas e dos Serviços da Sociedade da Informação (Lei n.º 23/11, de 20 de Junho – "LCE").

De modo geral, a LPDP detalha aspectos relacionados com a protecção de dados pessoais, componente essencial do direito fundamental à privacidade, conforme expresso no número 2 do artigo 32.º da Constituição da República de Angola. A LCE actua num âmbito específico, complementando ou sobrepondo-se às disposições da LPDP, dependendo do contexto, especialmente no tratamento de dados pessoais associados à oferta e utilização de redes e serviços de comunicações electrónicas e serviços da sociedade da informação, como o comércio electrónico ou serviços de localização.

Paralelamente à entrada em vigor da LPDP, foi projectada a implementação da Agência Angolana de Protecção de Dados ("APD"), com a missão de fiscalizar o cumprimento das disposições legais em matéria de protecção de dados, emitindo recomendações, orientações e instruções sobre as melhores práticas no tratamento de dados pessoais.

A APD foi formalmente constituída em 2016 e, nos últimos anos, intensificou a sua actuação na supervisão e fiscalização junto das entidades responsáveis pelo tratamento de dados pessoais. A APD também actua junto da sociedade civil, divulgando informações sobre os direitos dos titulares de dados pessoais.

Renata Valenti
José Luquinda
Elisabete Cardoso
PLMJ Colab Angola
- RVA Advogados

Nádia da Costa Ribeiro
PLMJ Advogados

A LPDP detalha aspectos relacionados à protecção de dados pessoais, componente essencial do direito fundamental à privacidade, conforme expresso no número 2 do artigo 32.º da Constituição da República de Angola.

ANGOLA

Actuação Fiscalizadora da APD

Recentemente, a APD adoptou várias decisões importantes, impondo sanções a várias empresas no mercado angolano por graves violações da LPDP.

Em Junho e Julho de 2024, a APD divulgou na sua página de internet a aplicação de sanções a cinco empresas de diversos sectores, após investigações que concluíram pela existência de violações da LPDP, nomeadamente:

- MAXAM – Companhia de Pólvoras e Explosivos de Angola, S.A.: Multada em USD 150.000,00 por transferência ilegal de dados pessoais para o Reino Unido e por não notificar a APD sobre actividades de tratamento de dados pessoais dos seus trabalhadores.

- BANCO COMERCIAL DO HUAMBO (BCH): Multado em USD 75.000,00 por não implementar medidas técnicas e organizacionais adequadas para proteger dados dos clientes, o que, por sua vez, resultou num ataque de ciber-segurança que comprometeu os sistemas de informação do BCH.

- UNITEL, S.A.: Multada em USD 75.000,00 por não implementar medidas de segurança adequadas, permitindo a transferência fraudulenta de dados pessoais de uma cidadã para entidades terceiras.

- COSAL – Comércio e Serviços de Angola, Lda.: Multada em USD 75.000,00 por implementar medidas de ciber-segurança inadequadas, que deram azo a que a infra-estrutura de IT da sociedade fosse permeável a um ataque de ransomware que comprometeu dados de clientes e trabalhadores.

- Empresa Nacional de Distribuição de Electricidade, ENDE - EP.: Multada em USD 225.000,00 por não implementar medidas de segurança adequadas, o que permitiu o acesso não autorizado a informações sensíveis durante um ataque de ransomware.

As multas aplicadas pela APD evidenciam a importância crítica de as organizações assegurarem a privacidade dos cidadãos e mitigarem impactos que possam comprometer a sua continuidade operacional.

O Nível de Exigência da LPDP para assegurar a Protecção de Direitos Fundamentais:

A LPDP estabelece um quadro legal exigente em matéria de obrigações para as entidades que tratam dados pessoais, utilizando meios total ou parcialmente automatizados ou destinados a ser incluídos em ficheiros manuais.

Essas obrigações visam garantir o respeito pelos direitos e garantias, exigindo a implementação de medidas técnicas e organizacionais robustas. O incumprimento destas obrigações pode resultar em incidentes de segurança (como violação de dados) e consequente aplicação de multas pela APD.

As recentes multas aplicadas pela APD sinalizam a relevância de as organizações adoptarem medidas para assegurar o cumprimento da LPDP. O legislador nacional estabeleceu multas avultadas para incentivar a proactividade na implementação de medidas de protecção de dados.

Além disso, a implementação das medidas previstas na LPDP fomenta uma cultura de privacidade, elemento cada vez mais relevante para a reputação das entidades públicas e privadas.

ANGOLA

TECNOLOGIA, MEDIA E TELECOMUNICAÇÕES

A conformidade com a LPDP não é apenas uma exigência legal, mas uma pedra angular da governança corporativa responsável num mundo interconectado.

Na concepção dos sistemas de informação, é fundamental que as entidades:

- Disponham de protocolos de criptografia robustos;
- Realizem actualizações regulares com patches de segurança;
- Implementem firewalls e Sistemas de detecção de Intrusões.

Organizacionalmente, as entidades devem realizar um levantamento exaustivo das actividades de tratamento de dados pessoais, essencial para notificar a APD dessas actividades e conceber políticas de privacidade claras. Essas políticas devem descrever as medidas organizacionais aplicáveis ao acesso e manuseamento dos dados.

É igualmente importante destacar que a lista de medidas organizacionais acima referida não é exaustiva. Outras medidas incluem a conscientização e formação de todos os colaboradores envolvidos em actividades de tratamento de dados pessoais, a realização de avaliações de impacto sobre a protecção de dados e auditorias regulares para assegurar o contínuo cumprimento da legislação aplicável.

A protecção dos dados não pode ser dissociada da ciber-segurança. Como tal, as medidas organizacionais devem incluir políticas de ciber-segurança que abordem matérias como o acesso a redes e sistemas de informação, e utilização de aplicativos e equipamentos informáticos pelos funcionários das organizações.

É ainda essencial que as organizações disponham de planos de resposta a incidentes (disaster recovery e business continuity) para rápida identificação e mitigação do impacto de violações de dados, implementando salvaguardas e recuperação da informação para garantir a continuidade operacional.

Conclusão

A intensificação da acção fiscalizadora da APD quanto ao cumprimento do quadro legal de protecção de dados exige que as organizações se dediquem cada vez mais a temas de compliance em matéria de dados pessoais e dotem as suas infra-estruturas de TI com mecanismos que assegurem uma operação contínua, sem comprometer a sua reputação e credibilidade.

A conformidade com a LPDP não é apenas uma exigência legal, mas uma pedra angular da governança corporativa responsável num mundo interconectado. A compreensão e implementação adequadas dos requisitos da LPDP são cruciais para mitigar riscos de ciber-segurança e fomentar a confiança na economia digital, fundamental para a dinamização do tecido empresarial de qualquer nação. ■