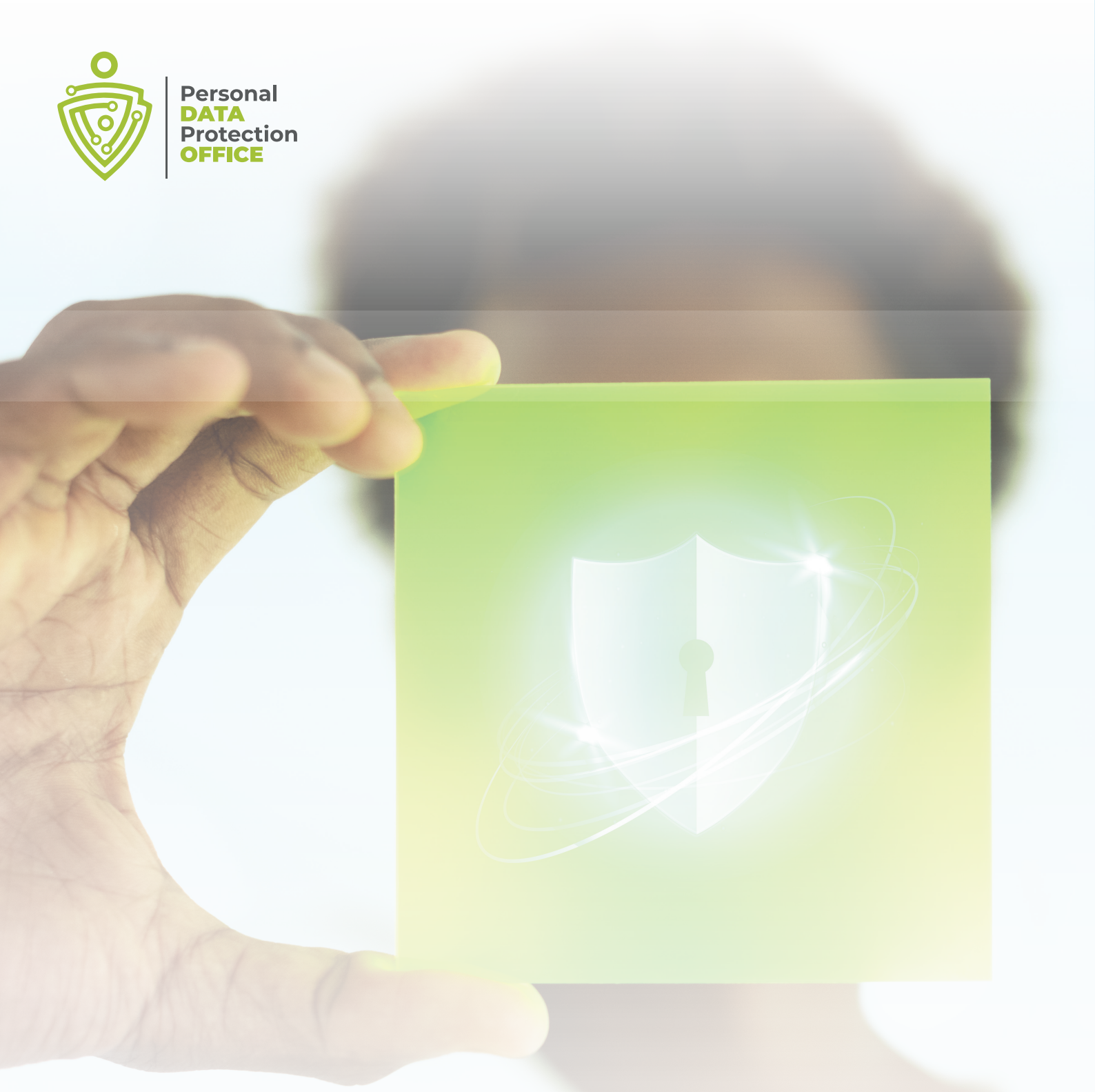
Personal
DATA
Protection
OFFICE



DATA PROTECTION OFFICER TRAINING NEEDS ASSESSMENT REPORT

NOVEMBER 2022

The role of a Data Protection Officer

Personal DATA Protection OFFICE

- Contribute to Information Security decisions
- Oversight of all data-sharing agreements
- Contribute to incident management processes
- Provide regular updates to senior management about data protection and privacy compliance.
- Conduct regular assessments and trainings.

TABLE OF CONTENTS

TABLE OF CONTENTS 1
LIST OF ACRONYMS 3
EXECUTIVE SUMMARY 5
1 INTRODUCTION 7
1.1 Background 7
1.2 Objectives of the survey 7
1.2.1 Specific objectives 7
2 SURVEY METHODOLOGY 8
2.1 Target audience and sample size 8
2.2 Data collection and processing 8
3 SURVEY FINDINGS 9
3.1 Social Demographic Characteristics 9
3.1.1 Organization type 9
3.1.2 Job Title/Positions of DPOs 10
3.1.3 Gender of DPOs 10
3.2 Education Background and Training 11
3.2.1 Education Background 11
3.2.2 Professional training and certifications 11
3.2.3 Data Protection Certifications 12
3.2.4 Attendance of a Data Protection and Privacy related training 12
3.2.5 Data Protection and Privacy knowledge domains trainings 13
3.2.6 Cyber Security trainings 13
3.3 Involvement in Governance of Data Protection and Privacy activities 14
3.3.1 Involvement in the development of data protection and privacy related policies and procedures 14
3.3.2 Involvement in the preparation and monitoring of data sharing agreements 15
3.3.3 Consultations in relation to handling of personal data 16
3.4 Awareness and Training 16
3.4.1 Involvement in the development and implementation of an organization awareness and training program 16
3.4.2 Areas identified for inclusion in an awareness and training programme 17
3.4.3 Training and awareness sessions facilitated 17
3.5 Records management and retention 18
3.5.1 Involvement in the process of development and implementation of asset and records management and retention procedures or guidelines 18
3.5.2 Involvement in working with records of details of persons. 18
3.5.3 Involvement in conducting regular data quality reviews of records. 19
3.5.4 Involvement in the process of erasure or destruction of office records 19
3.5.5 Considerations made before erasure or destruction of office records 20
3.6 Audit and Assessment 20
3.6.1 Involvement in conducting Data Protection Impact Assessments (DPIA) 20
3.6.2 Organization audit or assessments 20
3.6.3 Frequency of organizational audit or assessment 21
3.7 Breach and Complaints Management 21

3.7.1 Involvement in detection, identification and reporting of personal data security breaches 21
3.7.2 Resolution of a data protection and privacy complaint 22
3.7.3 Knowledge of data protection and privacy complaint resolution 22
3.7.4 Personal Data security breach encounters 22
3.7.5 Procedure of handling personal data security breaches 23
3.7.6 Consultative work 23
3.7.7 Training interests 23
4 CONCLUSIONS 24
5 RECOMMENDATIONS 25

LIST OF ACRONYMS

ACRONYM	DEFINITION
ACCA	Association of Chartered Certified Accountants.
API	Application Programming Interface
BBA	Bachelor of Business Administration
CCNA	Cisco Certified Network Associate
CCNP	Cisco Certified Network Professional
CDPSE	Certified Data Privacy Solutions Engineer
CEH	Certified Ethical Hacker
CHFI	Certified Hacking Forensic Investigator
CIPA	Certified Information Privacy Auditor
CIPM	Certified Information Privacy Manager
CIPP	Certified Information Privacy Professional
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
CISSP	Certified Information Systems Security Professional
B.COM	Bachelor of Commerce
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
B. ECON	Bachelor of Economics
GDPR	General Data Protection Regulation
IT	Information Technology
ISACA	Information Systems Audit and Control Association
ISC2	International Information Systems Security Certification Consortium
IT	Information Technology
ITIL	Information Technology Infrastructure Library

NGO	Non-Government Organisation
PDPO	Personal Data Protection Office

EXECUTIVE SUMMARY

The Personal Data Protection Office (PDPO) is an independent statutory Office under the National Information Technology Authority (NITA-U) that regulates the collection and processing of personal data in Uganda through a mandate proffered by the Data Protection and Privacy Act, 2019. To effectively execute its mandate as provided under the law, PDPO requires up-to-date data and information to inform and monitor technical capacity of Data Protection Officers to execute responsibilities enshrined under the law.

