Frequently Asked Questions on the Data Protection Officer (DPO) in Kenya

1. **Who is a DPO?**

   This is an individual in an organisation or group of organisations who is tasked with ensuring compliance with the applicable data protection laws and regulations; developing and overseeing organisational data protection policies, strategies, privacy assessments and standards; and industry specific data protection requirements.

2. **What does the Kenyan Data Protection Act provide about a DPO?**

   - The Act does not make it mandatory to appoint or designate a DPO.
   - The Act provides that a DPO may be a staff member of the data handler and may fulfil other tasks and duties provided that any such tasks and duties do not result in a conflict of interest.
   - A group of entities may appoint a single DPO provided that such an officer is accessible by each entity.
   - A person may be designated or appointed as a DPO, if that person has relevant academic or professional qualifications which may include knowledge and technical skills in matters relating to data protection.
   - A data handler should publish the contact details of the DPO on the website and communicate them to the Data Commissioner who shall ensure that the same information is available on the official website.

- A DPO shall:
    - advise the data handler and their employees on data processing requirements provided under the law,
    - ensure on behalf of the data handler that the law is complied with,
    - facilitate capacity building of staff involved in data processing operations,
    - provide advice on data protection impact assessments, and
    - cooperate with the Office of the Data Protection Commissioner and any other authority on matters relating to data protection.

3. Do all data handlers in Kenya need to have a DPO?

Both a data controller and a data processor may appoint a DPO. This applies both to public and private bodies; with the only exception being courts acting in their judicial capacity.

While it is advisable to have an appointed or designated DPO, the Kenyan Data Protection Act does not make it mandatory.

4. What qualifications and skills should a DPO have?

- Expertise and knowledge of data protection laws of the countries their organisation operates in.
- Basic knowledge of legal concepts and operation of the law.
- A good understanding of technology and information/data management.
- Knowledge of information/data management including data security, data governance, and data risk management.
- Knowledge of information/data management in their respective industry.
- Privacy and/or security certifications. These may include certifications offered by ISACA, IAPP, PCEB, etc.
- Project management skills
- Good communication skills.

- Ethical decision making.
- Independence and impartiality.
- Conflict resolution skills.
- Stakeholder management skills.

5. What responsibilities should be included in the job description of a DPO?

- Ensuring resources are allocated towards data protection compliance.
- Reporting to the Board /management and ensuring continuous Board buy-in for the privacy programme.
- Monitoring compliance with the law.
- Ensuring data protection by design and by default in all functions of the organisation.
- Advising, sensitising, and educating on data protection compliance.
- Conducting data protection assessments and audits.
- Drafting and revising data protection policies and notices.
- Handling data subject requests.
- Leading in incident and data breach response strategies.
- Vendor and third-party risk management.
- Record keeping.
- Monitoring data processing activities.
- Leading in data protection related risk management
- Addressing disputes related to data protection.
- Liaising with the Office of the Data Protection Commissioner.
- Providing reports on data protection compliance status.

6. What should a DPO do once designated or appointed?

A DPO once designated and appointed should:

- Seek to understand the organisational structure of the institution.
- Have one on one familiarisation sessions with the organisation's team leaders.

- Have a familiarisation session with all the organisation's team leaders as a group to clarify expectations, roles, responsibilities, and collaboration within the organisation.
- Craft a data privacy program/work plan with activities, deliverables, timelines, and resources required -
    - Carryout preliminary assessment of the level of compliance in the organisation.
    - Prioritise activities for compliance from the outcome of the preliminary assessment.
    - Coordinate, convene and align other departments to implement the privacy program on a regular basis.
- Share workplan and seek buy-in from all the organisation's team leaders.

7. Who should a DPO report to in an organisation?

A DPO ought to report directly to the highest management level within the respective organisation of the data handler.

The DPO office needs to be positioned high enough to ensure enterprise-wide authority and functionality similar to that enjoyed by the Risk or Audit Offices.

8. What about the independence of the DPO?

The DPO ought to be allowed to act independently and to not be under direction or instruction regarding their individual tasks.

9. How many DPOs should an organisation have?

This depends on the nature and scale of data processing activities, the complexity of data processing, and the applicable data protection regulations within an organisation.

A Chief DPO may have assistant or deputy DPOs working under them, particularly in an enterprise with multinational, regional, or continental reach.

10. What can an organisation do to support a DPO?

- Providing resources to the DPO: budget lines, office space, stationery, computers, laptops, etc.
- Identifying and assigning departmental 'Data Champions' to support the DPO function at grassroot levels.
- Training the DPO for recognised certification.
- Giving the DPO autonomy in executing their functions.
- Providing automated tools to support the DPO in data mapping, risk assessment, data inventory, data classification, data security i.e. Data Loss Prevention System (DLP).

11. Can a DPO be an external consultant, or must they be an internal employee?

The Kenya Data Protection Act does not require a DPO to be an internal employee. There are a number of pros and cons to consider when deciding what type of DPO to appoint:

Having Substantive in-house DPO:

Advantages:

- An in-house DPO can develop a deep understanding of an organisation's specific data protection needs and challenges. The DPO can provide tailored advice and guidance based on their familiarity with an organisation 's operations.
- In-house DPOs are readily available and can respond promptly to data protection issues or inquiries.

- An in-house DPO is likely to have a better understanding of an organisation's culture, values, and business processes, enabling them to align data protection efforts more effectively.
- In-house DPO may be more cost-effective than outsourcing, especially for larger organisations with substantial data processing activities.
- An organisation has direct control over the hiring, training, and performance of an in-house DPO, fostering a stronger sense of accountability.

