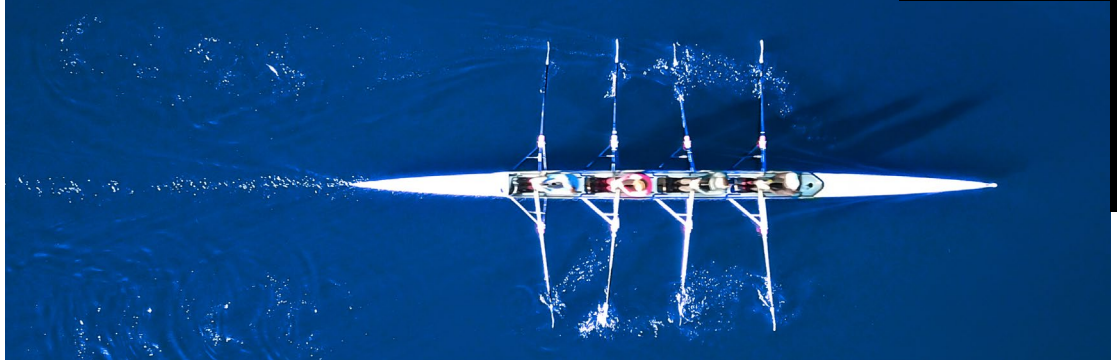




OCT. 26

ANGOLA

NEWS

TECHNOLOGY, MEDIA AND COMMUNICATIONS

Cybersecurity Law

Law No. 9/26 of 28 September (the “Cybersecurity Law”) was recently published in the Official Gazette, fully repealing Law No. 7/17 of 16 February (Law on the Protection of Computer Networks and Systems). The Law establishes the legal framework applicable to the protection of citizens and public and private entities against cyber threats and cyberattacks, as well as to the security of the country’s networks, information systems, critical infrastructure and essential services.

Compared with the previous regime, the Law has a significantly broader scope, covering all natural and legal persons, public and private, that use or operate in Angolan cyberspace. It also applies to acts carried out within and outside the national territory, whenever such acts are directed at, or produce effects in, Angolan cyberspace.

The Law also applies to acts carried out within and outside the national territory, whenever such acts are directed at, or produce effects in, Angolan cyberspace.

Key Changes

The main changes introduced include:

- i) The creation of the National Cybersecurity System, composed of the National Cybersecurity Council, the National Cybersecurity Centre (CNC) and the National CSIRT Network;
- ii) The definition of specific categories of entities subject to cybersecurity obligations, including operators of critical infrastructure and essential services, and providers of digital services, electronic communications, data centres, cloud and cybersecurity services;
- iii) The introduction of cyber risk management and assessment obligations;
- iv) An obligation to notify cybersecurity incidents to the competent authorities;
- v) Strengthened oversight, audit and supervisory powers.

Renata Valenti
José Luquinda
PLMJ Colab Angola
– RVA Advogados

Pedro Lomba
Mafalda de Brito
Fernandes
PLMJ Advogados

ANGOLA

Providers have a duty to Report incidents with significant impact to the competent authorities, including CERT.ao and the relevant sectoral CSIRT.

Main duties of covered providers

The main duties of covered providers include:

1. Registration and governance:

Registration with the National Cybersecurity Centre and, depending on the size, risk and criticality of the activity, setting up an institutional CSIRT, appointing a cybersecurity focal point or joining a sectoral CSIRT;

2. Security and risk management:

Adopting appropriate and proportionate technical and organisational measures to prevent, detect, respond to and recover from incidents, including risk management mechanisms, service continuity and access control;

3. Incident notification and response:

Reporting incidents with significant impact to the competent authorities, including CERT.ao and the relevant sectoral CSIRT, and, where applicable, submitting a final report on the response to and resolution of the incident;

4. Specific requirements for data centres and cloud computing services:

Adopting policies and measures to ensure business continuity, disaster recovery and risk management, taking out adequate insurance and informing customers or subscribers of relevant incidents and the related coverage;

5. Regulatory compliance:

Compliance with the technical requirements, procedures, deadlines and notification channels to be defined in the applicable regulations.

The duties that actually apply will depend on the nature, size, risk and criticality of the activity carried out, and each entity should assess its regulatory position in light of the services provided, the networks and systems used and its relationships with customers, subscribers and third-party providers.

ANGOLA

Penalties

Failure to comply with the obligations set out in the Law may constitute a minor, serious or very serious administrative offence, punishable by fines and, in certain cases, by additional penalties of temporary suspension of activities and a ban on participating in public procurement procedures for a period of up to 3 years. For legal persons, fines for very serious offences may reach 2,000 to 4,000 national minimum wages, without prejudice to the other consequences provided for in the Law. Oversight and the application of penalties are the responsibility of the National Cybersecurity Centre.

In certain cases, additional penalties of temporary suspension of activities and a ban on participating in public procurement procedures for a period of up to 3 years.

Entry into force and recommendations

The Law entered into force on its date of publication, 28 September 2026. Entities subject to registration have 180 days from the entry into force to register.

Entities potentially covered are advised to:

- i) confirm their classification and the applicable obligations;
- ii) complete registration and appoint responsible officers, focal points and response teams;
- iii) document their risk management, technical and organisational controls, and continuity and recovery plans; and
- iv) test their procedures for detection, containment, notification and preparation of the final report. ■