In line with this mandate, PDPO conducted a Training Needs Assessment among the 510 DPOs designated by the registered entities as at 13th October 2022. This aimed at establishing the gaps in skills required of DPOs to perform tasks related to ensuring compliance under the Act. This assessment specifically sought to identify the level of involvement of DPOs in governance of Data Protection and Privacy activities; establish whether DPOs develop and implement Data Protection and Privacy awareness programs; and establish DPOs' knowledge and understanding of audit/assessment, breach and complaints management procedures among others.

Key findings of the Survey

In terms of social demographic characteristics of the respondents, the majority of DPOs (73.6%) who responded to the survey were from the private sector, and 23.6% were designated as only DPOs with no additional job roles. Additionally, 32.5% had an education background in IT/Computer Science (or a related field). It was also established that there was a gender bias in favor of males who made up 59% of the DPOs.

Almost all the DPOs (90.6%) did not have any certification in data protection and privacy. Furthermore, it was established that 68.2% had attended a data protection and privacy related training in the previous two (2) years with the majority having been trained by PDPO.

As far the involvement of DPOs in governance of Data Protection and Privacy activities is concerned, the assessment shows that the DPOs who had been involved in the development of various data protection and privacy related policies and procedures accounted for more than half of the total (64.2%). The assessment further found out that the DPOs that had consulted with internal subject matter experts in relation to handling of personal data make up 60.4% with the areas least consulted in being learning and development, procurement and public relations.

It was observed that only a few of the 48.1% of the DPOs that had been involved in the development and implementation of an organizational awareness and training programme were able to correctly identify components of an awareness and training programme, such as objectives of conducting

the training, delivery methods, frequency of trainings, topics to be trained on and the target audience.

The assessment findings indicate that the majority (66%) of DPOs had been involved in the conducting regular data quality reviews of records containing personal data to make sure they were adequate, accurate and not excessive. However, it was established that 77.4% of DPOs had not been involved in the process of erasure or destruction of such records.

From the assessment findings, only 29.2% of the DPOs had carried out a Data Protection and Privacy audit. It was also established that a small percentage (29.2%) had been involved in conducting of a Data Protection Impact Assessment.

Regarding involvement in the detection, identification and reporting of personal data breaches, most of the DPOs (64.2%) had not partaken in such a process. It was also noted that almost all the DPOs (90.6%) had never resolved a data protection and privacy complaint.

The assessment found out that the majority (62.7%) of the DPOs had worked with other qualified personnel who are not necessarily staff of the organization such as consultants and contractors.

The majority of DPOs pointed out that they were interested in being trained in Data Protection Impact Assessments, data breach incident management, Privacy Management Program and Cyber Security tools overview.

Overall, the assessment established that most of the DPOs had limited skills required to perform tasks related to ensuring compliance under the Act.

1 INTRODUCTION

1.1 Background

The Personal Data Protection Office (PDPO) is an independent statutory Office under the National Information Technology Authority (NITA-U) that regulates the collection and processing of personal data in Uganda through a mandate proffered by the Data Protection and Privacy Act, 2019. To effectively execute its mandate as provided under the law, PDPO requires up-to-date data and information to inform and monitor technical capacity of Data Protection Officers to execute responsibilities enshrined under the law.

The Act requires certain data controllers and processors to designate a Data Protection Officer to among other duties ensure compliance with the law. As at 13th October 2022, 510 DPOs had been designated by both public and private entities registered with the Personal Data Protection Office. However, there is no in-depth programme in place to enhance and equip them with skills to perform tasks related to ensuring such compliance with the Act.

In line with this mandate, PDPO conducted a Training Needs Assessment of DPOs at the aforementioned entities to establish the skills gaps which would inform the development and implementation of a training programme to address the identified training needs/ gaps.

1.2 Objectives of the survey

The main objective of the survey was to establish areas where Data Protection Officers require training to efficiently perform tasks related to ensuring compliance with the Data Protection and Privacy Act.

1.2.1 Specific objectives

The specific objectives were to;

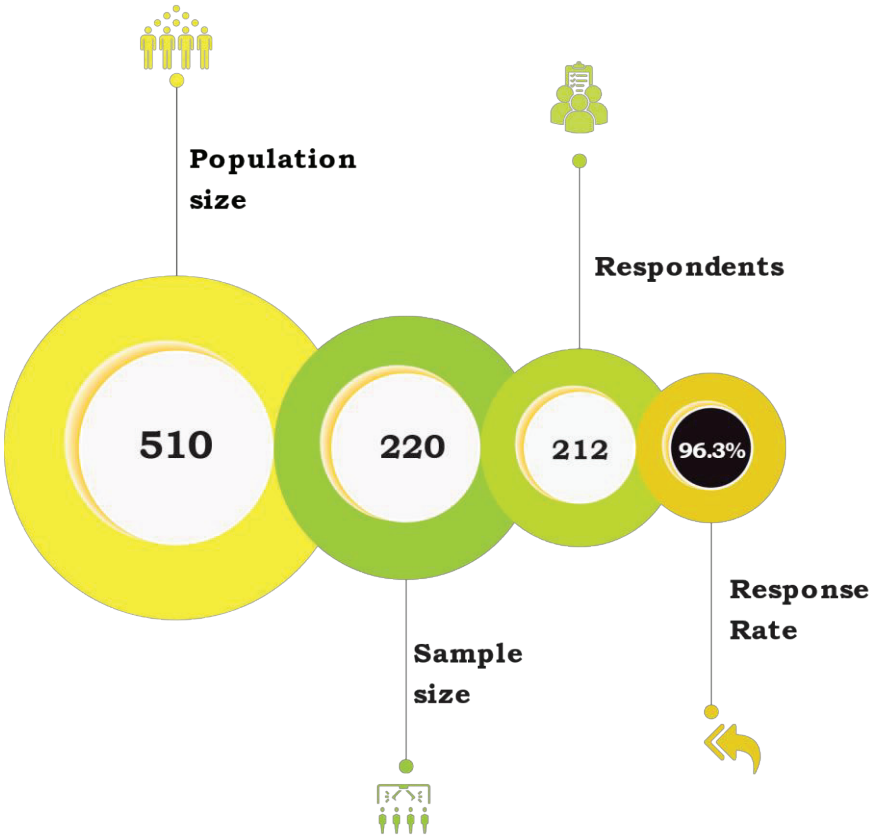
- Determine the education background of DPOs.
- Identify level of involvement of DPOs in governance of Data Protection and Privacy activities.
- Establish whether DPOs develop and implement Data Protection and Privacy awareness programs.
- Establish DPOs knowledge and understanding of records management, audit/assessment, and breach and complaints management procedures.

