



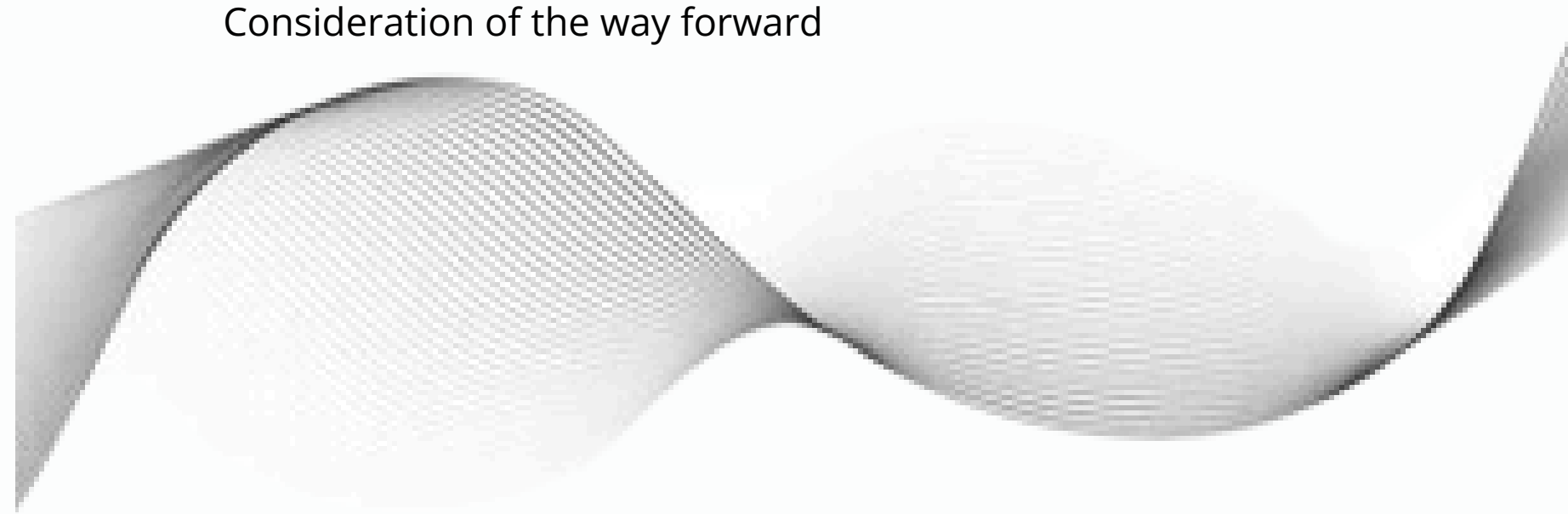
DATA PRIVACY & GOVERNANCE SOCIETY

Privacy and Governance Professionals Survey Report

June 2024

Contents

About DPGSK	01
Preface	02
Privacy and Governance Professional Survey	03
Membership & Demographics	04
Internal DPOs	10
External DPOs	15
DPGSK Member interaction	21
Key Takeaways	22
Consideration of the way forward	23



The Data Privacy and Governance Society of Kenya (DPGSK) is a leading organization under the Societies Act, dedicated to fostering a vibrant community of data privacy and governance professionals across Kenya. Committed to inclusivity and excellence, DPGSK promotes the lawful and ethical utilization of data while safeguarding the interests of its diverse membership. DPGSK remains steadfast in its mission to achieve its objectives through various multifaceted 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 broad spectrum of professionals, ranging from private practitioners and in-house data protection officers to academia, civil society, young professionals, and university students. DPGSK offers a variety of membership categories tailored to meet the unique needs and aspirations of individuals and organizations alike and together, we continue to lead the charge in shaping a responsible and transparent digital future for Kenya and beyond.



Preface

As data continues to influence every facet of society, understanding the experiences and challenges faced by data privacy and governance professionals is crucial. The Data Privacy and Governance Society of Kenya (DPGSK) recognizes the pivotal role these professionals play in ensuring compliance across various economic sectors.

To gain deeper insights into this profession, the DPGSK conducted a comprehensive survey among its members from the public sector, private sector, academia, and civil society. This survey aimed to provide an in-depth analysis of the current landscape, focusing on their roles, skills, aspirations, and the trends shaping their work. The valuable input from these professionals forms the cornerstone of this report.

This report delves into various aspects of the data privacy and governance profession. It highlights the educational backgrounds, industry affiliations, and years of experience of the respondents. It also sheds light on the challenges they face and offers recommendations to address these issues.

The insights gleaned from this report equip the DPGSK and its partners with the knowledge necessary to enhance the data privacy and governance field. We extend our sincere gratitude to all the participants who shared their valuable experiences and insights, making this survey report possible. Their contributions not only provide a snapshot of the profession but also guide us in understanding the necessary steps for improvement.

By highlighting the current state of the profession, we hope this report will be a valuable resource for data privacy and governance professionals, organizations, and policymakers. Our aim is to spark discussions, encourage collaborations, and advance the pursuit of excellence in data privacy and governance.

Sincerely,

Mugambi Laibuta
Chairperson, DPGSK

Privacy and Governance Professionals’ Survey

Background

The Data Privacy and Governance Society of Kenya (DPGSK) acknowledges the growing importance of data privacy and governance experts in ensuring regulatory adherence across various economic sectors. As data increasingly influences all aspects of our lives, understanding the experiences and challenges faced by these professionals is essential. To this end, DPGSK conducted a survey among its members, seeking to offer a detailed overview of the current landscape of data privacy and governance in Kenya.

Respondents

The survey engaged a wide range of professionals across multiple sectors, including those in the public sector, private industry, academia, and civil society. By gathering perspectives from individuals with varied backgrounds and affiliations, the survey aimed to provide a comprehensive view of the data privacy and governance profession.

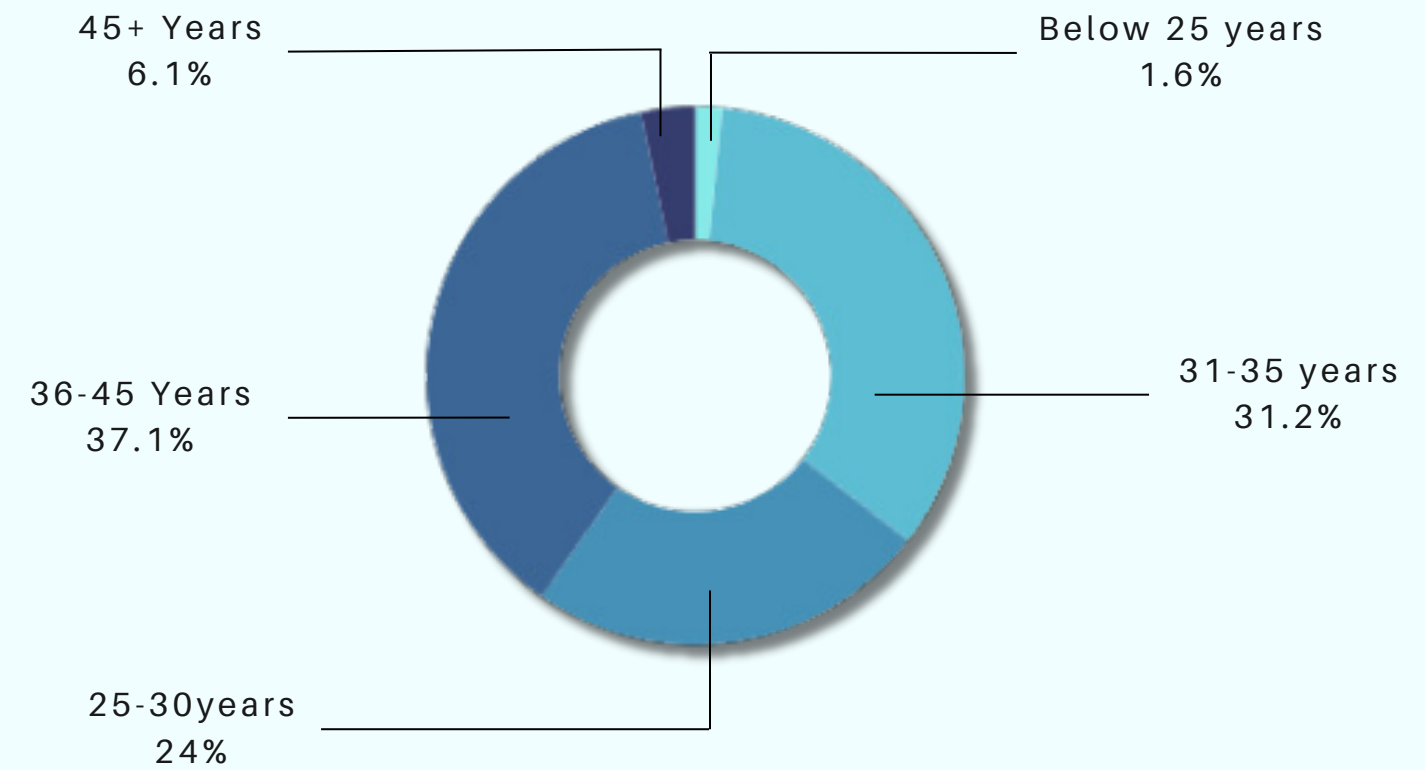
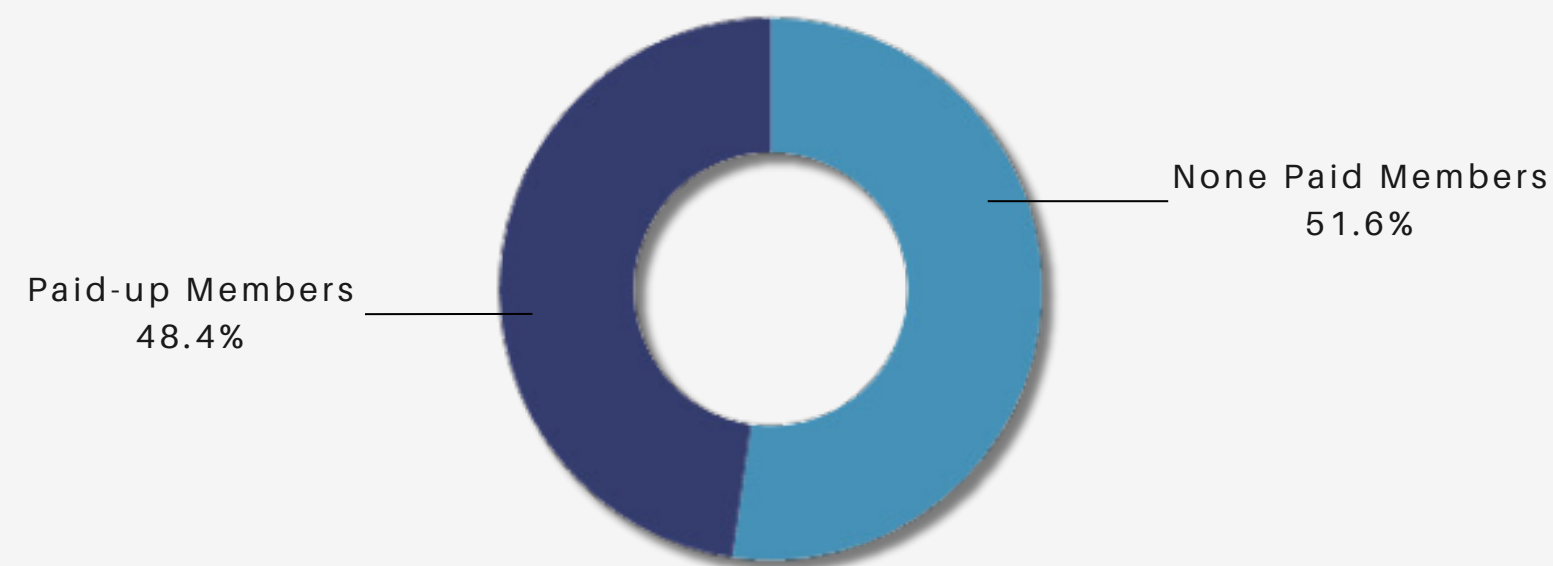
Survey

The main goal of the survey was to collect detailed information on various facets of data concerning privacy and governance professionals, including their roles, skills, aspirations, remuneration, and the prevailing trends shaping their work. Through an analysis of the survey responses and an in-depth examination of the various aspects, this report offers a thorough exploration of the challenges and opportunities encountered by these professionals.

