Privacy and Governance Professionals Survey Report

June 2023

Contents

About DPGSK

The Data Privacy & Governance Society of Kenya (DPGSK) is a registered Society under the Societies Act with a mission to become the most inclusive society of data privacy and governance professionals in Kenya. We are dedicated to championing the welfare of our members while ensuring the legal, responsible, and ethical use of data.

Our society aims to fulfil its objectives through various initiatives:

- Building a network of data privacy and governance professionals across Kenya and Africa.
- Facilitating continuous professional development and certification.
- Setting professional and ethical standards for data privacy and governance professionals.
- Championing and protecting the interests of members.
- Collaborating and partnering on projects and training.
- Engaging data privacy and governance regulators.
- Collaborating and partnering with regional and international societies in data privacy and governance.
- Creating an engaging community that provides leadership on data privacy and governance related issues in Kenya.
- Championing policy and legislative reforms in data privacy and governance.
- Engaging in strategic litigation on data privacy and governance matters.
- Providing mentorship and guidance to members.
- Facilitating knowledge sharing, lobbying, awareness raising, and networking.

Our membership encompasses a diverse range of professionals, including private practitioners, in-house data protection officers in the public and private sectors, academia, civil society, young professionals, and university students. We offer different membership categories to cater to the needs and aspirations of individuals and organizations

Preface

The Data Privacy and Governance Society (DPGSK) recognises the crucial role data privacy and governance professionals play in enabling regulatory compliance in all sectors of the economy. Data continues to shape society and it is critical that we understand the experiences and challenges faced by data privacy and governance professionals.

The survey carried out with DPGSK members was aimed at providing us with a comprehensive analysis of the current state of professionals shedding light on their roles, skills, aspirations, and the trends that influence their work. The survey was conducted on public sector, private sector, academia, and civil society professionals. Their valuable input, combined with our in-depth analysis, forms the foundation of this report.

This report explores diverse aspects of data privacy and governance professionals. It highlights educational backgrounds, industry affiliations, and years of experience. It also highlights the challenges faced by these professionals and proposes ways to address them.

Insight from this report provides DPGSK and partners the knowledge required to improve the data privacy and governance profession.

We must express our gratitude to all the participants who generously shared their insights and experiences, making this survey report possible. Their contributions not only provide a snapshot of the data privacy and governance professional landscape but also facilitate an understanding of what needs to be done.

It is our hope that this report will serve as a valuable resource for data privacy and governance professionals, organizations, and policymakers alike. By shedding light on the current state of the profession, we aim to foster discussions, inspire collaborations, and facilitate the advancement of data privacy and governance in their pursuit of excellence.

Sincerely,

Mugambi Laibuta

Chairperson, DPGSK

Privacy and Governance Professionals Survey

Background

The Data Privacy and Governance Society (DPGSK) recognizes the emerging significance of data privacy and governance professionals in Kenya in ensuring regulatory compliance across all sectors of the economy. As data continues to shape our society, it is crucial to gain a comprehensive understanding of the experiences and challenges faced by these professionals. To fulfil this purpose, DPGSK conducted a survey among its members, aiming to provide valuable insights into the current state of data privacy and governance professionals.

Respondents

The survey reached out to a diverse range of professionals from various sectors. This includes individuals working in the public sector, private sector, academia, and civil society. By incorporating viewpoints from professionals with diverse backgrounds and affiliations, the survey sought to capture a holistic representation of the data privacy and governance profession.

Survey

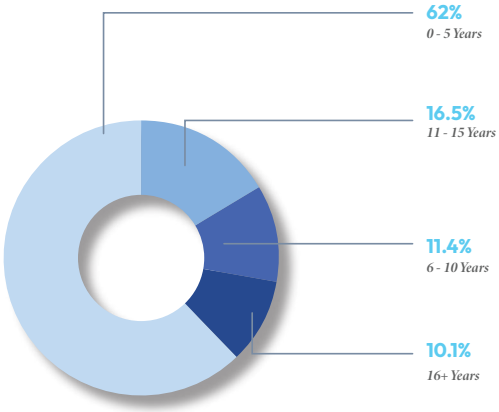
The primary objective of the survey was to gather comprehensive data shedding light on various aspects of data privacy and governance professionals' roles, skills, aspirations, remuneration and the prevailing trends that influence their work. By analysing the responses obtained from the survey, combined with in-depth analysis, this report presents a detailed exploration of the challenges and opportunities faced by these professionals.