2 SURVEY METHODOLOGY

2.1 Target audience and sample size

The training needs assessment targeted DPOs at entities registered with the PDPO. A sample of 220 out of 510 DPOs registered with PDPO as at 13th October 2022 was assessed. This sample was derived assuming a margin error of + or – 5% at a confidence level of 95%. Of the sampled DPOs, a response rate of 96.3% was achieved.

Figure 1: Sample size and Response Rate



2.2 Data collection and processing

An online assessment form was emailed to the DPOs to complete. Follow up emails were sent and phone calls also made to ensure the desired response rate was achieved. The collected data was exported to relevant statistical packages for analysis.

3 SURVEY FINDINGS

This section presents the findings from the 2022 DPO Training Needs Assessment Survey including the education background of DPOs, their level of involvement of governance of Data Protection and Privacy activities, development and implementation Data Protection and Privacy awareness programs and their knowledge and understanding of records management and retention, audit/assessment, and breach and complaints management procedures.

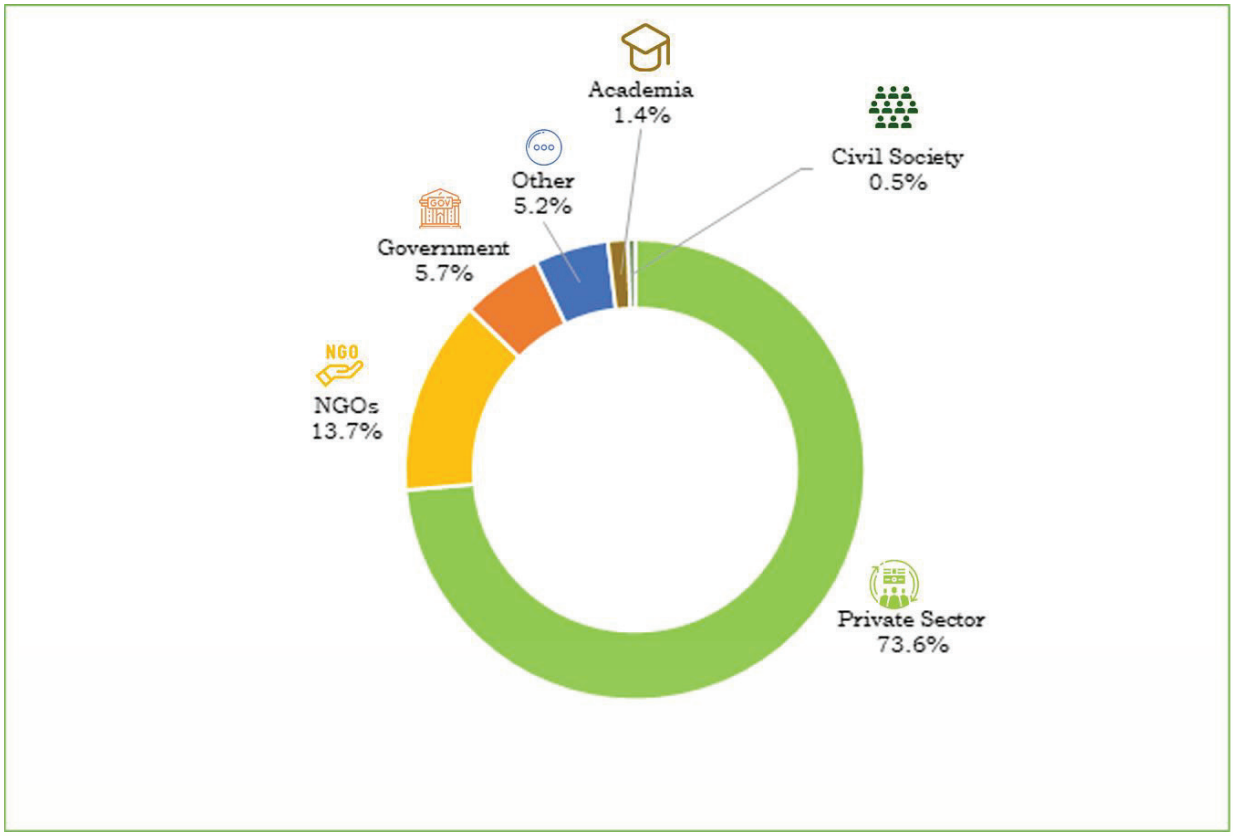
3.1 Social Demographic Characteristics

This portion of the report summarizes findings on the social demographic characteristics of DPOs including the organization type, gender and job titles/positions of the DPOs.

3.1.1 Organization type

A variety of organizations as shown in Figure 2 employed DPOs. However, the majority (73.6%) were from the private sector, Non-Government Organisations (NGOs) 13.7% and remaining organizations accounted for 12.4%.

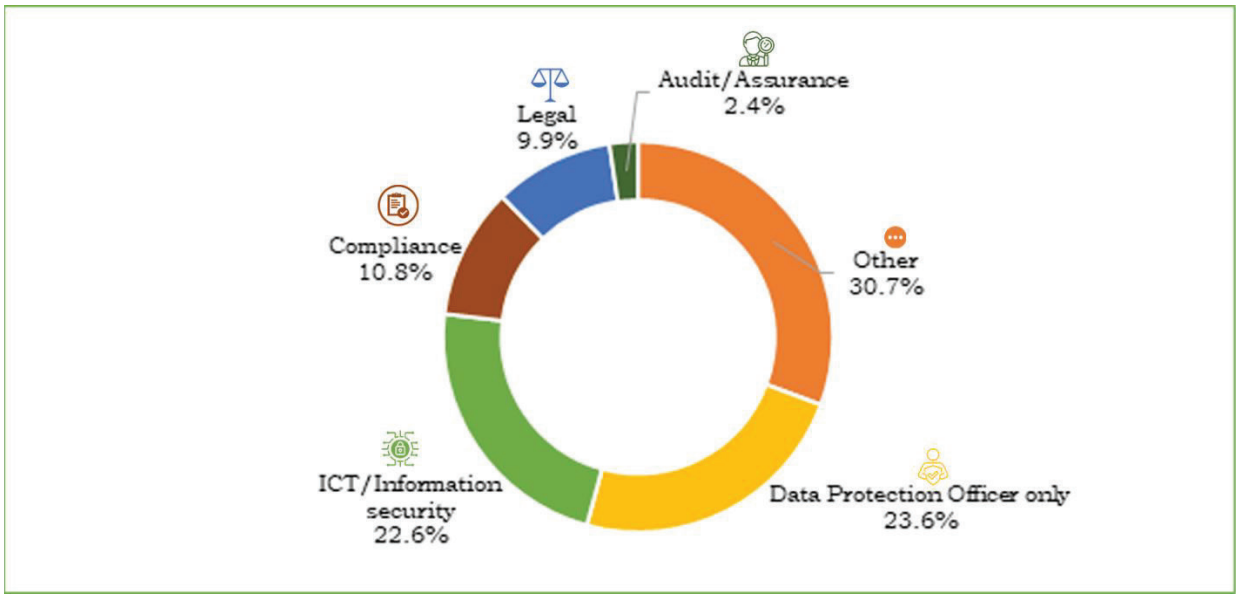
Figure 2: Proportion of DPOs by organization type



3.1.2 Job Title/Positions of DPOs

In regard to designation, 23.6% of the DPOs were designated Data Protection Officers with no additional job roles as shown in Figure 3.