DATA PRIVACY & GOVERNANCE MEMBERS

Number of Paid-up Members

The survey findings show a positive trend with 48.4% of respondents now being fully paid-up members. This significant proportion reflects the growing recognition of the value of membership. However, 51.6% reported not being paid members, highlighting the need to implement targeted outreach initiatives, offering incentives such as discounted membership fees for early renewals, and enhanced member benefits. Additionally, raising awareness through educational campaigns and ensuring that more professionals see the tangible advantages of being active, fully paid-up members of our society.

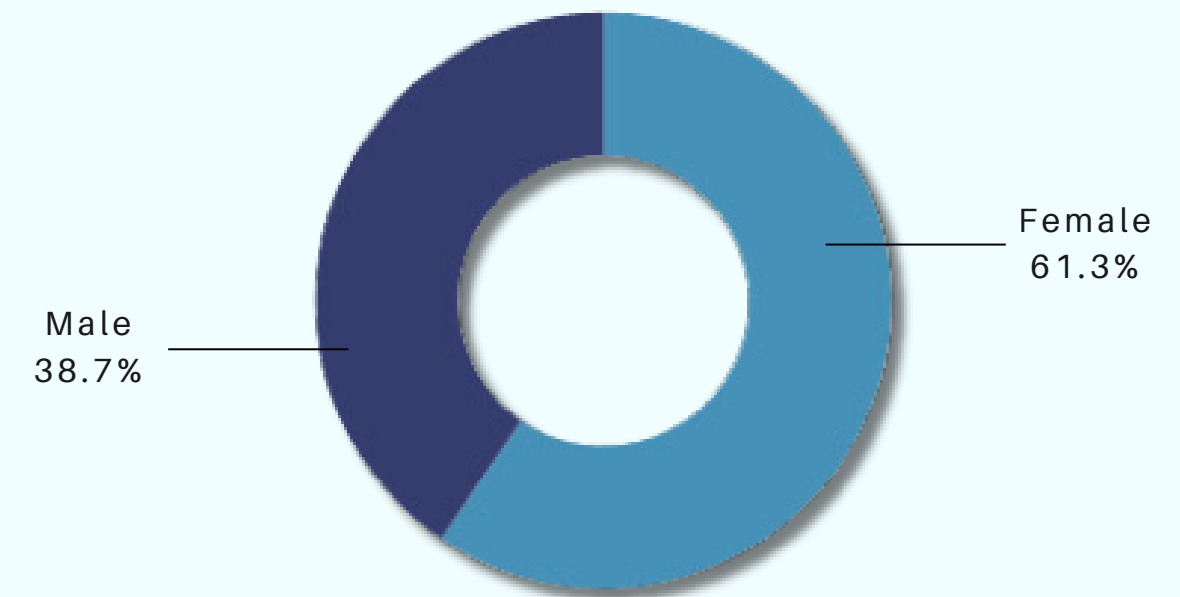


Age Demographics

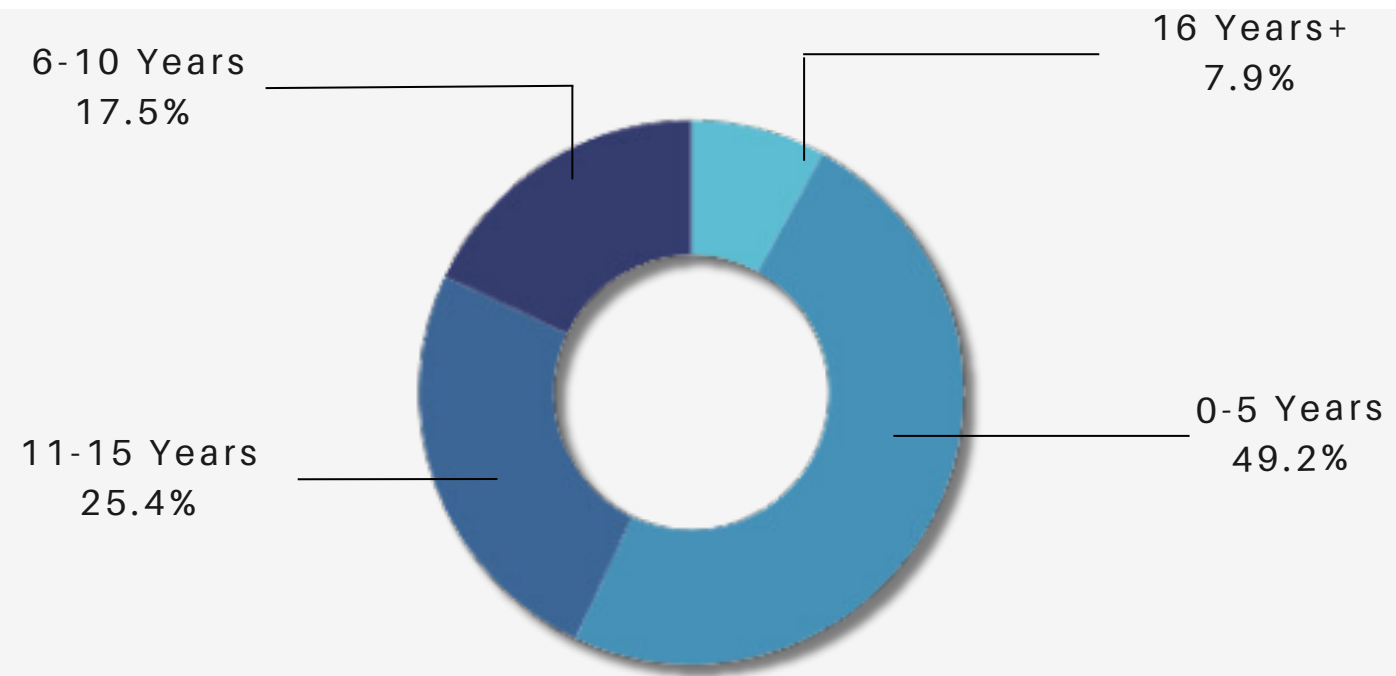
The survey on age demographics revealed that 33.9% of members are aged 26-30, highlighting a strong presence of young professionals. Additionally, 24.2% are between 31-35 years, representing those advancing in their careers. The largest group, 37.1%, is aged 36-45, indicating a significant proportion of seasoned professionals. The remaining members are either above 45 years or below 25 years. This diverse age range underscores the society's inclusivity and a well-balanced mix of fresh perspectives, mid-career dynamism, and veteran insights, enhancing the collective capability in data protection.



Gender Demographics



The survey revealed that among the respondents, 61.3% were female, indicating a predominant female representation. Gender inclusivity is vital for fostering diverse perspectives within our society. The significant participation of male respondents, comprising 38.7% of the total, underscores the importance of achieving gender balance. Encouraging greater participation from all genders can enhance discussions and decisions, leading to more comprehensive insights and inclusive outcomes in future discussions and membership initiatives focused on data privacy and governance..

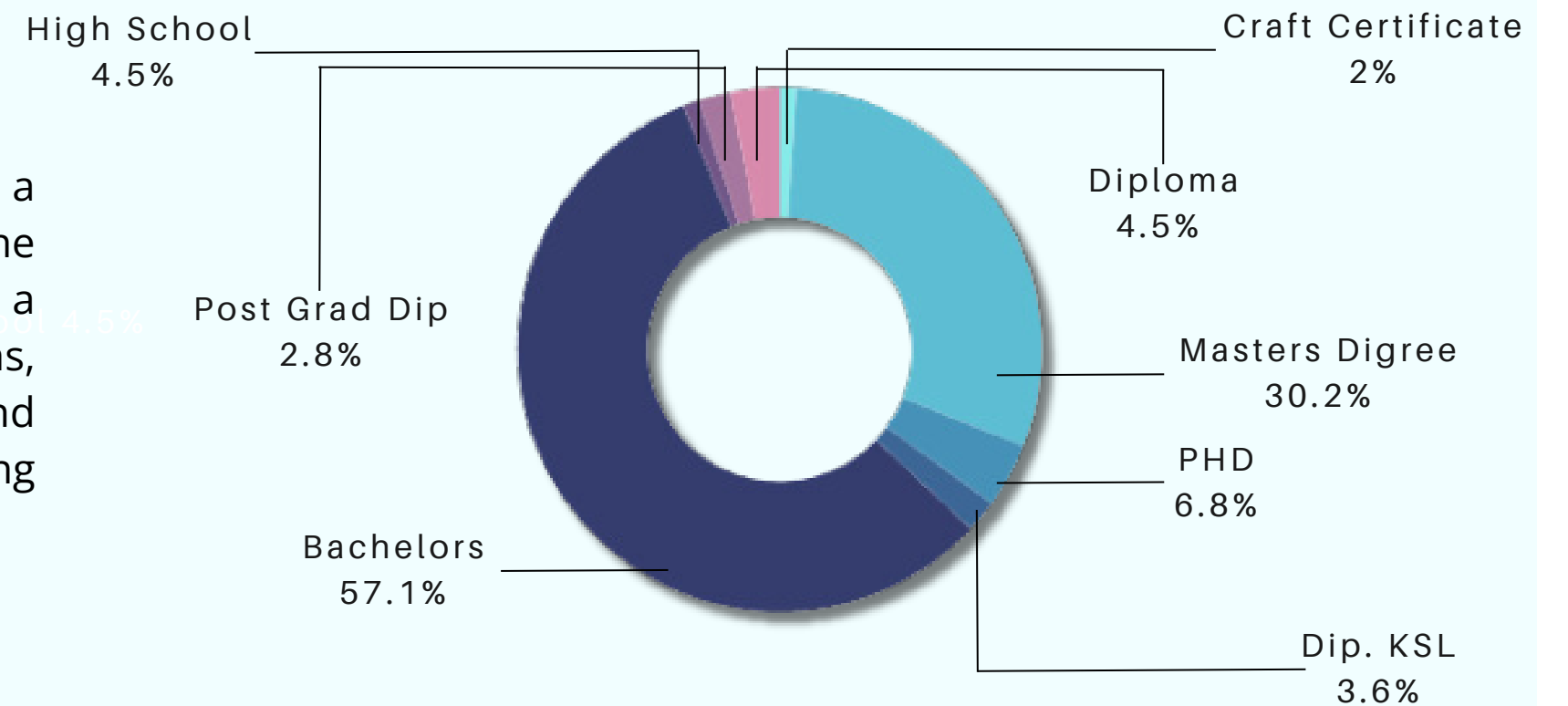


Professional Experience

According to the survey reports, the largest segment of respondents, comprising 49.2% has 0-5 years of experience, indicating a vibrant influx of newcomers eager to build their careers in data privacy and governance. This youthful energy is complemented by 17.5% of members who have 6-10 years of experience and 25.4% with 11-15 years of experience, highlighting a substantial group of seasoned professionals who bring depth and insights to the society. Finally, 7.9% of our members have over 16 years of experience, representing the veteran experts whose extensive knowledge is invaluable to our community. This distribution underscores a healthy balance of fresh talent and experienced professionals within DPGSK.