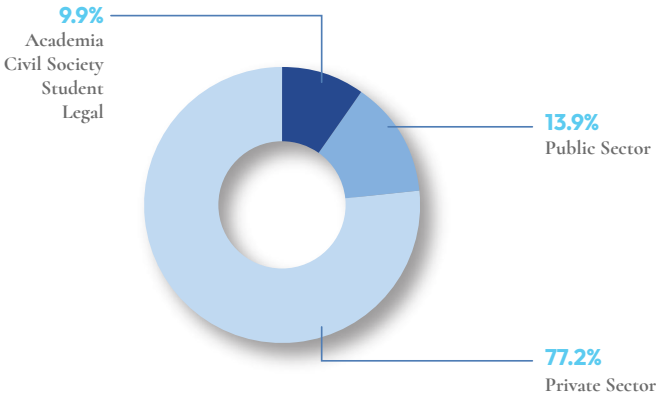
Experience

This survey unveiled a diverse distribution of experience levels among respondents, encompassing cumulative professional experience over and above data protection expertise.

Specifically, 62% of respondents had 1-5 years of experience, 16.5% had 11-15 years, 11.4% had 6-10 years, and 10.1% had 16+ years. This indicates a significant influx of emerging professionals, a notable segment of seasoned practitioners, and a valuable mid-career cohort.

The presence of experienced veterans reflects a dynamic profession with a healthy mix of fresh talent and dedicated experts driving advancements in data protection practices.



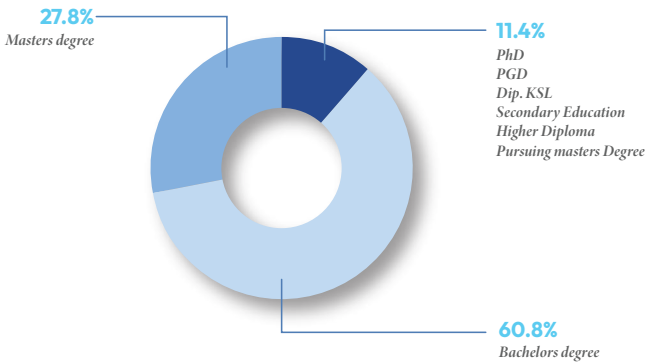


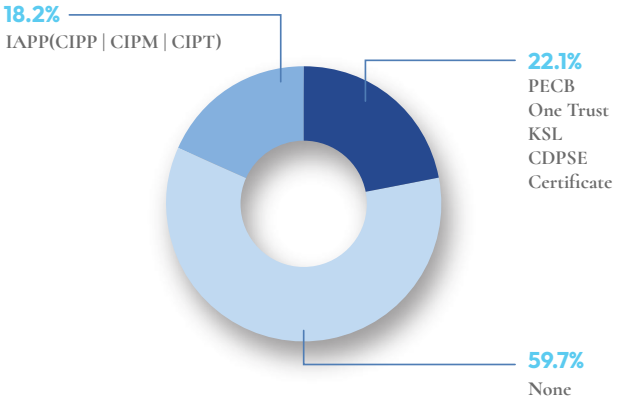
Sector Distribution

The survey revealed that 77.2% of respondents work in the private sector, while 13.9% are in the public sector. Academia, civil society, legal, and students, make up the remaining portion, with academia forming the majority. This distribution showcases the significant presence of data protection professionals in private organizations, the importance of academia in shaping the field, and the collaborative efforts across diverse sectors to promote responsible data practices.

Qualifications

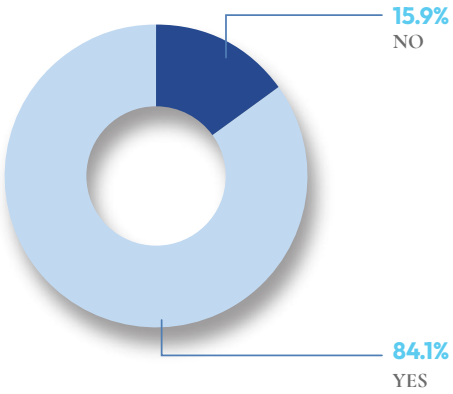
According to the survey results, a majority of the respondents (60.8%) have completed their bachelor's degree, while 27.8% hold a master's degree. The remaining 11.4% have varied educational backgrounds, including PHD, PGD, secondary education, and higher diploma. The respondents mainly consist of university graduates, with a significant number of professionals possessing advanced degrees, and a diverse mix of educational paths within the data protection profession.