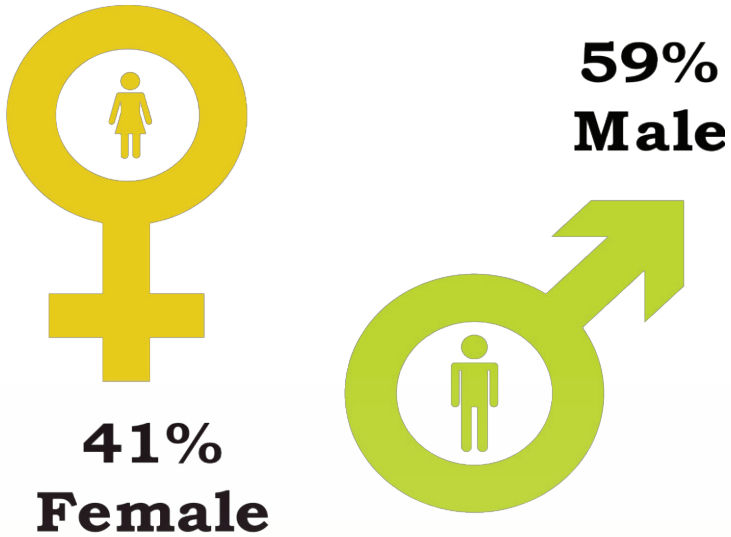
Figure 3: Proportion of DPOs by job titles/positions



3.1.3 Gender of DPOs

Of the DPOs that participated in the survey, it was established that the majority were male accounting for 59% and the females 41% indicating a gender bias in favor of males among DPOs as shown in figure 4.

Figure 4: Proportion of DPOs by gender

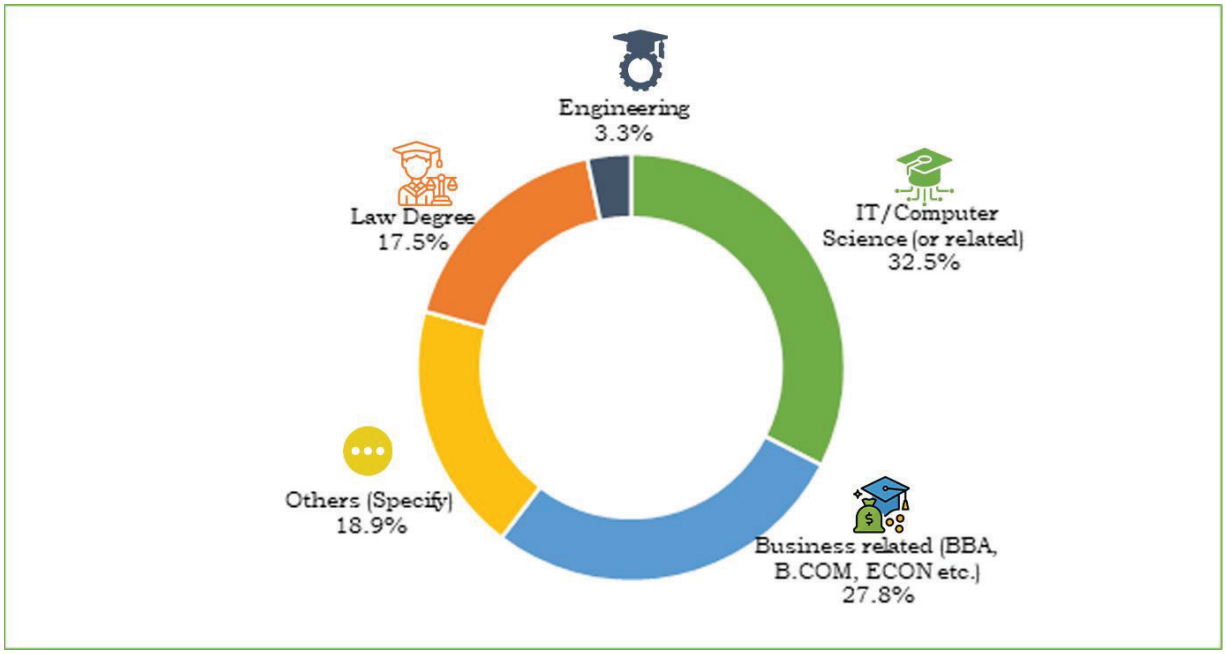


3.2 Education Background and Training

3.2.1 Education Background

DPOs that obtained education in IT/Computer Science (or a related field) course make up nearly a third (32.5%) of all. The least proportion (3.3%) accounts for those that obtained an education in engineering. Only 18.9% of the DPOs had obtained an education in other fields such as Social Sciences, Statistics, and Humanities (Figure 5).

Figure 5: Proportion of DPOs by education background.



3.2.2 Professional training and certifications

Almost half of the DPOs (46.7%) did not have any professional training and certification in audit and ICT Security. Nevertheless, those that had, were trained and certified in fields such as CCNA, ITIL, CCNP were found to be 31.6% of the total. Figure 6 shows the proportion of DPOs by professional training and certification.

Figure 6: Proportion of DPOs by professional and certifications (Multiple select)

3.2.3 Data Protection Certifications

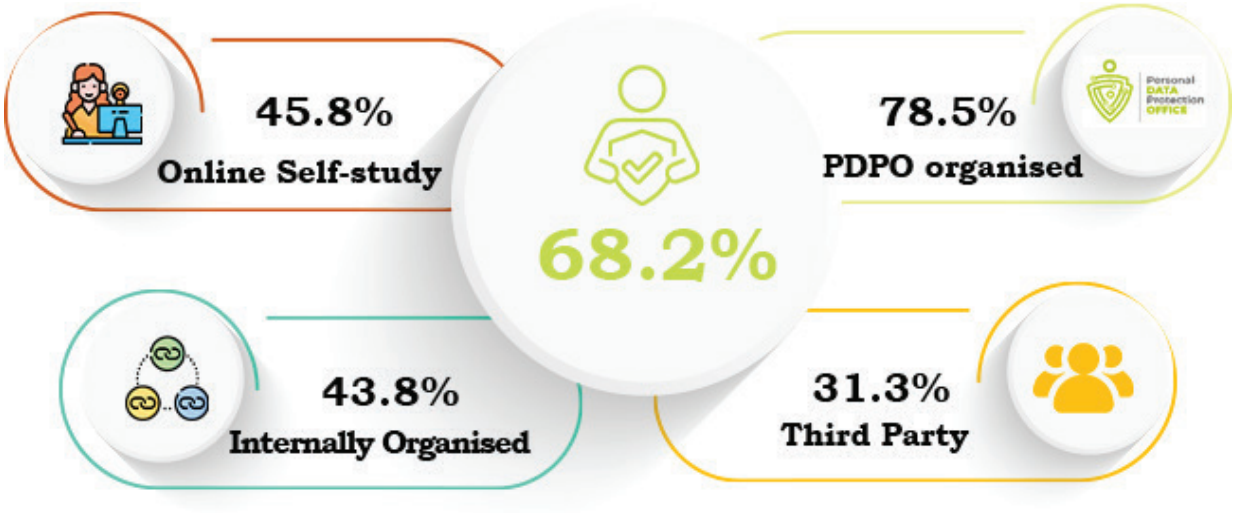
A staggering proportion of 90.6% had not acquired any certification in data protection and privacy. Only a minuscule had acquired CIPP, CIPM and other certifications such as, PECB among others as shown in Figure 7. None of the assessed DPOs had acquired either CDSPE or CIPA. Among the 6.6% of the DPOs who mentioned that they had acquired other certifications, erroneously stated that they were certified in the General Data Protection Regulation without specifying the certification domain or body.