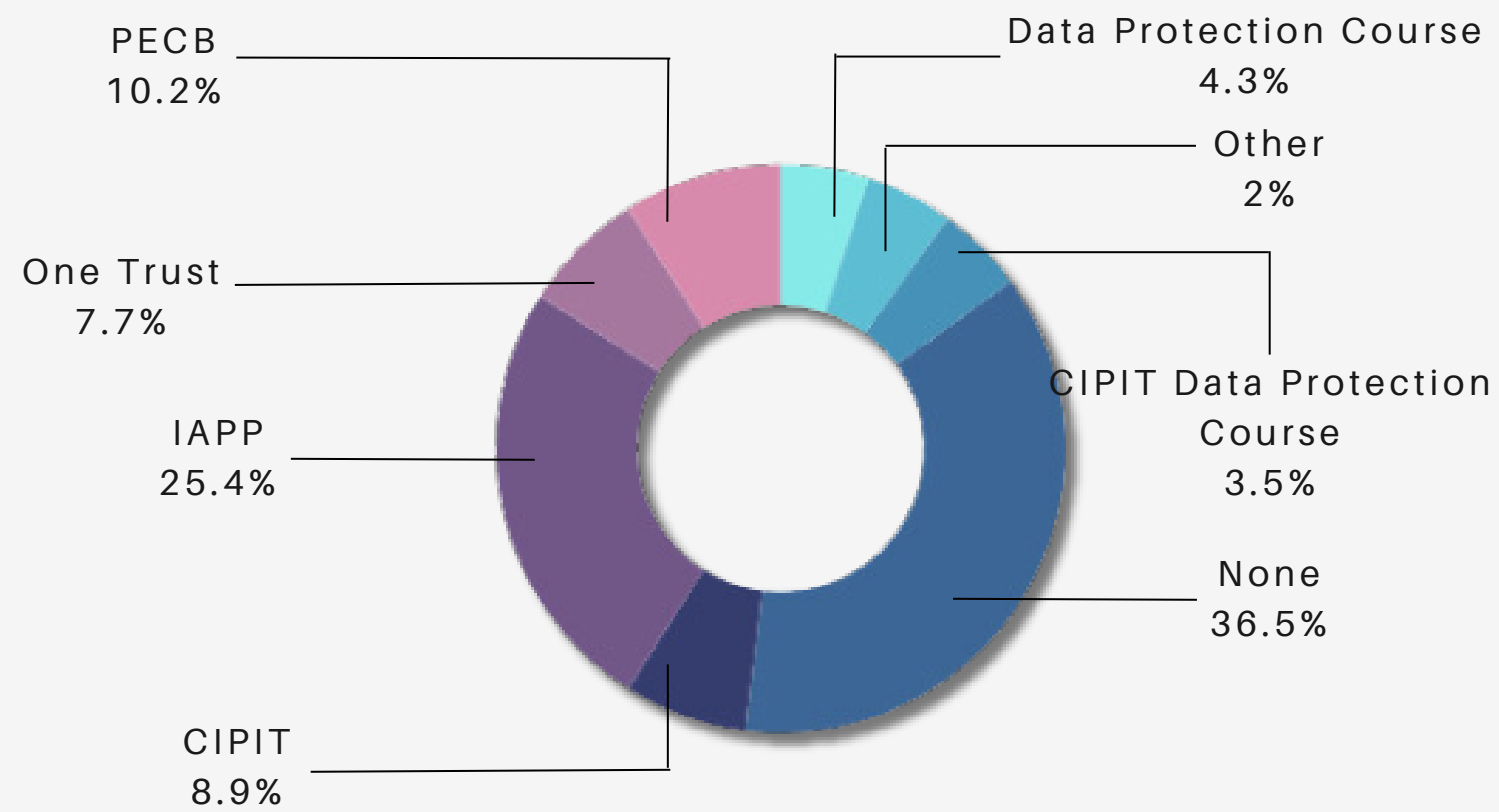
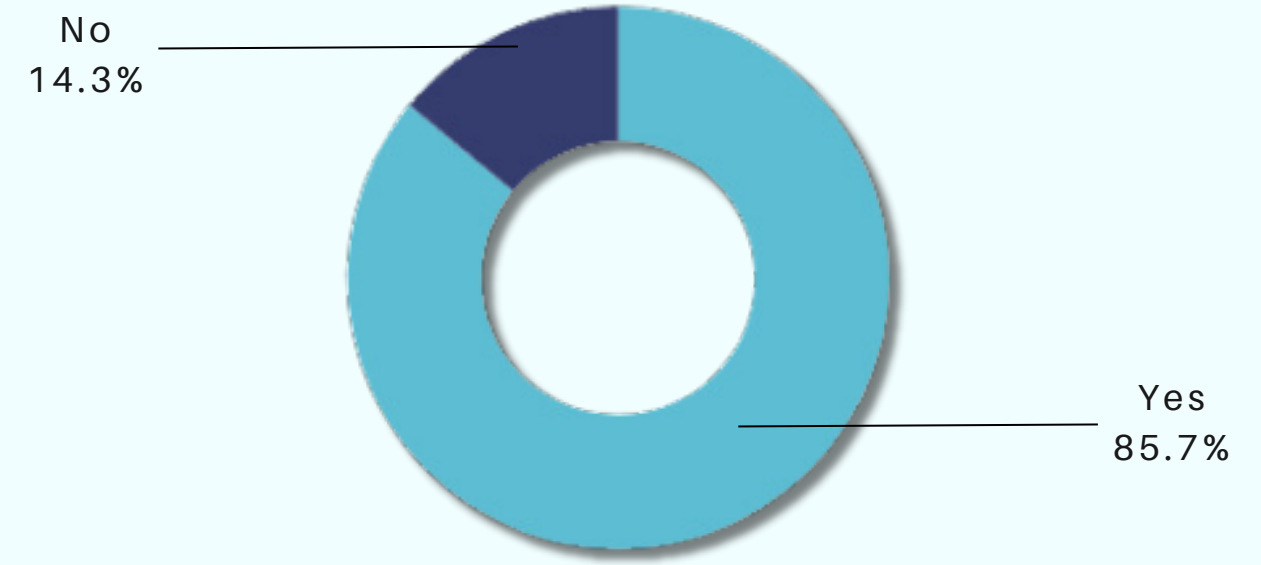
Academic Qualifications

The survey findings show that a majority of 57.1% of respondents hold a bachelor's degree, indicating that a solid undergraduate education is the foundation for many entering the field. Additionally, 30.2% have attained a master's degree, and the remaining members possess a variety of qualifications, including high school certificates, diplomas, PhDs, postgraduate diplomas, and KSL diplomas. This diverse academic background enriches our society, fostering a culture of continuous learning and professional development.



Professional Data protection Training.

The survey findings show that a majority of the 63 respondents, 85.7%, of rhave professional qualifications as trained Data Protection Personnel, 14.3% have no formal training.

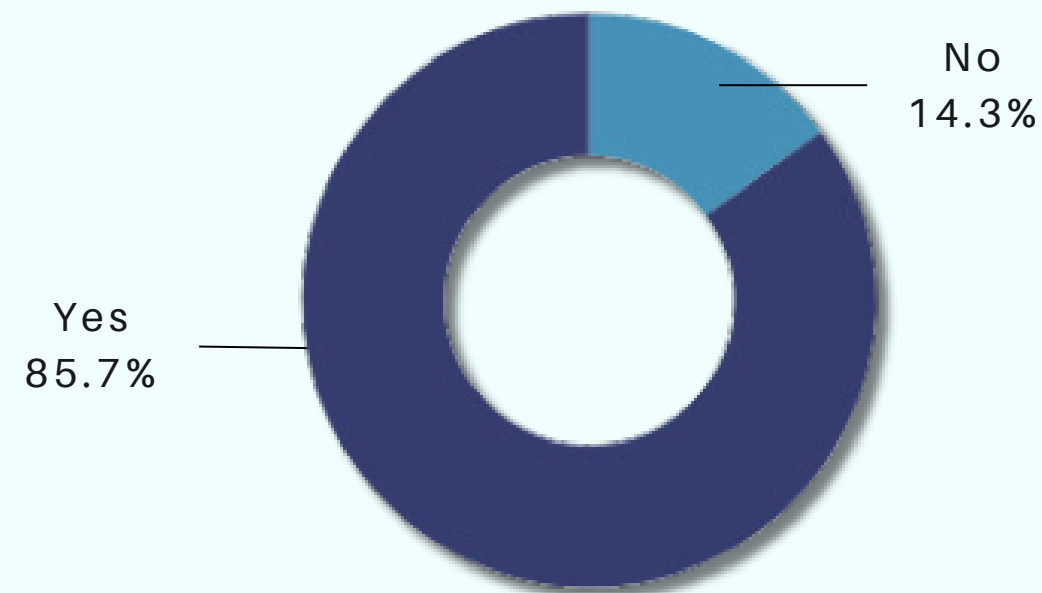


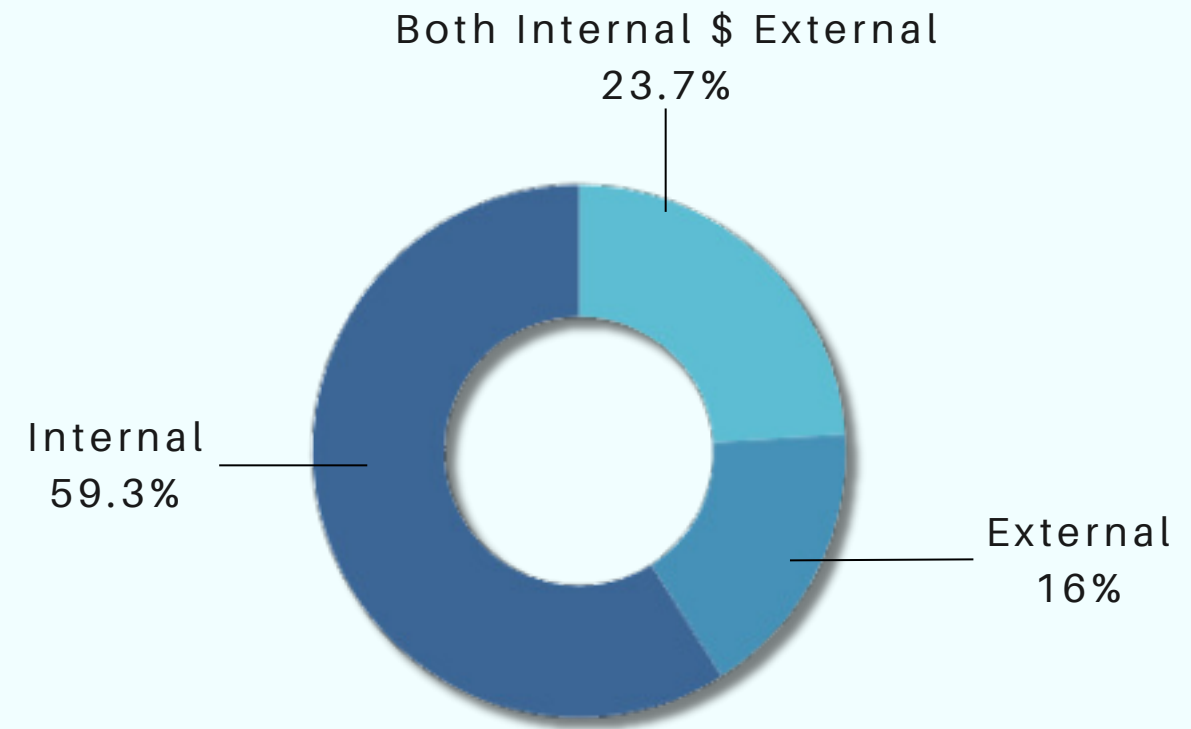
Professional Certifications

According to the survey 36.5% of respondents currently do not hold any data protection certification, indicating a significant opportunity for professional development within our community. Of those who are certified, 25.4% have obtained the International Association of Privacy Professionals (IAPP) certification, reflecting its prominence and recognition as a leading credential in the field. The remaining respondents are certified through various other programs, including PECB, One Trust, CIPIT, the CIPIT Data Protection Course, and other data protection courses. This diversity in certification underscores the various pathways available for professionals to gain specialized knowledge and credentials in data privacy. The variety of certifications also illustrates the comprehensive approach taken by DPGSK members to enhance their expertise and stay current with industry standards. To further support our members' professional growth, DPGSK aims to promote certification programs and provide resources and guidance to those seeking to enhance their qualifications and expertise in data protection.

