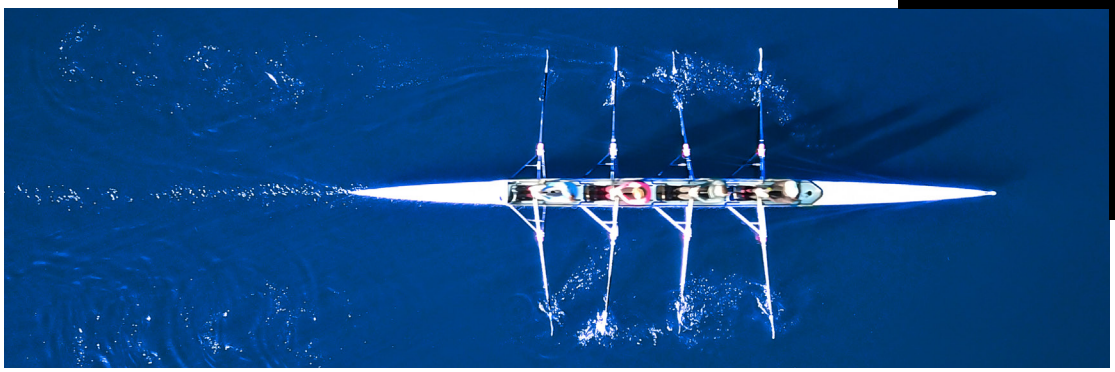
PLMJ



AUG. 24

ANGOLA

NEWS

TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS

Personal Data and Cybersecurity in Angola:

APD's Supervisory Role, Challenges faced by Organisations and Good Practices to consider

Introduction

The Angolan legal framework governing personal data protection has been in force since 2011, following the enactment of the Data Protection Law (Law No. 22/11 of 17 June - "LPDP") and the Electronic Communications and Information Society Services Law (Law No. 23/11 of 20 June - "LCE").

In general, the LPDP details aspects related to the protection of personal data, an essential component of the fundamental right to privacy, as expressed in Article 32(2) of the Constitution of the Republic of Angola. The LCE operates within a specific scope, by complementing or overlapping the provisions of the LPDP, depending on the context, particularly in the processing of personal data associated with the provision and use of electronic communications networks and services and information society services, such as e-commerce or location-based services.

The Angolan Data Protection Agency ("APD") was set up when the LPDP came into force and its role is to monitor compliance with the law regarding data protection, and to issue recommendations, guidelines and instructions on best practices in the processing of personal data.

APD was formally established in 2016 and in recent years has stepped up its efforts to supervise and monitor the organisations responsible for the processing of personal data. APD also collaborates with civil society organisations, by disseminating information on the rights of data subjects.

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

Nádia da Costa Ribeiro
PLMJ Advogados

The LPDP details aspects related to the protection of personal data, an essential component of the fundamental right to privacy, as expressed in Article 32(2) of the Constitution of the Republic of Angola.

ANGOLA

APD's supervisory role

Recently, APD took several important decisions that imposed penalties on various companies in the Angolan market for serious violations of the LPDP.

In June and July 2024, APD announced on its website that penalties had been imposed on five companies in different sectors, following investigations, which concluded that there had been violations of the LPDP:

- MAXAM – Companhia de Pólvoras e Explosivos de Angola, S.A.: A fine of USD 150,000.00 was imposed for the unlawful transfer of personal data to the United Kingdom and for failure to notify APD regarding the processing of its employees' personal data.
- BANCO COMERCIAL DO HUAMBO (BCH): A USD 75,000.00 fine was imposed for failure to implement appropriate technical and organisational measures to protect customer data, which in turn resulted in a cybersecurity attack that compromised BCH's information systems.
- UNITEL, S.A.: A USD 75,000.00 fine for failure to implement appropriate security measures, which facilitated the fraudulent transfer of a citizen's personal data to third parties.
- COSAL – Comércio e Serviços de Angola, Lda.: A USD 75,000.00 fine for the implementation of inappropriate cybersecurity measures that rendered the company's IT infrastructure susceptible to a ransomware attack that compromised customer and employee data.
- Empresa Nacional de Distribuição de Electricidade, ENDE - EP.: A USD 225,000.00 fine for failure to implement appropriate security measures, which facilitated unauthorised access to sensitive information during a ransomware attack.

The fines imposed by APD underscore the crucial importance of organisations safeguarding citizens' privacy and mitigating risks that could jeopardise their operational continuity.

The LPDP's Stringent Requirements for Safeguarding Fundamental Rights:

The LPDP establishes a demanding legal framework of obligations imposed on organisations that process personal data via the use wholly or partially, automated means, or that process personal data intended for inclusion in manual filing systems.

These obligations seek to ensure respect for rights and guarantees and require the implementation of robust technical and organisational measures. Failure to comply with these obligations may result in security incidents (such as data breaches) and result in fines imposed by APD.

The recent fines imposed by APD highlight the importance of organisations adopting measures to ensure compliance with the LPDP. Angolan law includes provision for the imposition of heavy fines to encourage proactivity in the implementation of data protection measures.

Moreover, the implementation of the measures outlined in the LPDP fosters a privacy-centred culture, which is an increasingly vital factor in terms of the reputation of public and private organisations.

ANGOLA

TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS

Compliance with the LPDP is not merely a legal obligation, but a fundamental pillar of responsible corporate governance in our interconnected world.

When designing information systems, it is essential that organisations:

- Implement robust encryption protocols;
- Update regularly with security patches;
- Deploy firewalls and intrusion detection systems.

From an organisational perspective, organisations must conduct a comprehensive audit of their data processing activities, which is essential for notifying APD of these activities and developing a clear privacy policy. These policies must outline the organisational measures applicable to data access and handling.

It should be noted that the above list of organisational measures is not exhaustive. Other measures include raising awareness and training all employees involved in personal data processing activities,and conducting data protection impact assessments. Furthermore, regular audits should also be conducted to ensure ongoing compliance with applicable legislation.

Data protection is integral to cybersecurity. Therefore, organizational measures must incorporate policies pertaining to cybersecurity which cover issues like network access, management of information systems, and protocols for employees' use of software and hardware within the organization.

It is also essential that organisations have incident response plans (disaster recovery and business continuity) to quickly identify and mitigate the impact of data breaches, to implement safeguards and recover information to ensure operational continuity.

Conclusion

The intensification of APD's supervisory action regarding compliance with the legal data protection framework requires organisations to dedicate themselves more and more to personal data compliance issues and to equip their IT infrastructures with mechanisms that ensure operational continuity without compromising their reputation and credibility.

Compliance with the LPDP is not merely a legal obligation, but a fundamental pillar of responsible corporate governance in our interconnected world. Correct understanding and implementation of the requirements imposed by the LPDP are crucial in terms of the mitigation of cybersecurity risks and the building of confidence in the digital economy, which is fundamental to the boosting the business fabric of any nation. ■