Figure 7: Proportion of DPOs by Data Protection Certifications acquired (Multiple select)

3.2.4 Attendance of a Data Protection and Privacy related training

The majority (68.2%) of DPOs had attended a data protection and privacy related training in the previous two (2) years and most of them (78.5%) had been trained by PDPO as seen in Figure 8.

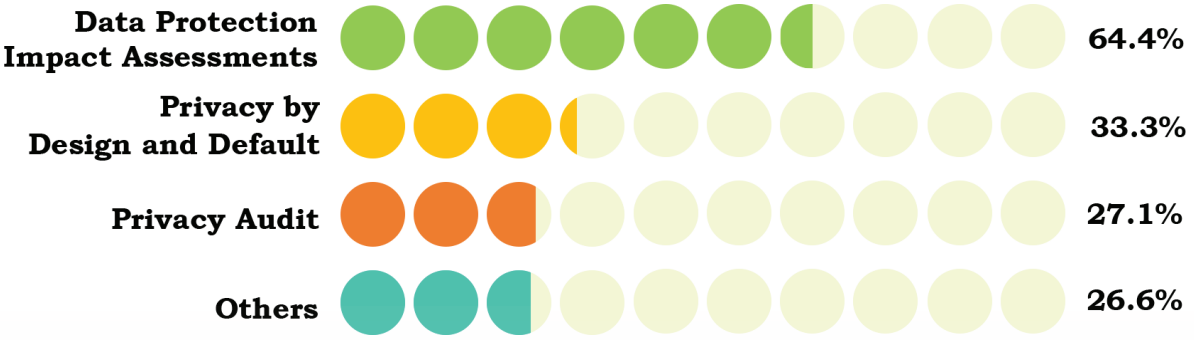
Figure 8: Proportion of DPOs by the Data Protection and Privacy related trainings attended in the previous 2 years (Multiple select)



3.2.5 Data Protection and Privacy knowledge domains trainings

More than a half of the DPOs (64.4%) had been trained in the Data Protection Impact Assessments domain. Besides Privacy by Design and Default and Privacy Audit, 26.6% of the DPOs had been trained in other domains such as Data Protection and Privacy Awareness, among others as shown in the Figure 9.

Figure 9: Proportion of DPOs by Data Protection and Privacy Knowledge Domains training (Multiple select)



3.2.6 Cyber Security trainings

The survey findings indicate that 59% of the DPOs had attended a cyber security training in the previous two (2) years. Figure 10 shows the various cyber security trainings attended by the DPOs.

Figure 10: Proportion of DPOs by Cyber Security trainings undertaken in the previous 2 years (Multiple select)

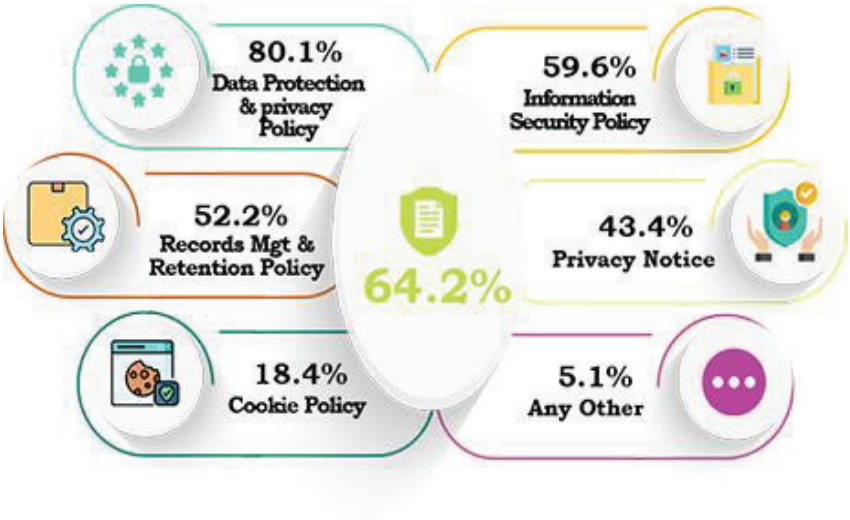
3.3 Involvement in Governance of Data Protection and Privacy activities

The assessment sought to establish the involvement of DPOs in the development of data protection and privacy related policies and procedures, preparation and monitoring of data sharing agreements and consultations with internal subject matter experts in handling of personal data. The next three sub sections give an in-depth report of what was established.

3.3.1 Involvement in the development of data protection and privacy related policies and procedures

The assessment established that the DPOs who had been involved in the development of data protection and privacy related policies and procedures accounted for more than half of the total (64.2%). A higher proportion (80.1%) of these individuals had been involved in the development of a Data Protection and Privacy Policy. Figure 11 shows the various policies and procedures the DPOs had been involved in.

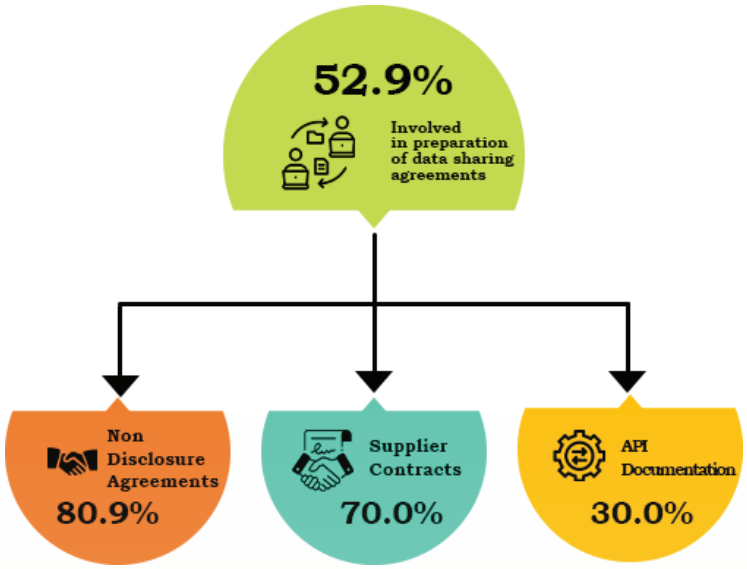
Figure 11: Proportion of DPOs by involvement in Data protection and privacy related policies and procedures' development (Multiple select)



3.3.2 Involvement in the preparation and monitoring of data sharing agreements

More than half (52.9%) of the DPOs had been involved in the preparation and monitoring of data sharing agreements. Those that had been involved in the preparation of Non-Disclosure Agreements accounted for 80.9%, preparation and monitoring of Supplier Contracts 70% and API Documentation 30% as represented in Figure 12.

