Design and Development of Curriculum for The Personal Data Protection Office Training Center

Bench marking and Stakeholder Consultation Report

Submitted to:
The Digital Economy Lead,
Financial Sector Deepening Uganda,
Plot 7A, John Babiiha Avenue, Kololo.

And
The National Personal Data Protection Director
Personal Data Protection Office, PDPO
Plot 7a Rotary Avenue Lugogo by Pass

Submitted by:
Eight Tech Consults Limited
P.O.BOX 36859, Kampala
Magdalene Lane, Opposite Ndere cultural Centre,
Ntinda Kisaasi road
Tel: 0776-844343/0774600884
Email: ceo@8technologies.net
Website: www.8technologies.net

Date: April, 2024

Copyrights and Disclaimer

Foreword

Eight Tech Consults Ltd was contracted to undertake Consultancy for the **Design and Development of Curriculum for A Data Protection Training Center Under the Personal Data Protection Office** as contained in the Contract received from FSDU in line with the procurement reference Number: **FSDU/SRVC/2023/00087**. Pursuant to the terms of reference and all issuing confidentiality and non-disclosure bindings, **Eight Tech Consults Ltd** presents the bench-marking and stakeholder consultation report as a second deliverable of the assignment. The responses, conclusions and recommendations will be used for the development of a comprehensive curriculum and establishment of Data Protection Training Centre.

Dr. Drake Patrick Mirembe, PhD
Senior Consultant and CTO,
Eight Tech Consults Ltd.

Table of Contents

List of Tables

List of Figures

List of acronyms

8TECH	**Eight Tech Consults Ltd**
APEC	Asia-Pacific Economic Cooperation
BOU	Bank of Uganda
BCS	British Computer Society
CDPSE	Certified Data Privacy Solutions Engineer
IIA	Institute of Internal Auditors
ITC	Insurance Training College of Uganda
CEH	Certified Ethical Hacker
CHFI	Certified Hacking Forensic Investigator
CIPM	Certified Information Privacy Manager
CIPP	Certified Information Privacy Professional
CIPT	Certified Information Privacy Technologist
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Management.
CISSP	Certified Information System Security Professional
CPA	Certified Public Accountant
DPA	Data Protection Training Center
DPO	Data Protection Officer
FIPA	Freedom of Information and Privacy Association
FSDU	Financial Sector Deepening Uganda
GDPR	General Data Protection Regulation
IAPP	International Association of Privacy Professionals
ICT	Information and Communications Technology
ISACA	Information Systems Audit and Control Association
LCD	Liquid Crystal Display
M&E	Monitoring and Evaluation
Mak	Makerere University
MoICT & NG	Ministry of Information Technology and National Guidance
MS	Microsoft
MUBS	Makerere University Business School
NCDC	National Curriculum Development Centre
NITA-U	National information Technology Authority Uganda

PDPL	Personal Data Protection Law
PDPO	Personal Data Protection Office
PECB	Professional Evaluation and Certification Board
PIA	Privacy Impact Assessment
PIPED	Personal Information Protection and Electronic Documents Act
RFCs	Request for Comments
UBTEB	Uganda Business and Technical Examinations Board
UICT	Uganda Institute of Communication Technology
WOUGNET	Women of Uganda Network
PDPOTC	The Personal Data Protection Office Training Centre

1. Introduction and Background

Eight Tech Consults Ltd (hereinafter referred to as "the Consultant") was contracted under Procurement number: **FSDU/SRVC/2023/00087** by FSDU (hereinafter referred to as "the Client") to Design and Develop a Curriculum for The Personal Data Protection Office Training Center (PDPOTC) under the Personal Data Protection Office (PDPO). It is worth noting that the development of the proposed curriculum is informed by the extensive DPO knowledge and skills gap analysis study which was conducted by PDPO. The study found that most DPO's lack sufficient knowledge and skills to enforce the provisions of the personal data privacy and protection Law. Thus, in order to develop a pragmatic curriculum for PDPO training Centre and in line with best practices of curriculum development and per the Terms of Reference for the assignment, an extensive stakeholder consultation and bench marking exercised was conducted. This document is a process deliverable and articulates the key highlights of the stakeholder consultation and bench marking.