Professional Data Protection Training

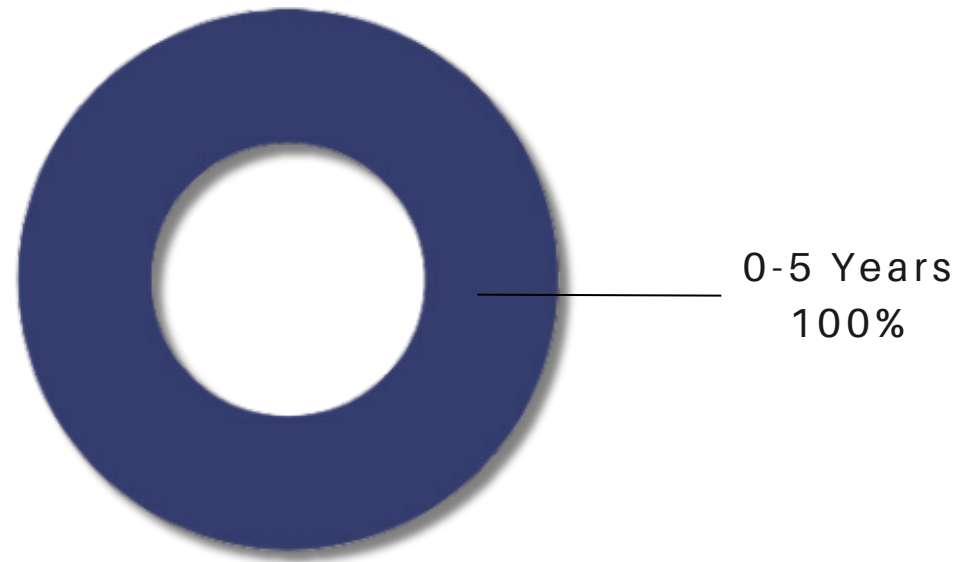
The survey reveals 85.7% of respondents have undergone professional training in data protection, underscoring a strong commitment to upholding high standards within the field.





Type of DPO Role

The survey reveals a diverse range of responsibilities with a majority of 59.3% serving as internal DPOs, indicating that many organizations are recognizing the importance of in-house expertise to manage their data protection needs. Meanwhile, 16.9% operate as external DPOs, highlighting the demand for specialized external consultancy services. Additionally, 23.7% of respondents fulfill both internal and external DPO roles, showcasing the flexibility and adaptability in today's dynamic data protection landscape.

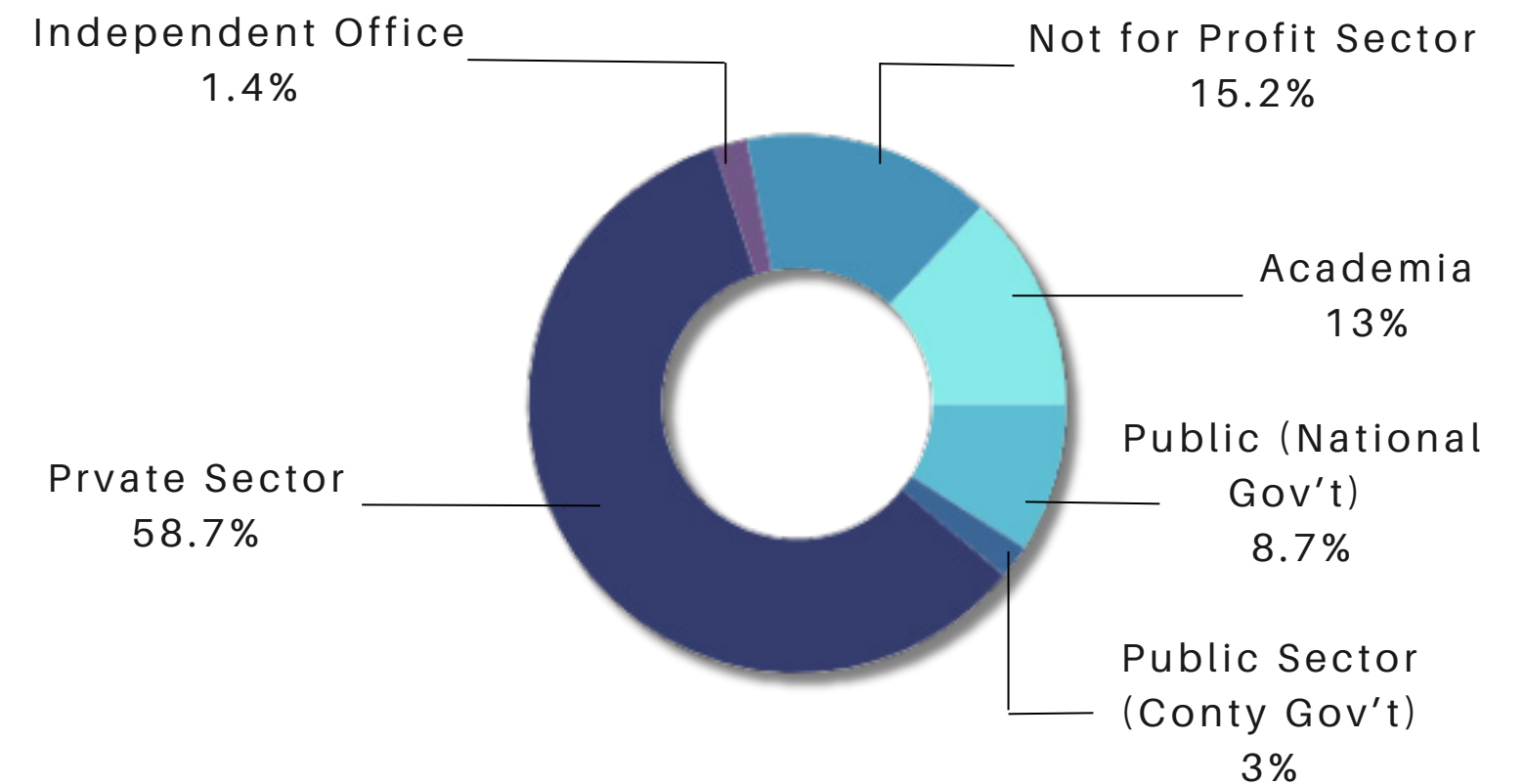


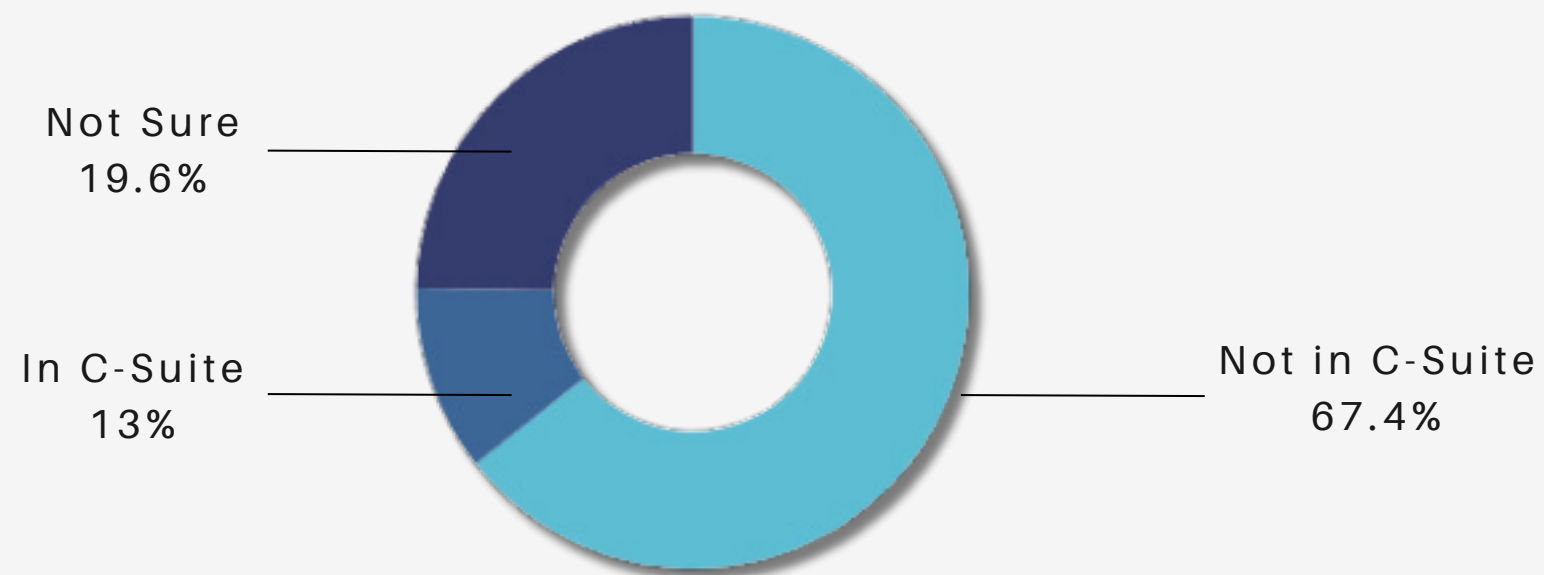
Internal DPOs

The survey revealed all respondents have served as internal DPOs for less than five years, indicating a relatively nascent but rapidly growing field

Sector of DPO Practice

Sector-wise, a majority of 58.7% are employed in the private sector, 15.2% in Non-profit organizations and 13% in Academia. Additionally, 8.7% work within the national government, demonstrating the public sector's efforts to enhance data governance. The remaining DPOs are distributed across county governments and independent offices, further illustrating the widespread need for data protection expertise across various domains. This distribution highlights the diverse application of data protection practices and the critical role DPOs play in ensuring compliance and safeguarding data across different sectors.



