



Terms of Reference (TOR) for Legal Advisor

1. Background

The Federal Government of Somalia has recently enacted the Somali Data Protection Law (DPL) 2023, mandating the establishment of the Somali Data Protection Authority (DPA). The DPA will serve as the primary federal institution responsible for the implementation, enforcement, and oversight of the DPL, ensuring compliance and developing national regulations on data protection and privacy.

To support its mission of promoting transparency, accountability, and public awareness regarding data privacy rights and obligations, the DPA seeks to engage a qualified Legal Advisor.

2. Objectives

The objective of this ToRs is to recruit a Legal Advisor to support the DPA by:

- (a) Strengthening the DPA's internal expertise in established and emerging legal and regulatory issues relating to data protection and data governance;
- (b) Providing expert legal guidance to the DPA to ensure adherence to national laws and consistency with international good practices in the field of data protection, by referring to data protection practices in other leading jurisdictions; and
- (c) Assisting in the drafting of guidelines, standard operating procedures, rules, regulations, and comprehensive legal frameworks that may be required to implement the DPA and related legislations, overseeing cybersecurity protocols, and addressing ethical considerations related to Artificial Intelligence (AI) within the scope of data protection.

3. Key Responsibilities and Deliverables

A. Legal Advisory

- Draft, review, and update data protection regulations and policies, identify key gaps, and recommend improvements aligned with international good practices.
- Provide legal opinions on data privacy, cybersecurity, and AI governance, and any other related issue that may arise in the implementation of the DPA.
- Ensure compliance and consistency of all internal rules, procedures, and regulations, with Somalia's Data Protection Act and related legislation.

B. Policy and Framework Development

- Develop and implement legal frameworks to strengthen data protection and cybersecurity measures.
- Draft guidelines on the ethical and legal use of Artificial Intelligence.
- Collaborate with stakeholders to address emerging challenges in data governance.

C. Capacity Building

- Organize and lead training sessions for staff and stakeholders on data protection laws and international best practices.
- Develop tools and resources to raise awareness about cybersecurity and AI-related risks.
- Develop internal notes, guidance tools, and presentation materials on identified topics related to data governance.

D. Stakeholder Engagement

- Facilitate advisory discussions with government agencies, private sector entities, and international organizations on data governance issues.
- Offer strategic recommendations to the DPA for legal and policy discussions at national and international levels.
- Develop guidance notes to support awareness building and compliance across entities.

E. Monitoring and Compliance

- Monitor compliance with cybersecurity protocols and data protection standards.
- Conduct audits and assessments to identify gaps in data protection measures.
- Advise on enforcement strategies that align with the Data Protection Act and DPA's institutional capacities.

4. Qualifications and Experience

A. Academic Background

- Bachelor's degree in Law (LLB) is mandatory and Master's degree in Law, Governance, Cybersecurity, or related fields is must.

B. Professional Experience

- Minimum 10 years of experience in data protection and privacy, with a strong track record of providing legal and policy advisory support to governments.
- Proven expertise in data protection, cybersecurity laws, and legal aspects of Artificial Intelligence.
- Experience working with government agencies, international organizations, or private entities on data governance.
- Demonstrated experience in supporting organizational development in public sector settings with strong understanding of and experience in building institutional capacities related to data governance.
- Privacy certifications from recognized international organizations are a plus.

C. Key Competencies

- In-depth knowledge of international and regional data protection laws (e.g., GDPR, AU Convention on Cybersecurity). Familiarity with international best practices such as the EU GDPR, Convention 108+ and data protection legislations in other African countries is an added advantage;
- Experience in developing and implementing data governance frameworks and privacy strategies, with strong knowledge of relevant laws, regulations.
- Strong understanding of cybersecurity and AI ethics (ideally in developing country context).
- Excellent written and oral communication and presentation skills coupled with an ability to quickly synthesize, analyze, and effectively present legal materials to high-level technical and non-technical audiences.
- Experience working with a variety of legal and non-legal stakeholders, including government officials, policymakers, regulators, consultants, and academics.
- ICT proficiency, including legal research tools and office software.
- Familiarity with cybersecurity tools and technologies is an added advantage.
- Proficiency of English and Somali is mandatory.