1.1 Introduction

A comprehensive stakeholder consultation and bench marking exercise was undertaken to inform the development of a robust curriculum for PDPO Training Centre. To develop appropriate curriculum aligned to the knowledge and skills demand of all actors along the data Lifecyle value chain, it is important to seek stakeholders' inputs, but also benchmark with best practices from other domains. This report presents key stakeholders' insights in terms of; awareness of national and international legal and regulatory frameworks, capacity building requirements for various actors along the personal data Life cycle, available training opportunities in areas of personal data protection and privacy, modes of training delivery of similar programmes, best practices in running similar programmes and accreditation frameworks among others.

1.2 Background

The Personal Data Protection Office was established by the Data Protection and Privacy Act, 2019, with a core mandate of regulating the collection, processing and use of personal data in Uganda. PDPO operates as an independent office under the supervision of the National Information Technology Authority, Uganda (NITA-U) Board which is responsible for overseeing the implementation of and enforcement of the Data Protection and Privacy Act 2019. The Law regulates the collection, processing and use of personal information and protects the rights of the persons whose data is collected.

The Data Protection and Privacy, Act 2019 Section (5) provides the key functions of the Personal Data Protection Office headed by the Director. The roles of the Office are further elaborated in the Data Protection and Privacy Regulations 2021 section 4 (a, d & h) which grants the powers to The Personal Data Protection Office (PDPO) to set, monitor and regulate standards in the areas of Data Protection and Privacy, but also build capacity of data controllers and processors to enhance compliance with the Law. While the Law clearly describes the profile of the holders of the Personal Data Protection Office (PDPO), it does not provide similar characteristics for Data Protection Officers (DPO) in terms of education background, personal traits, knowledge and skills desired to perform these roles. In executing the mandate, the PDPO commissioned a Needs Assessment study to establish the level of knowledge and skills possessed and required by the designated Data Protection Officers among registered data

controllers and processors so as to inform the capacity building needs and approaches of meeting their needs.

The results of the Needs Assessment revealed that the majority of DPOs possessed limited knowledge and skills to perform tasks related to ensuring compliance under the Law. The study findings showed that majority of DPO's (90.6%) did not have any formal training and certification in data protection and privacy, about (64.2%) of DPO's had never participated in detection, identification and reporting of personal data breaches and a whooping (90.6%) had never resolved any data protection and privacy complaint. Yet, these are critical knowledge and skills areas for DPO's to be effective in enforcing the compliance with the law.

Therefore, the study recommended various capacity building areas for DPOs including: *Development and implementation of policies and procedures on data protection and privacy; information security; Basic knowledge on cyber security tools; Conducting a cyber security maturity assessment; 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; Data protection and privacy audits; Data protection impact assessments; Privacy by design and default; and Management of cross-border data transfer mechanisms*.

It was observed that the needs assessment study of 2022 was limited only to designated DPO's therefore, there was a need to seek inputs from others stakeholders so as to enrich the findings of the capacity building areas identified in the need's assessment report of November 2022. This, is critical for the development of a realistic curriculum that is responsive to the capacity needs of various actors/stakeholders along the data life cycle value chain.

1.3 Objectives and Research Questions

The main objective of stakeholder consultation and bench marking was to fill the ecosystem needs assessment gaps emerging from the need's assessment study of DPO capacity needs of November 2022, in order to have a demand driven and stakeholder responsive curriculum developed. The specific objectives were to;

i. Establish the level of awareness of the key data privacy and protection regulatory frameworks among stakeholders,
ii. Determine the data protection and privacy key capacity building needs of stakeholders involved along the data life cycle value chain
iii. Establish best practices in developing and running professional certification programmes,
iv. Establish how to operationalize the Data Protection and Privacy Training Centre.

2. Approach and Methodology

The section below describes the approach and methodology used for the stakeholder consultation and the bench marking.