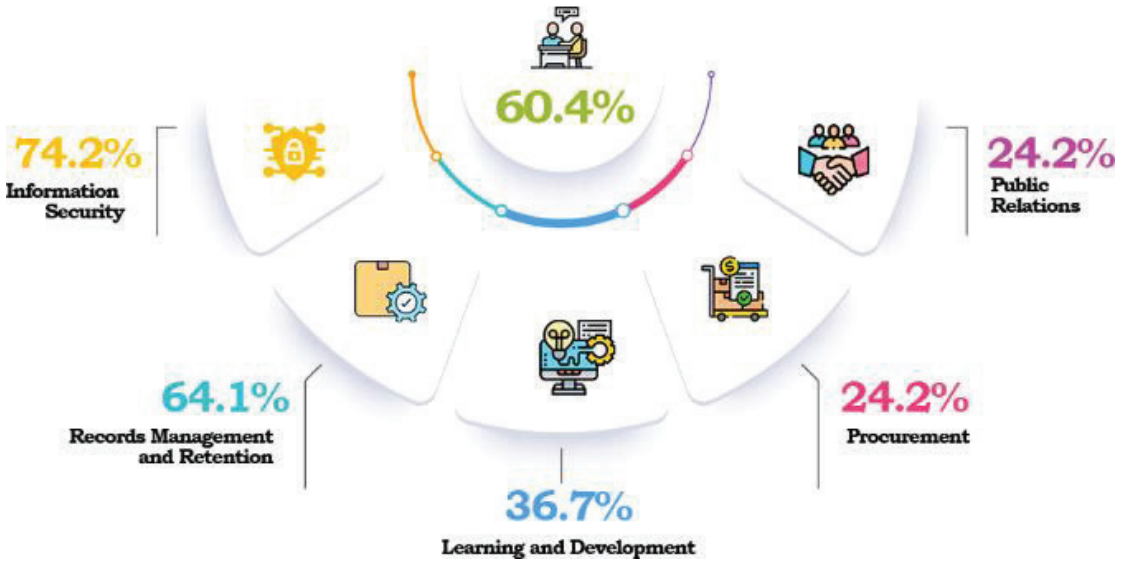
Figure 12: Proportion of DPOs by data sharing agreements prepared and monitored (Multiple select)



3.3.3 Consultations in relation to handling of personal data

It was also established that of the 60.4% DPOs that had consulted with internal subject matter experts in relation to handling of personal data. Among those that had consulted, 74.2% did so in information security. Figure 13 is a representation of the various areas consulted in.

Figure 13: Proportion of DPOs by Consultations in relation to handling of personal data (Multiple select)



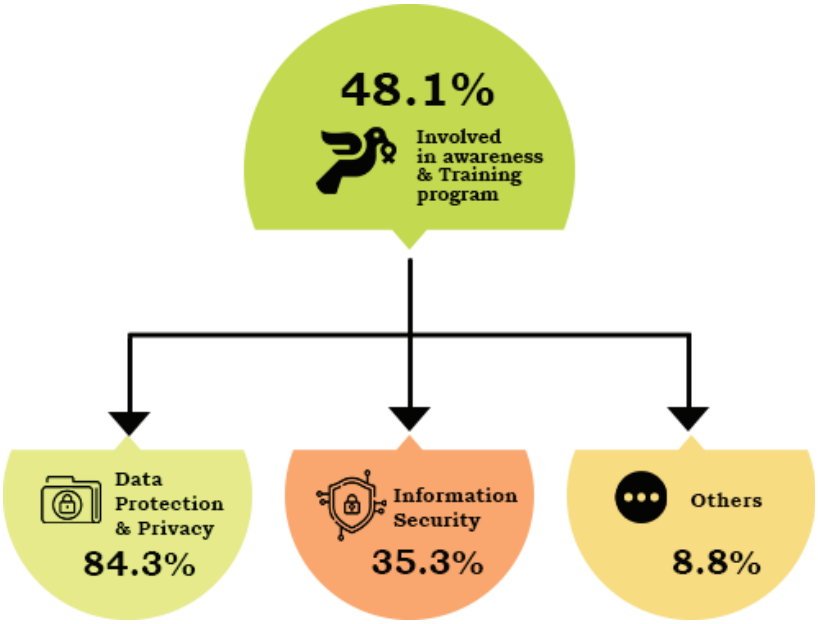
3.4 Awareness and Training

This sub section of the report documents the findings on the DPOs' involvement in development and implementation of an organization awareness and training program and whether or not they had facilitated any awareness and training sessions for members of staff in the past two years.

3.4.1 Involvement in the development and implementation of an organization awareness and training program

It was found that less than half of the DPOs (48.1%) had been involved in the development and implementation of an organization awareness and training program. Figure 14 shows that the majority (84.3%) of the 48.1% had been involved in Data Protection and Privacy awareness training. At the lower end, 8.8% is the proportion of those that were involved in other organization awareness and training programs such as Anti-Money Laundering measures, Regulatory Compliance etc.

Figure 14: Proportion of DPOs by involvement in organization awareness and training programs (Multiple select)



3.4.2 Areas identified for inclusion in an awareness and training programme

It was observed that only a few of the 48.1% of DPOs that had been involved in the development and implementation of an organization awareness and training programme were able to correctly identify components of an awareness and training programme, such as objectives of conducting the training, delivery methods, frequency of trainings, topics to be trained on and the target audience.

However, the rest of the respondents could only list topics to be trained mainly on information security and implementation of principles of data protection and privacy.

3.4.3 Training and awareness sessions facilitated

The survey established that 42% of the DPOs had not facilitated any training and awareness sessions for members of staff in the previous 2 years. However, some DPOs had facilitated data protection and privacy and information security training and awareness sessions as shown in Figure 15. The least proportion (6.6%) had facilitated other areas namely Anti-Money Laundering, Regulatory Compliance among others.

Figure 15: Proportion of DPOs' facilitations in training and awareness sessions. (Multiple select)

3.5 Records management and retention

This subsection of the report covers assessment findings in the involvement of DPOs in the process of development and implementation of assets and records management and retention procedures or guidelines, working with records of details of persons, conducting data quality reviews of records and erasure or destruction of office records.

3.5.1 Involvement in the process of development and implementation of asset and records management and retention procedures or guidelines

More than a half (56.6%) of the DPOs had been involved in the development and implementation of asset and records management and retention procedures or guidelines as shown in Figure 16.

Figure 16: DPOs' involvement in the process of development and implementation of asset and records management and retention procedures or guidelines

3.5.2 Involvement in working with records of details of persons.

Figure 17 shows that 77.8% of the DPOs had been involved in working with records of details of persons such as data entry, analysis, or reporting.

Figure 17: Proportion of DPOs by involvement in working with records of details of persons

3.5.3 Involvement in conducting regular data quality reviews of records.

The survey findings indicate that the majority (66%) of DPOs had been involved in the conducting regular data quality reviews of records containing personal data to make sure they were adequate, accurate and not excessive (Figure 18)

Figure 18: Proportion of DPOs by involvement in conducting regular data quality reviews of records

3.5.4 Involvement in the process of erasure or destruction of office records

It was found out that 77.4% of DPOs had not been involved in the process of erasure or destruction of office records while only 22.6% had been involved as shown in the Figure 19.

