



ASSIGNING THE DPO's ROLE! – The Explainer

FEBRUARY EDITION
EXPERT'S EXPLAINER

Where do you believe is the optimal place within your organization to designate the Data Protection Officer Role?

The role of the Data Protection Officer (DPO) stands as a linchpin in organizations striving for data protection compliance, particularly in the wake of global regulations like GDPR and Kenya's Data Protection Act of 2019. The legal framework, as outlined in Section 24 of the Kenya Data Protection Act and Article 37 of the GDPR, mandates organizations processing personal data to appoint a DPO. This key figure shoulders the responsibility of ensuring organizational compliance with data protection regulations, acting as a point of contact for authorities and data subjects, educating staff on compliance requirements, and offering advisory services on data protection matters.

“*The challenge lies in finding equilibrium, ensuring the DPO performs optimally with independence in carrying out duties while fostering collaboration with data owners.*”



CAROLINE MURIITHI
SENIOR CONSULTANT

DATA PROTECTION & INFORMATION SECURITY



The designation of the DPO has spurred debates, revolving around their role as either implementers or checkers and the requisite expertise and collaboration. The challenge lies in finding equilibrium, ensuring the DPO performs optimally with independence in carrying out duties while fostering collaboration with data owners.

Traditionally viewed as legal experts, DPOs were often placed within legal departments, leveraging their skills in interpreting laws and regulations. However, this perspective may overlook the technical nuances of data protection. Information security and cyber security, crucial for data privacy compliance, demand a more integrated approach.

In response to the growing emphasis on cybersecurity, some organizations place the DPO within the IT or security department. While this ensures collaboration on technical measures, it introduces a challenge of segregation of duty, as the DPO becomes involved in implementing controls they should objectively assess.

Another perspective suggests placing the DPO within the risk and compliance department, aligning with their responsibility for adherence to laws and internal policies. However, this may limit their ability to address legal and technical challenges comprehensively.

#meaningfulmondays



Did you

Know

Assigning the **DATA PROTECTION OFFICER** role to the **IT Department** may not be ideal, given the inherent oversight responsibilities associated with the DPO Role.

#dataprotectionandprivacy





In Conclusion

An alternative approach involves engaging an independent DPO or contracting the role externally - an outsourced Data Protection Officer like Sentinel Africa. This offers the organization access to talent with necessary legal and technical expertise while ensuring an unbiased assessment of data protection compliance.

The choice of placement carries its pros and cons, necessitating careful consideration of the DPO's skills, independence, and their ability to present data protection matters strategically to the management. In the evolving landscape of data protection, finding the right fit for the DPO designation is paramount for organizational resilience and compliance.



BY www.sentinel africa.co.ke

CAROLINE MURIITHI
CERTIFIED DATA PROTECTION OFFICER

Your Advisor of Choice



www.sentinel africa consulting.com

 FOLLOW US : SENTINEL AFRICA CONSULTING