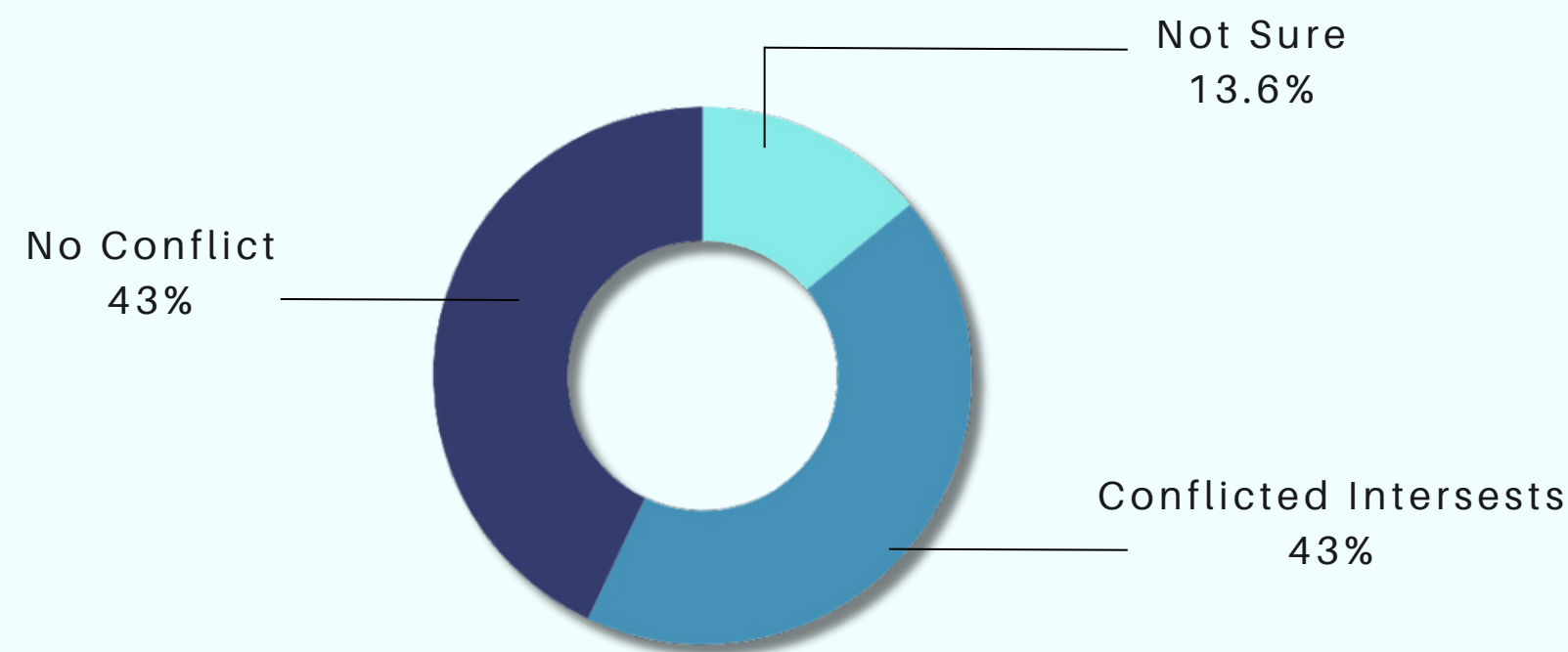


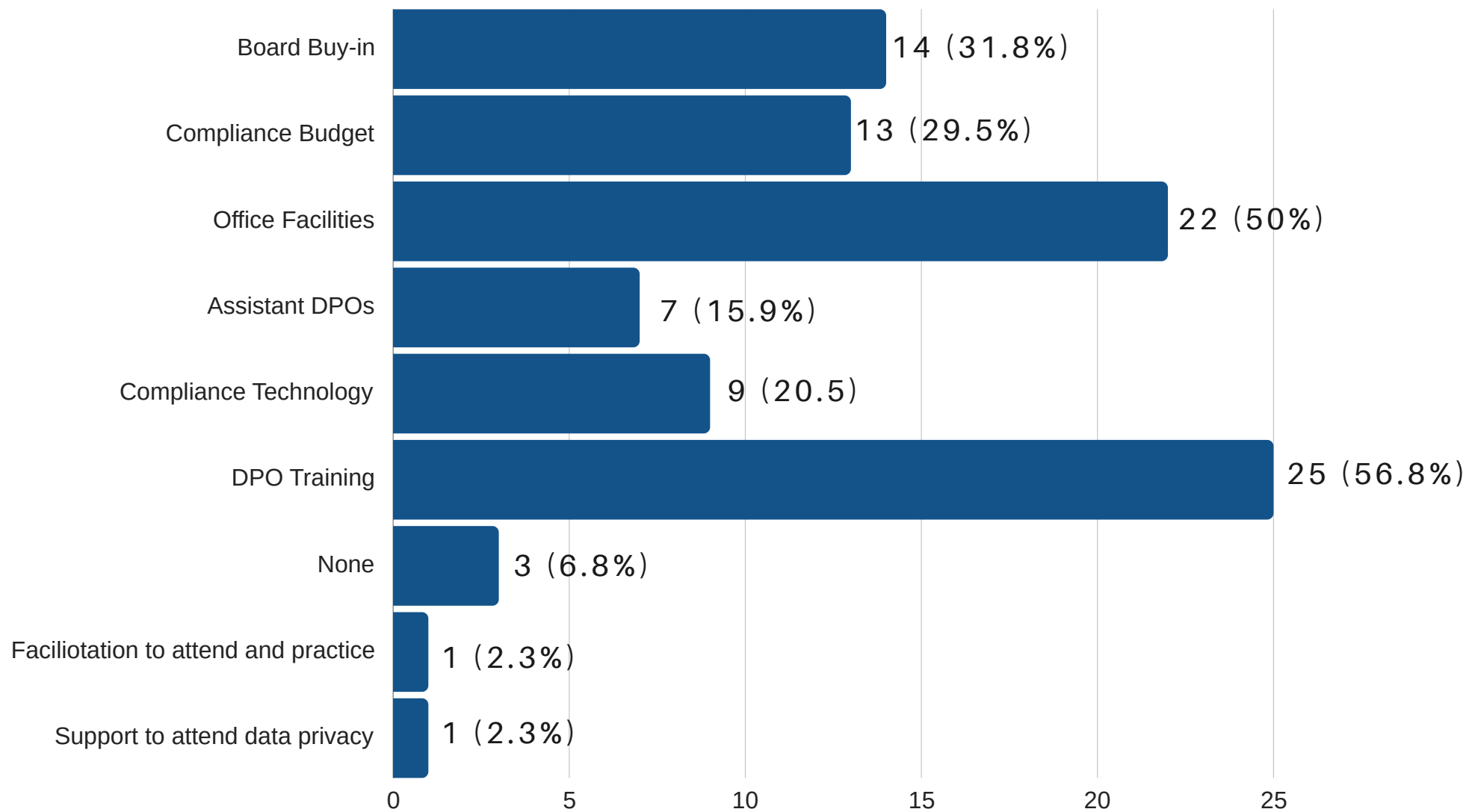
Internal DPO's in C-suite

Among the internal DPO's, 67.4% operated outside C-suite positions, suggesting that organizations may still view data protection as a specialized function rather than a core strategic role. Conversely, 13% of DPOs occupy C-suite roles, indicating that a growing number of organizations recognize the strategic importance of data protection. Meanwhile, 19.6% of respondents are unsure of their status, which may reflect a lack of clarity about their organizational hierarchy or evolving roles within their companies.

Conflicted Interests

Conflict of interest was reported by 43.5% of DPO's, while an equal percentage reported no conflict. Additionally, 13% of respondents are unsure, indicating a possible lack of awareness or clarity regarding what constitutes a conflict in their professional environment. These findings underscore the need for clearer guidelines and training on identifying and managing conflicts of interest.

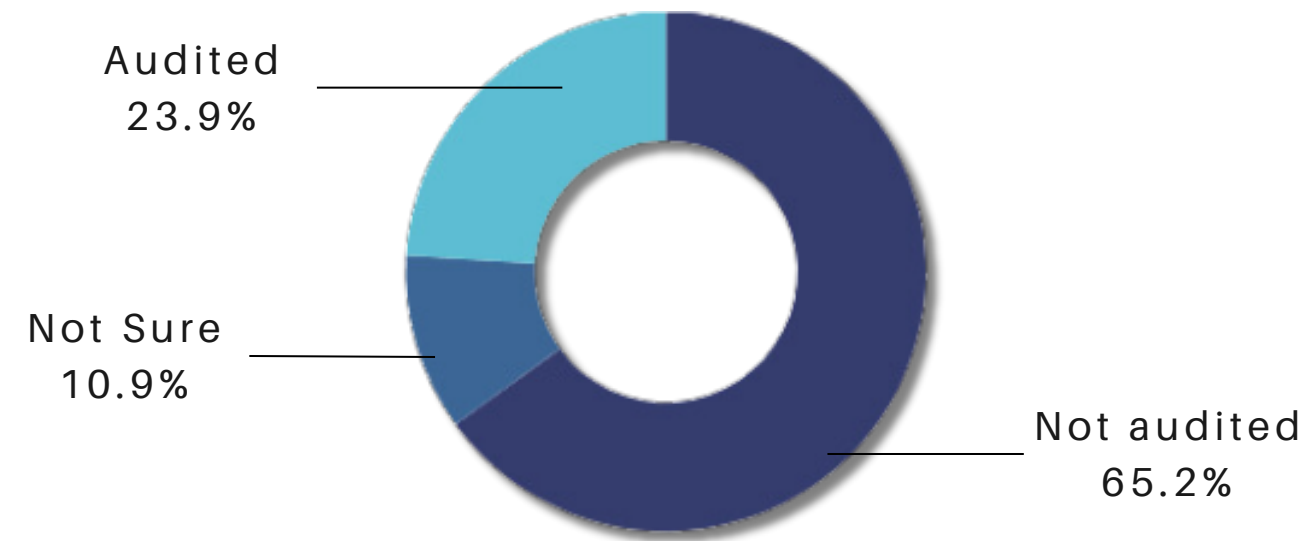




Organizational Support

Among internal DPO's 56.8% receive DPO training, indicating a commitment to professional development. Office facilities are provided to 50% of DPOs, board buy-in is secured for 31.8% of DPOs with a compliance budget allocated for 29.5%.

However, only 15.9% of DPOs have assistant DPOs, suggesting limited personnel support. Compliance technology is available to 20.5% of respondents, with facilitation and support to attend relevant events are critically low at 2.3%, which could hinder continuous learning and networking opportunities. Alarmingly, 6.8% of DPOs report receiving no support, pointing to a pressing need for organizations to enhance their support structures.

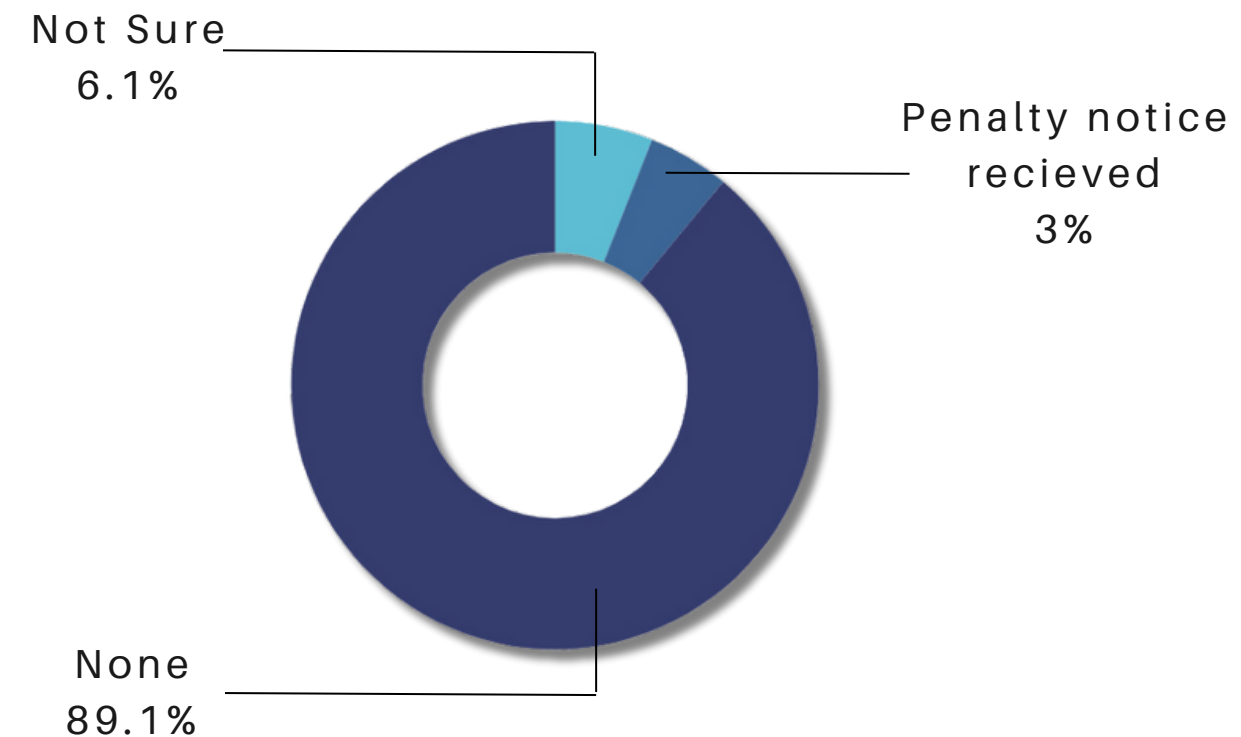


Organizational audits by ODPC

Based on the survey, a majority of 65.2% of DPOs report not having been audited, indicating that many organizations have yet to undergo formal scrutiny of their data protection practices. In contrast, 23.9% of respondents have experienced an ODPC audit, reflecting a subset of organizations that have been actively engaged with regulatory compliance checks. Meanwhile, 10.9% of DPOs are unsure if their organization has been audited, suggesting a possible lack of communication or awareness within those entities. These findings underscore the importance of increasing awareness and preparedness for ODPC audits, as well as the need for more comprehensive and transparent auditing processes to ensure all organizations adhere to data protection regulations effectively.