Figure 19: Proportion of DPOs by involvement in the process of erasure or destruction of office records

3.5.5 Considerations made before erasure or destruction of office records

Of the 22.6% of the DPOs that had been involved in the process of erasure or destruction of office records, most of them considered the following;

a) Relevant statutory/regulatory retention periods,
b) Appropriate methods to carry out the erasure or destruction,
c) Any internal standard operating procedures to guide erasure or destruction, and
d) Whether the data subject is required to consent to the erasure or destruction.

3.6 Audit and Assessment

The assessment also sought to establish the involvement of the DPOs in conducting DPIAs, organization audits and their opinion on how often organisations should carry out audits/assessments.

3.6.1 Involvement in conducting Data Protection Impact Assessments (DPIA)

The survey found out that 29.2% of the DPOs had been involved in conducting DPIA as represented in Figure 20.

Figure 20: Proportion of DPOs by Involvement in conducting DPIA

3.6.2 Organization audit or assessments

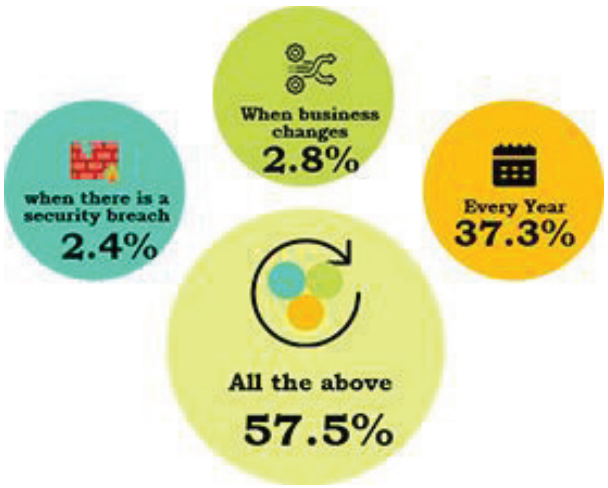
The assessment findings show that more than a half (54.2%) of the DPOs had not carried out Information Security Audits or IT Assessment and/or Data Protection or IT Assessments. Figure 21 shows that an equal proportion of 29.2% accounts for each of the DPOs that carried out the aforementioned audits or assessments.

Figure 21: Proportion of DPOs by organization audits or assessments carried out (Multiple select)

3.6.3 Frequency of organizational audit or assessment

More than half (57.5%) of the DPOs shared the opinion that organizational audits should be carried out as often as every year, when there is a security breach and when business changes. The findings also show that 2.4% believed audits or assessments were necessary only when there is a security breach as shown in Figure 22.

Figure 22: Opinions on the frequency of organization audits or assessments



3.7 Breach and Complaints Management

This portion of the report shows assessment findings in the involvement of DPOs in detection, identification and reporting of personal data security breaches, resolution of a data protection complaint and opinions on the procedure to be undertaken, data security breach encounters and consultative work. The section also covers the training interests of the DPOs.

3.7.1 Involvement in detection, identification and reporting of personal data security breaches

Regarding involvement in the detection, identification and reporting of personal data breaches, most of the DPOs (64.2%) had not partaken in such a process as shown in Figure 23.

Figure 23: Proportion of DPOs by involvement in detection, identification and reporting of personal data security breaches.

3.7.2 Resolution of a data protection and privacy complaint

Figure 24 shows that almost all the DPOs (90.6%) reported that they had never resolved a data protection and privacy complaint.

Figure 24: Proportion of DPOs by involvement in the resolution of a data protection and privacy complaint

3.7.3 Knowledge of data protection and privacy complaint resolution

Of the 9.4% of the DPOs that had been involved in the resolution of data protection and privacy complaints, majority of them were able to list the steps that are involved from start to closure. The respondents listed the following among the steps taken;

a) Acknowledgment of receipt and recording of the complaint
b) Assess the complaint and affected personal data
c) Communication with the affected data subject(s) and other stakeholders
d) Review and evaluate the complaint
e) Resolution and closure of complaints within the statutory timelines

3.7.4 Personal Data security breach encounters

The survey findings in Figure 25 show that 87.7% of the DPOs had not encountered a personal data security breach in their work as DPOs.

Figure 25: Proportion of DPOs by data security breach encounters

3.7.5 Procedure of handling personal data security breaches

Responses received from the 12.3% of the DPOs that had encountered breaches in their organisations showed that they had clear knowledge and understanding of what needs to be done to handle personal data security breaches. The respondents provided the following key common actions taken during the handling of personal data security breaches;

a) Establish details about the breach
b) Communication of personal data security breach to relevant stakeholders, such as PDPO
c) Convene the responsible team for investigation
d) Isolate affected computers/devices on the network to contain the breach and assess the risk to the privacy of the individuals and their personal data
e) Invoke the disaster recovery plan (preserve and contain the evidence)

3.7.6 Consultative work

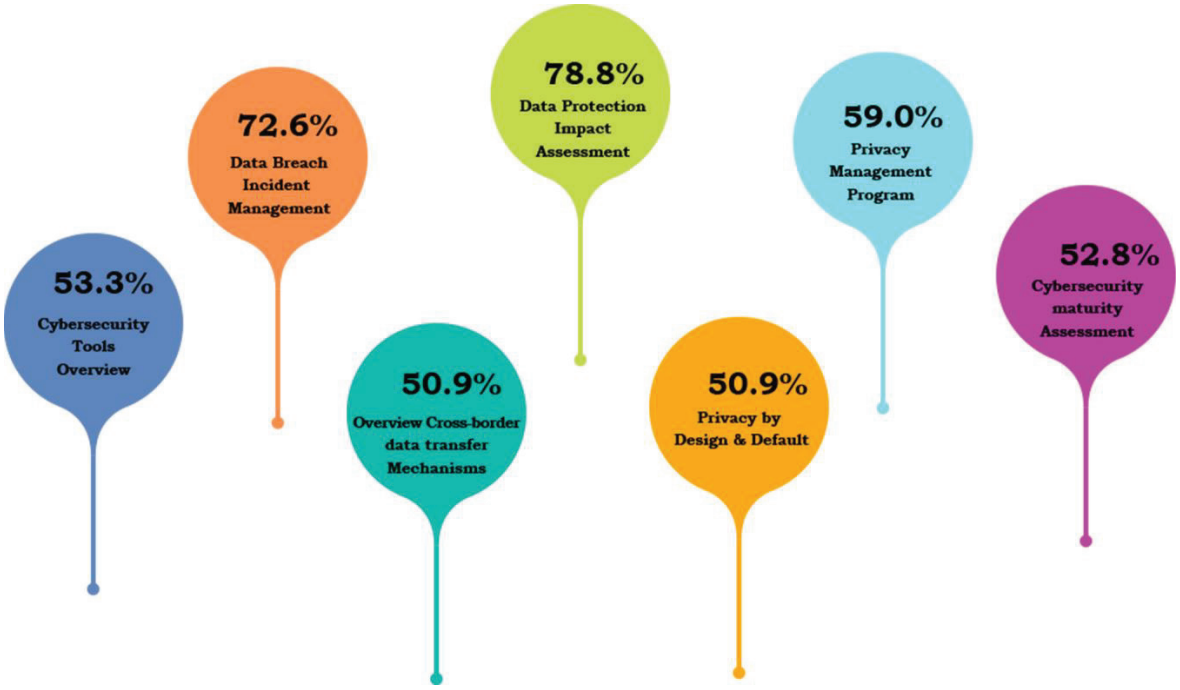
It was found out that the majority (62.7%) of the DPOs had worked with other qualified personnel who are not necessarily staff of the organization such as consultants and contractors as shown in Figure 26.