Professional Certification

The survey revealed that 59.7% of respondents did not possess professional qualifications specific to data privacy and governance. However, 18.2% had completed at least one IAPP training, demonstrating their dedication to specialized education in the field. The remaining respondents held diverse qualifications outside of the IAPP training, showcasing the breadth of expertise and backgrounds within the data protection profession.

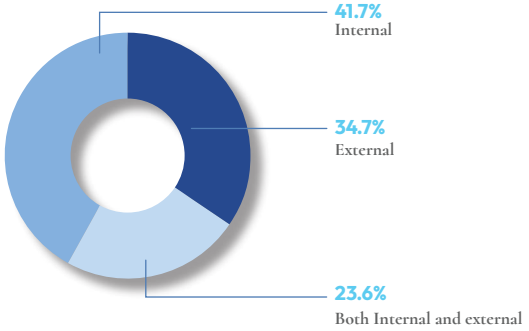


Other Data Protection Training

The survey findings show that 84.1% of respondents received data protection training, even if not resulting in certification. This reflects a positive trend in addressing data protection concerns. However, 15.9% reported no training, highlighting the need for increased education and awareness. Ongoing training and the promotion of best practices are crucial for a well-prepared workforce in data protection. Trainings were mainly offered by; CIPIT, The Lawyers Hub, One Trust & KeSIG

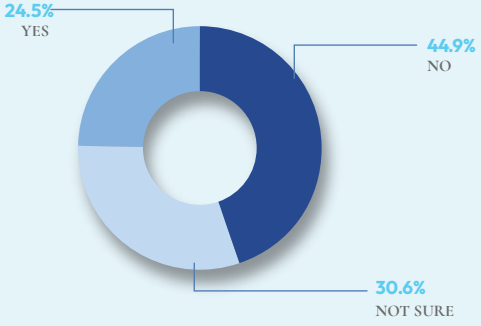
Type of DPO Role

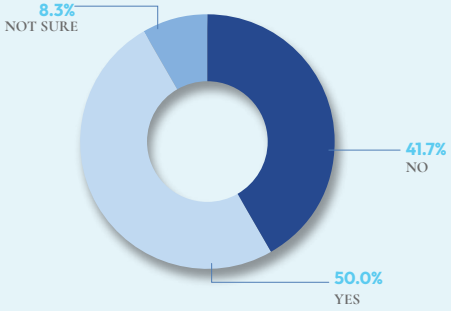
The survey findings reveal diverse role distributions among respondents, with 41.7% as internal Data Protection Officers (DPOs), 34.7% as external DPOs, and 23.6% fulfilling both internal and external DPO responsibilities. This highlights the flexibility in addressing data protection needs, combining in-house and outsourced expertise.



Internal DPOs

Among internal DPOs, 44.9% operated outside the C-suite, while 24.5% held C-suite positions, reflecting varying organizational structures and recognition of data protection as a strategic priority. Conflict of interest was reported by 50% of internal DPOs, while 41.7% reported no conflicts, and 8.3% were uncertain. These findings underscore the complexity and dynamics internal DPOs face in balancing data protection obligations and organizational interests.

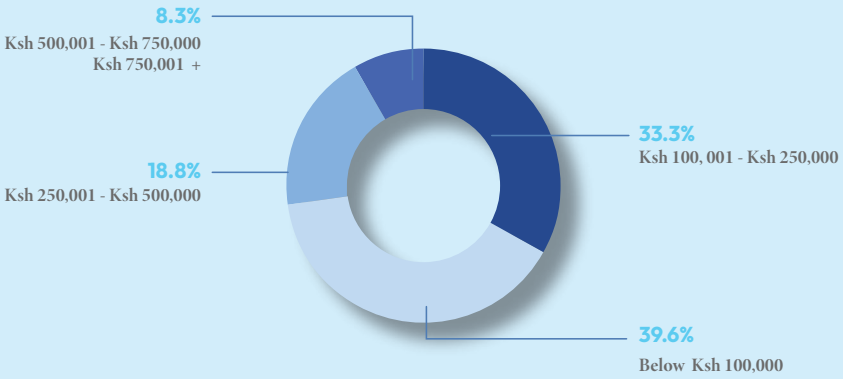




Internal DPO Additional Responsibilities

The survey revealed that respondents held various roles in addition to the DPO position. These roles included legal operations, as well as positions in risk and compliance, communications and marketing, ICT function, IT security and administration, regulatory compliance, internal control among others. This diverse range of roles highlights the multifaceted responsibilities and expertise of professionals in the data protection field, covering legal, risk, IT, compliance, and operational aspects.