Disadvantages:

- An in-house DPO may face conflicts of interest, especially if they are involved in decision-making processes that could impact data protection compliance.
- Smaller organisations may struggle to allocate sufficient resources for hiring and maintaining an in-house DPO, potentially leading to a lack of expertise or time to address all data protection requirements.
- An in-house DPO might have a narrower perspective compared to external experts who work with multiple organisations and industries, potentially missing out on innovative solutions or best practices.
- Depending on the size and complexity of the organisation, an in-house DPO may face a heavy workload, leading to burnout and decreased effectiveness in managing data protection issues.
- If the in-house DPO leaves an organisation, there might be a gap in data protection knowledge and compliance until a replacement is found.
- There might be challenges in maintaining independence, as the DPO should act independently and not take instructions from the management. This can be more challenging when the DPO is part of the internal structure.

Having in-house DPO with dual roles:

Advantages:

- Integration with other organisational functions.

- Broader understanding of an organisation 's overall operations.
- Potential cost savings for an organisation with limited resources.

Disadvantages:

- Potential conflicts of interest between dual roles.
- Risk of data protection priorities being overshadowed by other responsibilities.
- Challenges in maintaining independence in data protection decision-making.

Having an external DPO:

Advantages:

- External DPOs often bring a wealth of experience and expertise, having worked with various organisations and industries. They can provide a broader perspective on data protection issues.
- External DPOs are typically more independent and less likely to face conflicts of interest, as they are not directly integrated into the internal decision-making structure of the organisation.
- Organisations can access specialised skills on-demand without the need to hire a full-time, in-house DPO. This can be particularly beneficial for smaller companies with limited resources.
- External DPOs can take on the responsibility of managing data protection compliance, reducing the workload on internal staff, and allowing them to focus on core business activities.
- For smaller organisations, hiring an external DPO can be more cost-effective than maintaining a full-time, in-house position, considering salary, benefits, and training costs.
- External DPOs may be in a better position to engage and influence the Board and snr. Management compared to internal staff.
- External DPOs free up the organisation to concentrate on its core business.

- External DPOs are more likely to hold everyone in the organisation, including senior management, to account compared to an internal DPO who may be reporting into one of the departmental heads.

Disadvantages:

- External DPOs might not have an in-depth understanding of an organisation's internal processes, culture, and specific challenges, which could affect the relevance of their advice.
- There may be challenges in communication and coordination, especially if the external DPO is not readily available or lacks a strong understanding of the organisation's day-to-day operations.
- External DPOs might not be as readily available as an in-house DPO, potentially leading to delays in addressing urgent data protection issues.
- Organisations relying on external DPO services are dependent on the performance and availability of the external provider. If the provider faces issues, the organisation's data protection compliance could be impacted.
- External DPOs may need access to sensitive information, raising concerns about data security and confidentiality. It's crucial to establish clear contractual agreements and security measures.

- External DPOs may have less commitment to the organisation compared to an in-house DPO. This lack of attachment might affect the level of dedication and understanding of the organisation's specific needs.

12. What issues should a DPO be aware of before signing into the role?

- Resources available for establishing, managing, assessing, and auditing the privacy programme. This will include budgetary allocations, allocated personnel, software and hardware for compliance, and office space.
- Job description: make reference to the responsibilities cited in these FAQs.
- Who the DPO will report to.

- Compensation for the role:
    - Monetary compensation will vary depending on years of experience, education level, certifications, professional experience, and demonstrated competence.
    - Monetary and non-monetary benefits of the role.
    - A prospective internal or external DPO should carry out research on the compensation scales for the role in view of the industry, years of experience, education level, certifications, professional experience, and demonstrated competence.

13. Can a DPO be held liable for non-compliance?

A DPO is not personally liable for non-compliance with the law. A DPO acts as a facilitator and advisor within an organisation, assisting in ensuring compliance with data protection laws. Under the Data Protection Act, it is the data handler - the data controller or data processor who is responsible for compliance.

Ideally, the DPO should not handle tasks which are deemed to be "data processing" activities yet they are supposed to monitor the same for compliance.

14. What happens when a DPOs advice is ignored?

A DPO should always ensure they keep a record and document all activities undertaken by them while reminding the decision-making organs in the organisation about the consequences of non-compliance with the law.

The Data Privacy and Governance Society of Kenya

Mission statement: to be the most inclusive society of data privacy and governance professional in Kenya that champions for the welfare of its members while ensuring legal, responsible, and ethical use of data.

About us: we are a Society registered under the Societies Act with the objective to:

- Build a network of data privacy and governance professionals across Kenya and Africa.
- Facilitate continuous professional development and certification.
- Set professional and ethical standards for data privacy and governance professionals.
- Champion and protect the interests of members.
- Collaborate and partner on projects and training.
- Engage data privacy and governance regulators.
- Collaborate and partner with regional and international societies in data privacy and governance.
- Create an engaging community that provides leadership on data privacy and governance related issues in Kenya.
- Champion policy and legislative reforms in data privacy and governance.
- Engage in strategic litigation on data privacy and governance matters.
- Provide mentorship and guidance to members.
- Facilitate knowledge sharing, lobbying, awareness raising, and networking.

Our members: we have representation from private practitioners, inhouse data protection officers in public and private sector, academia, civil society, young professionals, and university students.

Membership categories:

- Student Members
- Professional Members
- Corporate Members

Contact: dataprivacyke@gmail.com

Linkedin: Data Governance Pros Kenya | **Twitter:** @DataGovProsKe