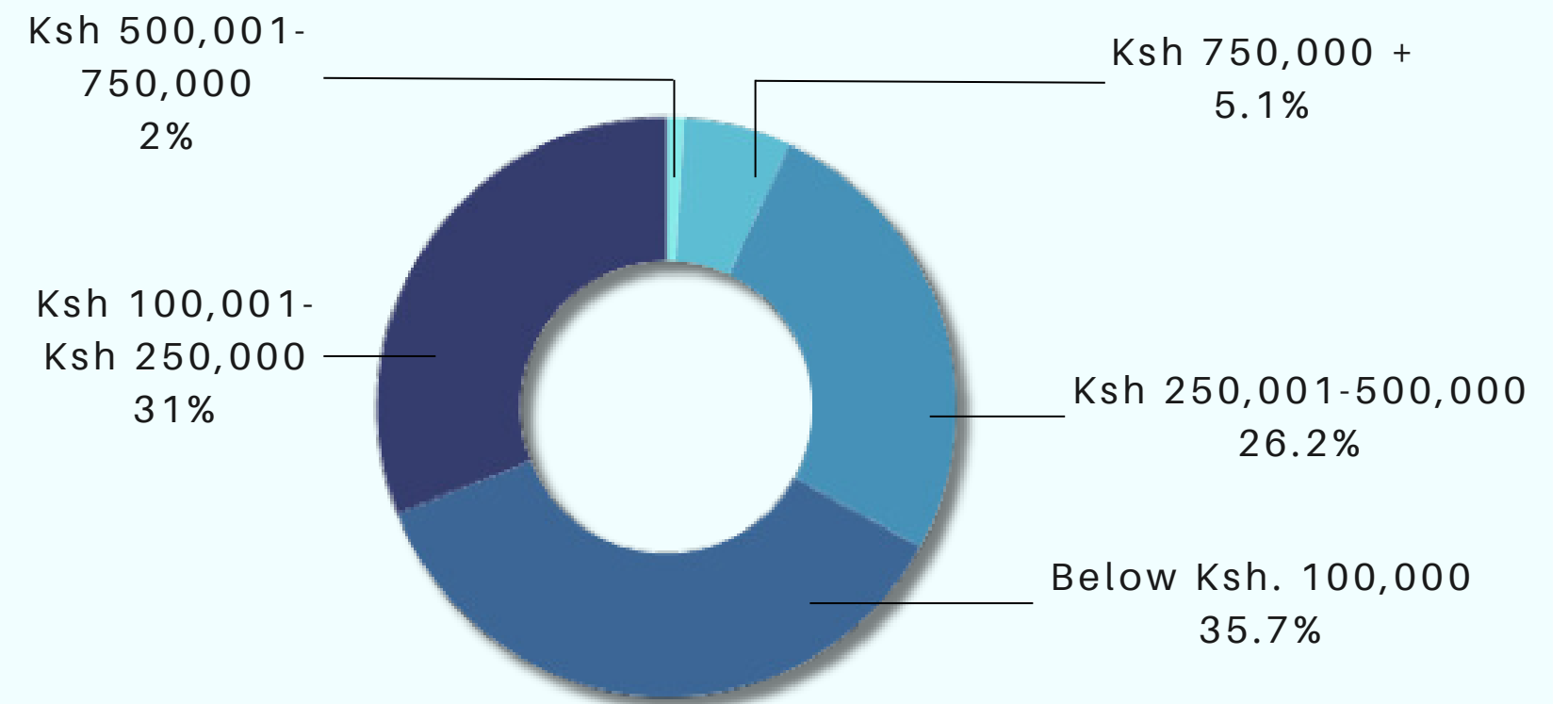
Penalties Received

An overwhelming 89.1% of organizations report not having received any penalty notices, with the remaining organizations have either received penalty notices or are unsure of their status.



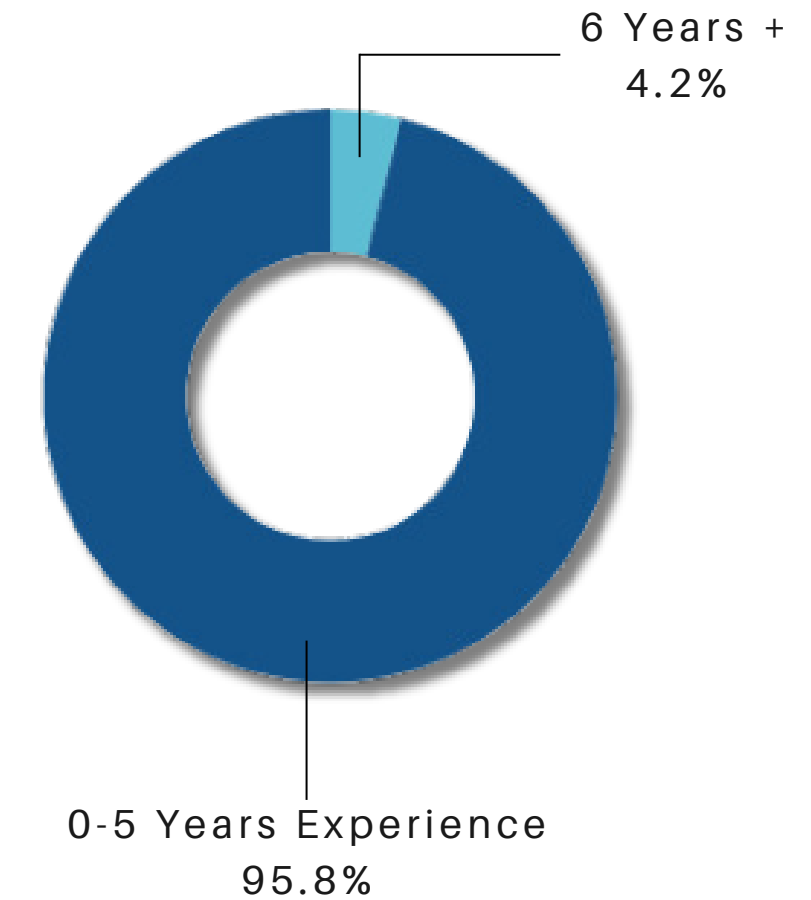
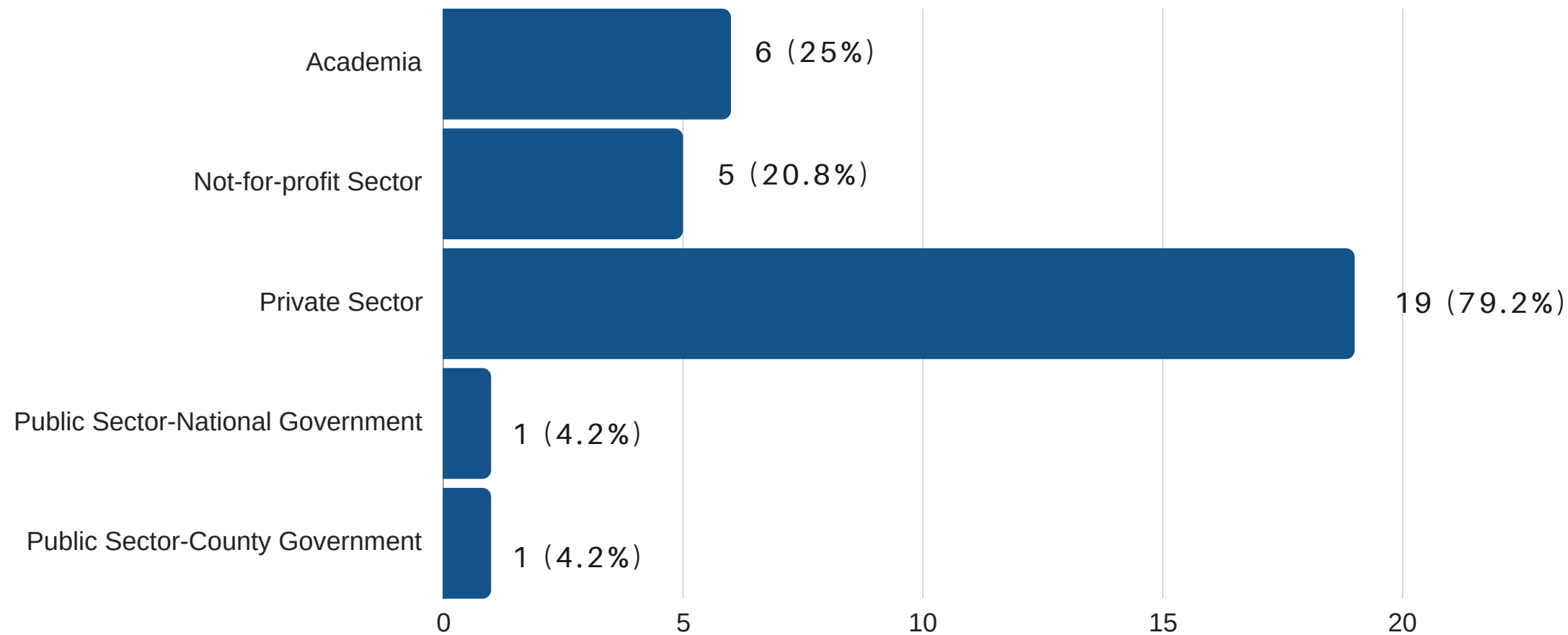
Internal DPO remuneration

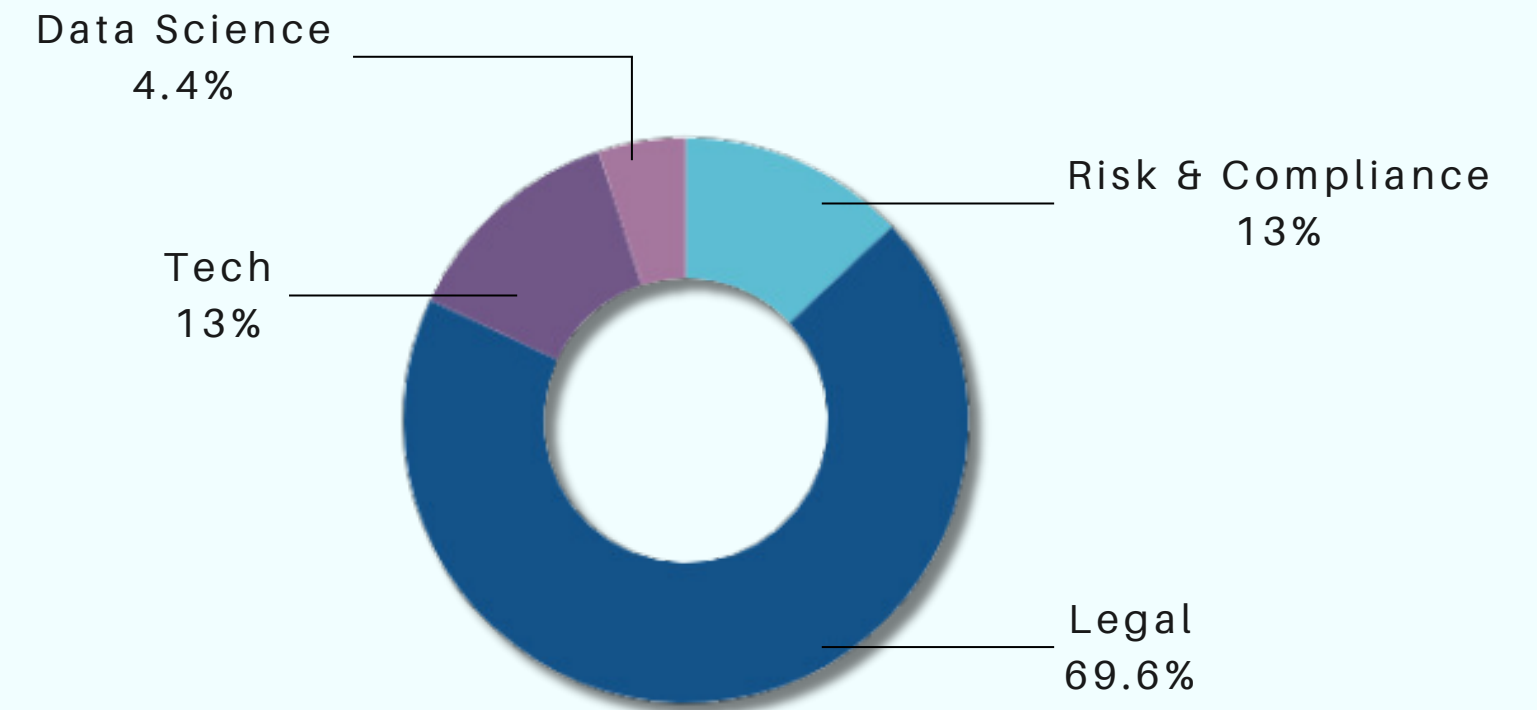
The survey findings on earnings of internal Data Protection Officers (DPOs) indicate a diverse distribution. Among respondents who disclosed their income, 35.7% earned less than KES 100,000, 31% earned between KES 100,001 and KES 250,000, and 26.2% earned between KES 250,001 and KES 500,000, with the remaining 7.1% earning above KES 500,001. These findings highlight the range of salaries among internal DPOs, influenced by factors such as experience, qualifications, and organizational context. This is an improvement from previous reports, indicating an increase in appreciation of professionals in the field.