Internal DPO Remuneration

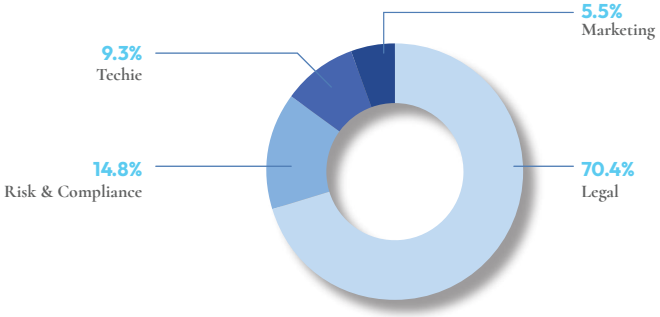


The survey findings on earnings of internal Data Protection Officers (DPOs) indicate a diverse distribution. Among respondents who disclosed their income, 39.6% earned less than KES 100,000, 33.3% earned between KES 100,001 and KES 250,000, and 18.8% earned between KES 250,001 and KES 500,000. Only 6% earned above KES 750,000, while 2% fell between KES 500,001 and KES 750,000. These findings highlight the range of salaries among internal DPOs, influenced by factors such as experience, qualifications, and organizational context.

Internal DPO Role Challenges

Based on the survey, here is a list of the top ten challenges respondents identified as areas of concern faced by internal DPOs

- Lack of understanding and prioritization of the DPO role within the organization.
- Insufficient investment and resources dedicated to the DPO role.
- Knowledge gaps and lack of awareness about data protection among staff and management.
- Limited experienced support available to the DPO.
- Challenges in convincing the board to hire a DPO.
- Inadequate salary and cooperation from management.
- Micromanagement and lack of independence for the DPO.
- Work overload with insufficient compensation.
- Conflicting roles and responsibilities assigned to the DPO.
- Compliance challenges, including limited resources, internal resistance, and conflicting interests.



External DPOs

The survey revealed that 70.4% of external DPOs have a legal professional background, indicating the importance of legal expertise in external data protection services. Additionally, 14.8% have a background in risk and compliance, emphasizing regulatory adherence and risk mitigation. Interestingly, 9.3% of external DPOs have a technical background, highlighting the growing need for technology skills in managing data protection obligations.

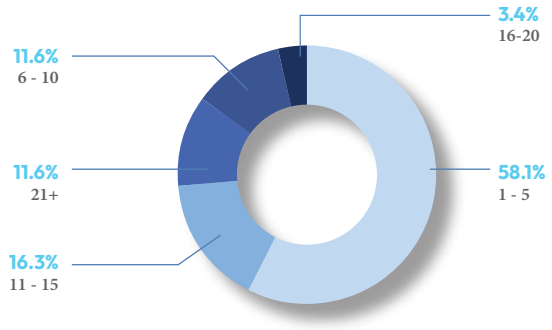
External DPO Services

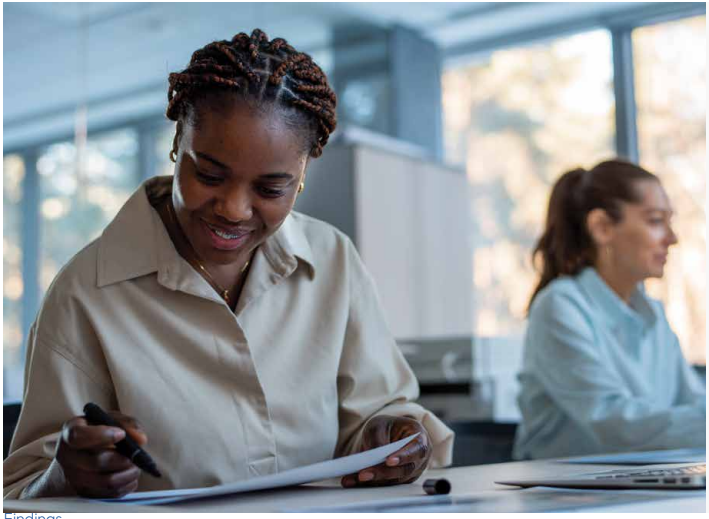
Based on the survey, here is a list of common services sought after from external Data Protection Officers (DPOs):

- Policy drafting and legal frameworks training.
- Document review.
- Data Protection Impact Assessments (DPIA)
- Compliance review and sensitization training.
- ODPC Registration
- Full data protection compliance services, including policy drafting, training, and registration.