Figure 26: Proportion of Respondents by Consultative work

3.7.7 Training interests

A good number (78.8%) of DPOs were interested in being trained in Data Protection Impact Assessments. The least proportion (50.9%) accounts for those interested in Privacy by Design and Default (Figure 27).

Figure 27: Proportion of respondents by training interests (Multiple select)



4 CONCLUSIONS

Almost all the DPOs did not have any certification in data protection and privacy. However, a good number had attended a data protection and privacy related training in the previous two (2) years largely those organized by PDPO.

Most of the DPOs had limited knowledge required to develop and implement a privacy management programme, such as policies on data protection and privacy, information security, records management and retention, privacy notices; management of personal data security breaches and complaints and how to conduct audits.

It was observed that where DPOs consulted with internal subject matter experts, such as those in records management and retention, their knowledge of what the law requires of them in this particular area was high. Where there were no consultations for example in learning and development a few of the DPOs could correctly list components of an awareness and training programme which is a component of learning and development.

Majority of DPOs had not been involved in conducting Data Protection Impact Assessments. Also most of the DPOs had not carried out a data protection and privacy audit . Majority of the DPOs shared the opinion that organisation audits should be carried out as often as every year, when there is a data security breach and when business changes.

Overall, most of the DPOs had limited skills required to perform tasks related to ensuring compliance under the Act.

5 RECOMMENDATIONS

Based on the DPOs' Training Needs Assessment findings, the following are the recommendations to address the identified gaps that may hinder efficient performance of tasks related to ensuring compliance of their organisations with the Data Protection and Privacy Act.

There is need for DPOs to be trained in the following areas that will support them in development and implementation of a Privacy Management Program;

- Development and implementation of policies and procedures on data protection and privacy; information security; records management and retention; and privacy notices
- Development and implementation of an awareness and training program
- Management and resolution of personal data security breaches and complaints
- How to conduct data protection and privacy audits and Data Protection Impact Assessments
- Overview of Cyber Security tools
- Conducting a Cyber Security Maturity Assessment
- Privacy by Design and Default
- Overview of cross-border data transfer mechanisms

PDPO should encourage DPOs to obtain certifications in data protection and privacy and in information security to advance their skills required to effeciently perform tasks related to ensuring their organisations' compliance with the Data Protection and Privacy Act.

PDPO should develop and publish guidance notes in the following areas;

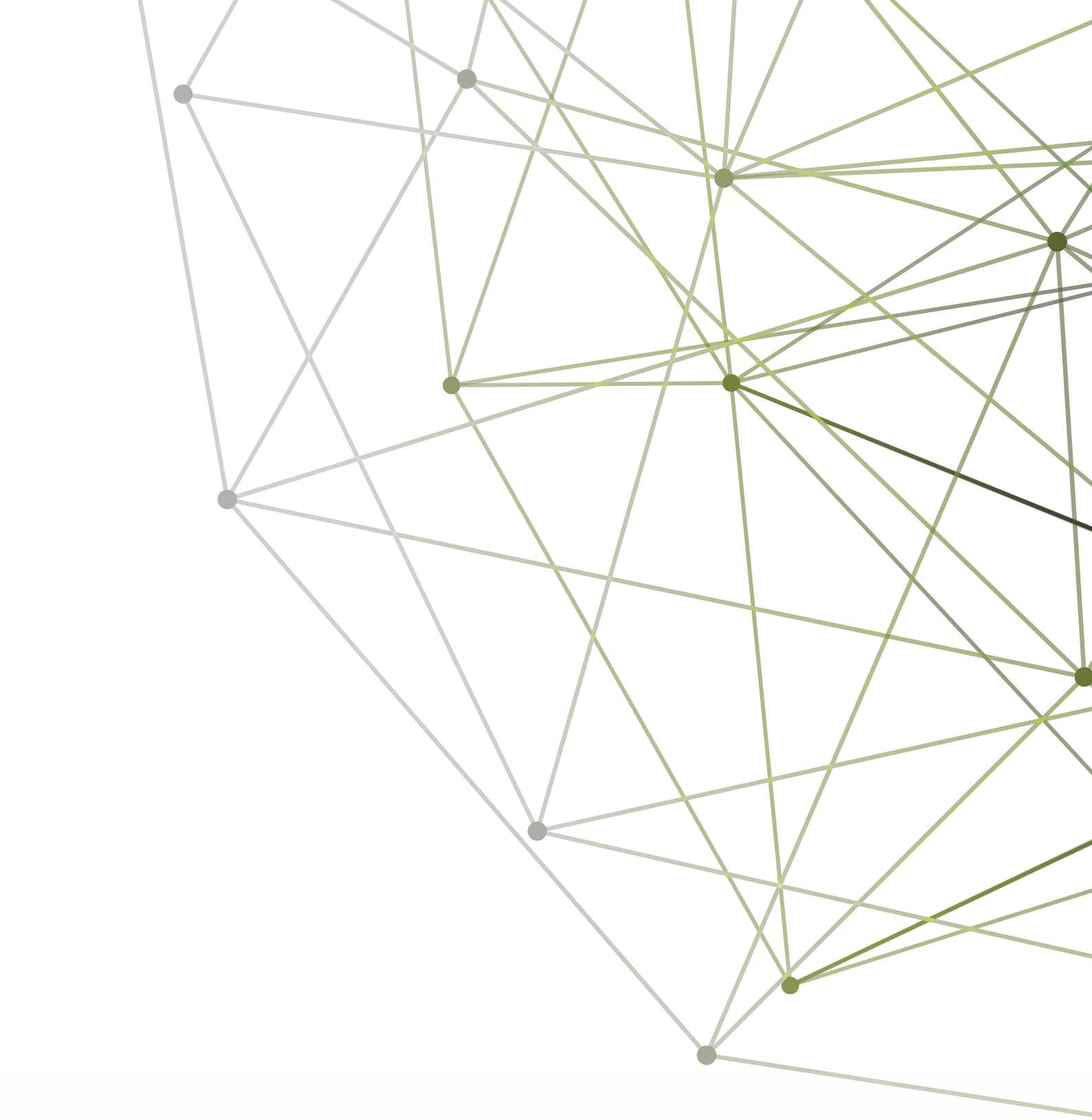
- Designation of a Data Protection Officer highlighting skills needed to perform the role.
- Cross-border data transfer mechanisms under the Data Protection and Privacy Act, 2019.

Ensure Compliance.

Personal DATA Protection OFFICE

Ensure that Employees / contractors / vendors comply with the Data Protection and Privacy principles.


● Designate a DPO
● Develop notices and policies
● Training and Awareness
1. Collection
● Implement Deletion procedures.
4. Disposition
High Level Data Protection and Privacy Compliance
2.Distribution
3. Inactive and Active storage
● Data Sharing agreements
● Non-disclosure agreements
● Implement security measures
● Develop Retention policies



+256 417 801 011
+256 417 801 008
+256 417 801 009

info@pdpo.go.ug
www.pdpo.go.ug
@pdpoUganda