External DPO Assessment

The survey reveals striking 95.8% of respondents have been external DPOs for less than five years, indicating that this is a relatively new and growing field. The majority, 79.2%, are engaged in the private sector, 25% in academia, and 20.8% in the nonprofit sector. Smaller proportions are involved in government roles, with 4.2% each in national and county government positions, indicating that while there is some reliance on external DPOs in the public sector, it is less pronounced compared to the private sector. These findings emphasize the broadening scope of external DPOs across various sectors, driven by the need for specialized knowledge and compliance.



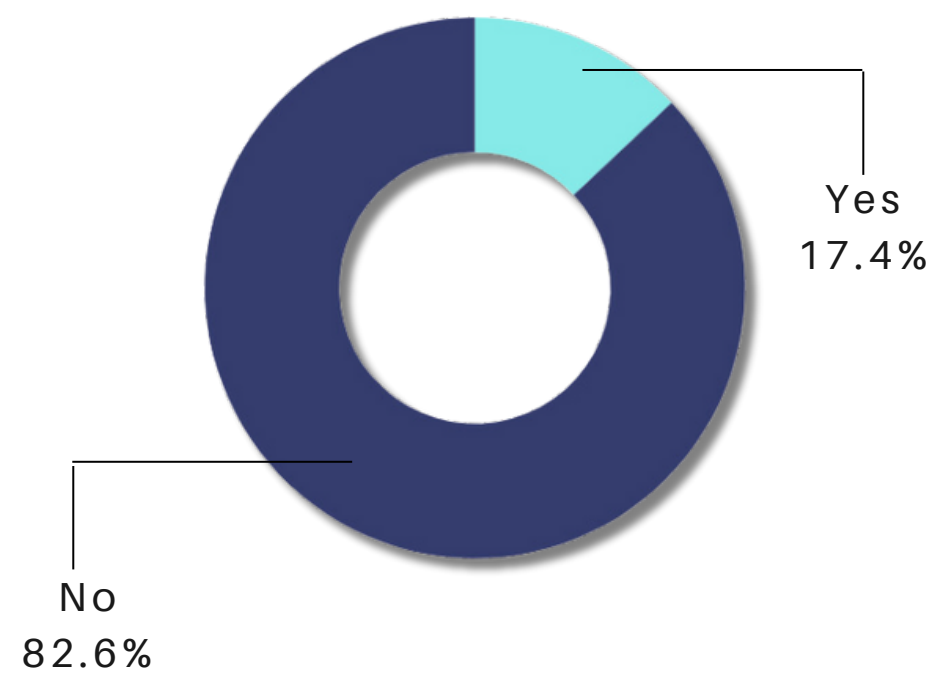


Core Professions

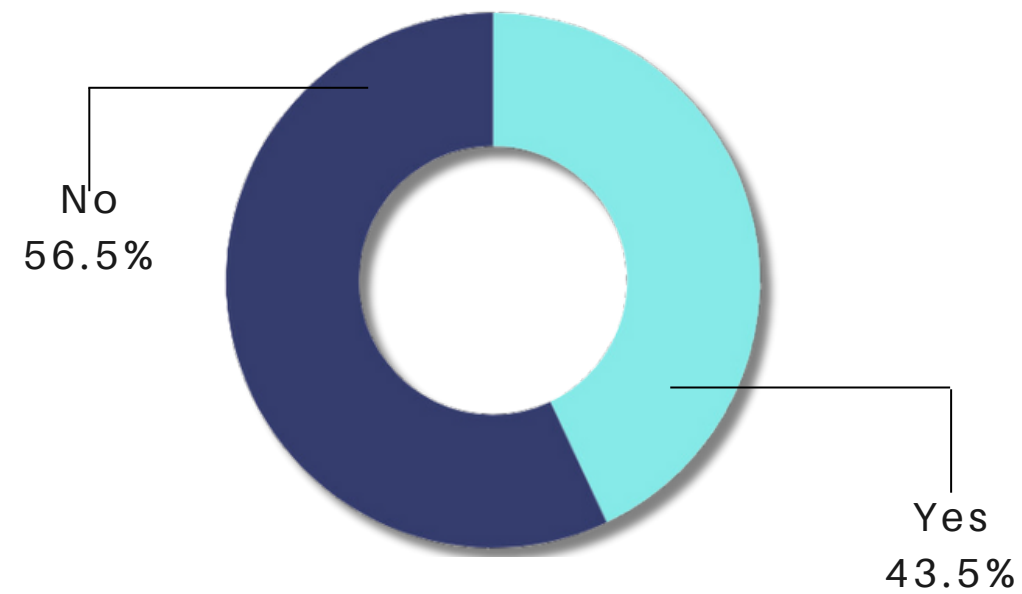
The survey on the core professions of Data Protection Officers (DPOs) highlights a substantial 69.6% of DPOs come from legal fields. This majority underscores the importance of understanding legal frameworks to ensure compliance and mitigate risks. Additionally, 13% of DPOs are from risk and compliance professions, emphasizing the significance of managing and mitigating data-related risks within organizations. Another 13% come from technical backgrounds, or "techies," indicating the need for technical expertise in implementing and managing data protection measures. Finally, 4.4% of DPOs are data scientists, bringing analytical perspectives to the role. This combination of legal, risk management, technical, and analytical skills safeguard sensitive information comprehensively.

External DPOs, Data Handlers and ODPC Compliance.

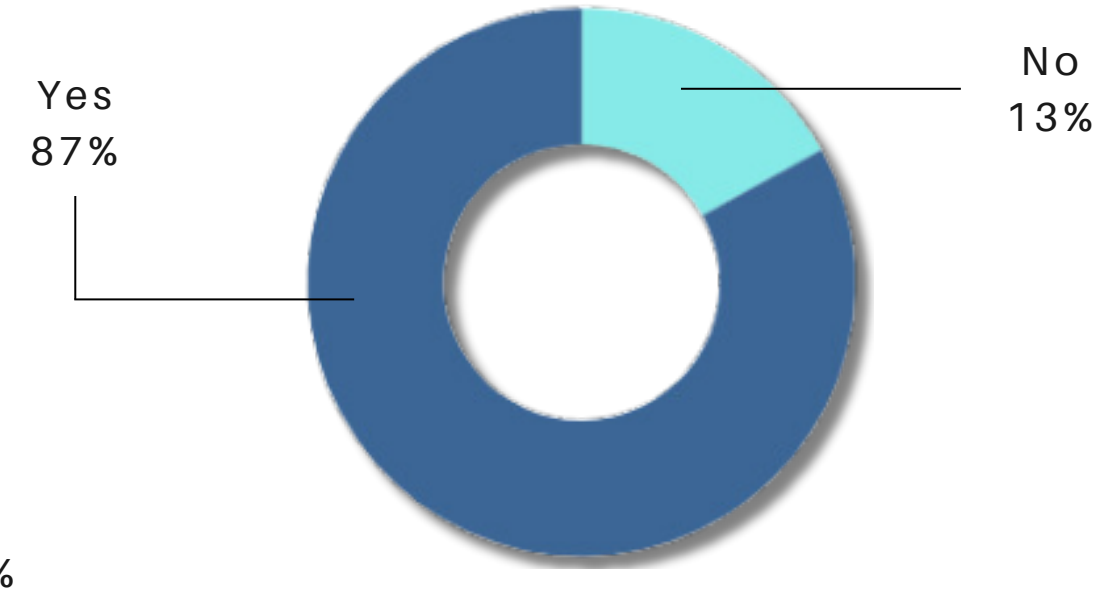
The survey on external Data Protection Officers (DPOs) assisting data handlers with compliance in the Office of the Data Protection Commissioner (ODPC) reveals only 17.4% of external DPOs have assisted with audits, suggesting a relatively low involvement in this area and potentially indicating that many data handlers manage audits internally. In contrast, 43.5% of respondents have assisted with the complaints process. Most notably, 87% of external DPOs have assisted with registration. These findings highlight that while external DPOs are primarily engaged in facilitating registration and addressing complaints, there is a significant opportunity for increased involvement in audit support to enhance overall compliance efforts.



Assisted Data Handler Being audited by ODPC



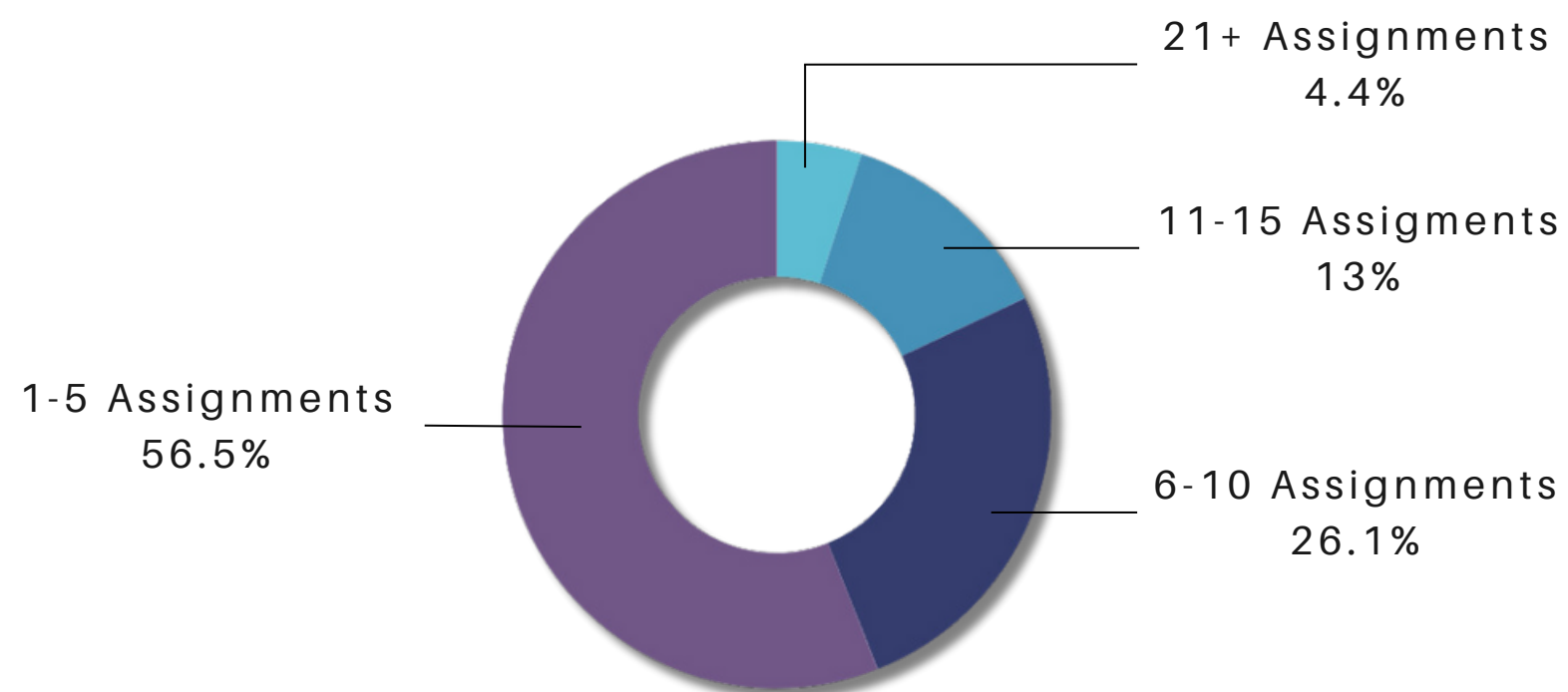
Assisted with the Complaints Process



Assisted with ODPC registration.