Number of Successful assignments

The survey findings indicate that external DPOs have varying workloads as of June 2023. 58.1% of respondents reported handling between 1-5 assignments, 16.3% handled 11-15 assignments, and 11.6% managed over 21 assignments. These findings highlight the diversity in caseloads for external DPOs, with some managing a moderate workload while others handle a higher volume of cases.





External DPO Fee Range

The survey findings reveal diverse charging rates among external DPOs. 42.9% charge between KES 0 to KES 10,000 per day, 21.4% charge between KES 20,001 and KES 30,000 per day, 19% charge over KES 50,000 per day, and 11.9% charge between KES 10,001 and KES 20,000 per day. These findings highlight a range of pricing options within the market, accommodating different budgetary needs. The rates reflect the value attributed to the expertise and services provided by external DPOs.

DPIA pricing

The survey findings highlight the lack of consistent pricing for Data Protection Impact Assessments (DPIAs), with rates varying widely from as low as KES 5,000 to exceeding KES 500,000. This indicates a potential lack of understanding about the scope and complexity of DPIAs. The differing rates can be attributed to varying interpretations of the requirements and levels of expertise among external DPOs.

External DPO Role Challenges

Based on the survey, here is a list of 6 challenges highlighted by external DPOs

- **Lack of understanding and awareness about data protection among organizations and individuals.**
- **Unclear demarcation of the DPO role and its relationship with cyber security.**
- **Resistance to change and organizations' reluctance to invest in data protection.**
- **Undercutting and pricing inconsistencies within the market.**
- **Limited availability and access to relevant information from different departments within organizations.**
- **Insufficient support from key stakeholders, including management and decision-makers.**

Key Take aways

The survey findings provide valuable insights into the landscape of data protection professionals and the challenges they face. Four key takeaways include:

01

Diverse Roles and Backgrounds

The survey reveals a diverse range of roles and professional backgrounds among data protection professionals, including legal, risk and compliance, and technology expertise. This highlights the multidimensional nature of data protection and the need for collaboration across different domains.

02

Varying Workloads and Pricing

The survey highlights variations in workloads and pricing among external Data Protection Officers (DPOs). While some DPOs handle a moderate number of briefs, others face a higher volume of cases. Pricing for services, including DPIAs, also varies widely, indicating a need for better understanding and standardization in the market.

03

Challenges and Resistance

The survey identifies several challenges faced by both internal and external DPOs, such as resistance to change, lack of understanding, and limited support from key stakeholders. These challenges highlight the importance of raising awareness, promoting education, and advocating for the role and value of data protection professionals.

04

Opportunities for Improvement

The survey findings underscore the need for continuous training, networking, and collaboration among DPOs. It highlights the importance of standardizing practices, providing mentorship programs, and addressing remuneration issues to ensure the growth and professionalism of the data protection field.

05

Need to clarify internal DPO role

The survey revealed the inconsistency in defining the role of the internal DPO across different organisations. This is despite the guidance in the Act that the role should avoid being held by persons with other conflicting roles given that it is an audit role. There's need for standardisation of internal job descriptions and reporting structures as well as compensation packages across the board.

Consideration of the way forward

To address the challenges and further enhance the data protection profession, several measures can be taken:

01

Awareness and Education

Efforts should be made to raise awareness among organizations, individuals, and key stakeholders about the importance of investing in data protection programs.

02

Collaboration and Networking

Establishing more platforms for networking, knowledge sharing, and collaboration among data protection professionals such as the DPGSK Continuous Professional Development (CPD) webinars is essential. This can be done through conferences, and regular meetups to facilitate learning, exchange of best practices, and collective advocacy

03

Standardization and Certification

Developing standardized guidelines, procedures, and pricing structures for data protection services, including DPIAs, can promote consistency and professionalism. Certification programs should be enhanced to ensure the competence and credibility of data protection professionals. Price recommendations can be provided to establish fair and reasonable rates for data protection services especially for external DPOs.

To learn more about Data Governance Pros Kenya and how to get involved, please contact us at dataprivacyke@gmail.com. You can also connect with us on LinkedIn at Data Governance Pros Kenya and follow us on Twitter at @DataGovProsKe.

Edited By

James Mbugua
Treasurer DPGSK

Philip Kisaka
Assistant Secretary DPGSK