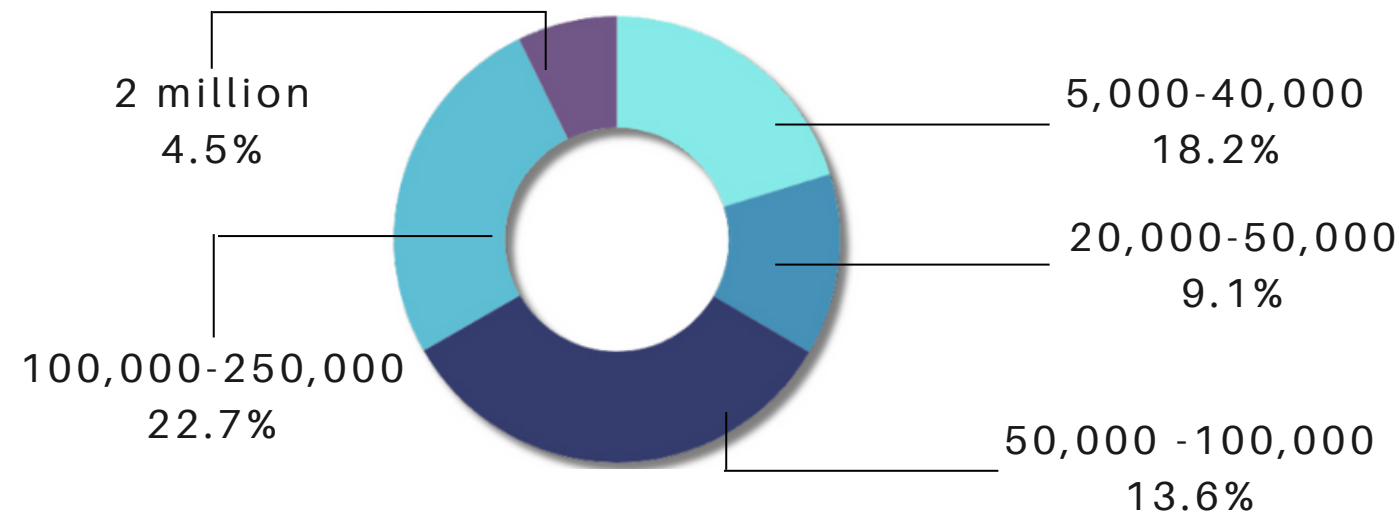
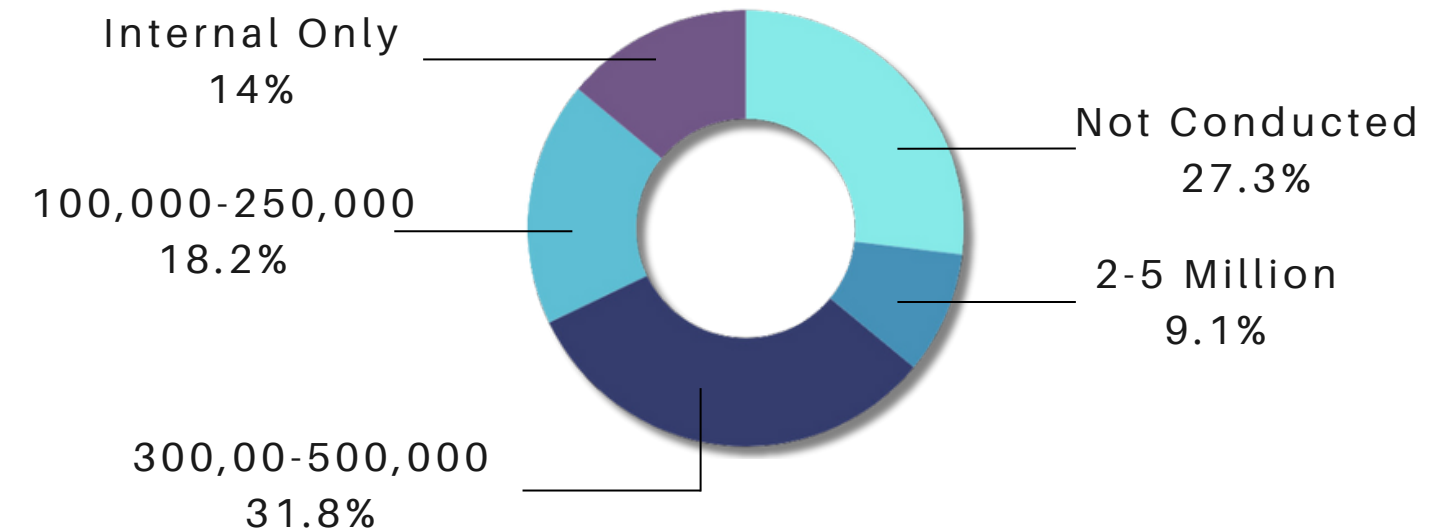
Number of Successful assignments.

The survey on DPO workloads as of June 2024 reveals a varied distribution of responsibilities. A majority, 56.5%, handle between 1-5 assignments, suggesting a manageable workload for many. Meanwhile, 26.1% manage 6-10 assignments, reflecting a moderate level of activity. Additionally, 13% deal with 11-15 assignments, indicating a higher demand on their time and resources. Notably, 4.4% of DPOs are managing over 21 assignments. These findings underscore the need for tailored support to help DPOs effectively balance their responsibilities and ensure robust data protection.



External DPO Fee Range

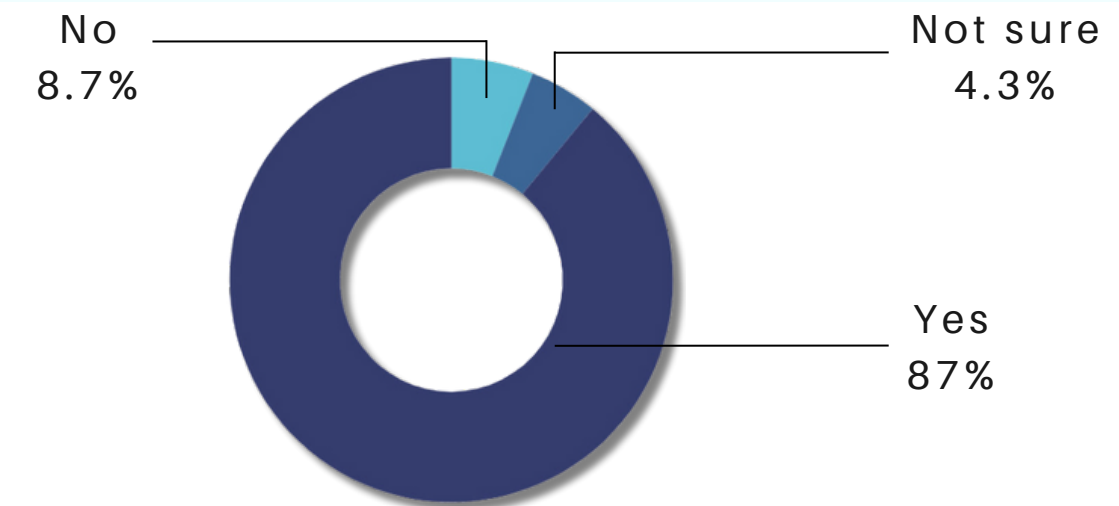
The survey results reveal significant variations in the fees charged by external Data Protection Officers (DPOs) for different services, highlighting the need for standardized professional fees. For conducting Data Protection Impact Assessments (DPIAs), fees range widely, with 9.1% charging between Ksh. 2 Million and 5 Million, 18.2% charging between 100,000 to 250,000, and 31.8% charging between 300,000 to 500,000. Notably, 27.3% of DPOs have not conducted a DPIA, and 14% have only done so internally.



In terms of data protection training, fees also vary: 4.5% charge 2 Million, 9.1% charge between 20,000 to 50,000, and 22.7% charge between 100,000 to 250,000. Daily rates range from 2,500 to between 50,000 and 100,000, with 13.6% charging hourly rates between 5,000 to 40,000. Additionally, 18.2% have not conducted training before.

For registration with the ODPC, 4.8% charge 3 Million, 33.3% charge 50,000, and 19.0% charge between 30,000 to 70,000, with 19.0% having not conducted a registration.

The survey also shows a strong consensus among respondents (87%) for establishing a schedule of minimum professional fees to bring consistency and fairness to the market, with only 8.7% disagreeing and 4.3% unsure. This broad agreement underscores the need for a regulated fee structure to ensure that DPO services are accessible and fairly compensated.





External DPO Role Challenges

Based on the survey, here is a list of 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.
- Resistance to registration in the ODPC by data handlers.
- Undercutting and pricing inconsistencies within the market.
- Lack of standardized guidelines on pricing of services and performance of duties.
- Limited availability and access to relevant information from different departments within organizations.
- Insufficient support from key stakeholders, including management and decision-makers.
- Competition from Audit firms and Law firms.

DPSGK Member interaction

The survey on interactions among DPGSK members reveals active engagement and positive experiences within the community. A notable 66.1% of members attended Continuing Professional Development (CPD) sessions, indicating a strong commitment to ongoing learning.

Additionally, 11.9% served as moderators at these sessions, showing leadership and knowledge-sharing roles. Volunteerism is also significant, with 18.6% participating in the pro bono lawyers scheme and 15.3% providing mentorship to university students. Attendance at key events is robust, with 40.7% at the DPGSK AGM, 47.5% participating in 2023 professional survey, 13.6% attending DPGSK/Amnesty International sessions, and another 13.6% at end-year meetups. Furthermore, 22% of members, reflecting engagement in policy development, demonstrate active involvement in shaping data privacy laws. Information sharing is prevalent, with 52.5% engaging in discussions.

When rating the value received from being part of the DPGSK community, most members gave positive ratings: 27.4% rated it a 4, and 30.6% rated it a 5, indicating a high level of satisfaction and perceived benefit from their membership. However, a small portion rated it lower, with 6.5% giving a 1 and 14.5% a 2, suggesting areas for improvement in meeting all members' expectations.



Key Takeaways

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

- 1. Professional Development and Training:** There is a strong emphasis on professional development, with the majority of members having received professional data protection training. Institutions like Strathmore University CIPIT and IAPP are prominent training providers. However, there is an opportunity to increase training uptake among the members who have not yet pursued it.
- 2. Diverse Professional Backgrounds:** The survey reveals a majority of DPOs come from legal fields, with significant representation from risk and compliance, technological backgrounds, and data science. This highlights a diversity which enhances the multidisciplinary approach required for effective data protection.
- 3. Roles and Workloads:** Most DPOs, both internal and external, have less than five years of experience in their roles, indicating a relatively new field. Workloads vary, with most handling 1-5 assignments, but a small percentage manage over 21 assignments, suggesting some DPOs face significant demands.
- 4. Organizational Support:** While many DPOs receive training and office facilities, fewer have board buy-in or compliance budgets. Support in the form of assistant DPOs and compliance technology is limited, indicating areas for improvement.
- 5. Member Engagement and Value:** The survey showed that DPGSK members are highly engaged, with the majority attending CPD sessions, the AGM, and participating in 2023 events, highlighting active involvement. The community is valued, with 58% rating their experience as 4 or 5 out of 5.

Consideration of the way forward

To improve the effectiveness of the Data protection profession, the following considerations and solutions are proposed to address the challenges

1. **Increase Professional Development and Training:** Efforts should be made to offer more targeted training sessions and workshops. Partnering with additional reputable institutions can expand the range of training options available together with developing online courses and webinars to make training more accessible and convenient.
2. **Standardization and Certification:** Developing standardized guidelines, procedures, and pricing structures for data protection services, including DPIAs, can promote consistency and professionalism. Certification should be encouraged by offering subsidies and highlighting its benefits. The 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.
3. **Enhance Organizational Support for DPOs:** Advocate for increased board buy-in and allocation of compliance budgets within organizations. Highlight the importance of data protection to senior management to secure better support. Create guidelines and best practices for organizations to follow, ensuring they provide necessary resources like office facilities, compliance technology, and assistant DPOs.
4. **Boost Member Engagement and Value:** Organize more interactive and value-driven events, such as networking sessions, knowledge-sharing forums, and mentorship programs. Ensure a diverse range of topics to cater to different interests and professional needs. Solicit regular feedback from members to continually improve the offerings and increase the perceived value of DPGSK membership.



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](https://twitter.com/DataGovProsKe).

Edited By

Naisenya Katampoi
Member DPGSK

Philip Kisaka
Assistant Secretary DPGSK