2.1 Stakeholder Consultation Approach and Methodology

In term of approach for stakeholder consultation, the consultant adopted the Five Step Best Practice model of effective stakeholder consultation comprised of the following steps; a) *Stakeholder identification, b) Determination of consultations methods, c) Conduct consultations, d) Analyze stakeholder feedback, and e) report consultation outcomes*. The consultant applied a knowledge co-creation, participatory and consultative approach in the implementing the five steps best practice model of effective stakeholder consultation, involving the consulting team, FSDU project team and PDPO technical team.

a) **Stakeholder Identification:** Stakeholders were identified through a consultative process involving the consultant, PDPO and FSDU teams. The 8TECH in consultation with the Client PIT conducted a stakeholder mapping and established key stakeholders for consultation. The organizations were selected based on their roles in processing large data sets or running professional training programmes. The respondents from these organizations were identified based on their critical role along the data lifecycle or their role in human capacity development in entities providing similar programmes. The individual respondents and some key informants were identified by the designated accounting officers of the target organization based on; their involvement in the different forms of data processing, their capacity to handle big data volumes, expertise in information security, their experience in the areas of data protection, their experience in curriculum development, and their knowledge of the different data privacy, protection frameworks, knowledge and experience in professional certification programmes among others (*Refer to Annex III: List of stakeholders consulted)*

b) **Determination of stakeholder Consultation Methods:** The stakeholder consultation method was determined through a consultative process involving the consultant and the client. The choice of consultation methods was informed by the nature of information desired from the stakeholders, stakeholder preference and stakeholder availability. ***Explorative Key Informant Interviews*** and a ***Focus Group Discussion*** were used to gather information from stakeholders. (*Refer to Annex II)*

c) **Consultation Process:** This step involved developing a comprehensive roadmap for the stakeholder consultation process, preparation and delivery of introduction letters and follow up communication, request and scheduling of appointment, sharing of tools to enable sufficient stakeholder preparation for the KIIs. The scheduling was designed with flexibility putting into consideration their availability of stakeholders and the fact that this work is voluntary. The schedules is maintained in a shared drive and all communications had the PDPO and FSDU team copied in.

d) **Conducting stakeholder Consultations and FDGs:** A total of 94 stakeholders were consulted, 84 KII where majority (74 KII) were conducted online while ten (10 KII) were done physical. One FGD was conducted virtually with 10 respondents.

e) i. **Analysis of Stakeholder Feedback:** A thorough review and analysis of the gathered information, identifying common themes, recurring concerns, and noteworthy recommendations was done and is presented in this report.

2.2 Approach and methodology to Desk review and Bench Marking

The Bench marking process for the development of the Data Protection and Privacy Curriculum involved a systematic and strategic approach to comparing educational practices with industry leaders and recognized standards.

The bench marking methods followed a 4-step framework as shown in the figure 1 below;

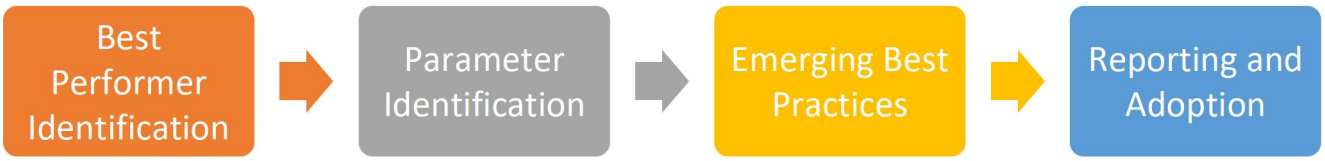

Figure 1: Step by step guide to international bench marking

a) Best Performer Identification:

This step involved identifying organizations / institutions that are considered a) best performers in the field of data privacy and protection, b) Carrying out similar or related professional certification or trainings within the country and outside. Some of the institutions selected include; Information Systems Audit and Control Association (ISACA), Professional Evaluation and Certification Board (PECB), International Association of Privacy Professionals (IAPP), - British Computer Society (BCS), Privacy and Electronic Communications Regulations (PECR), International Council of E-Commerce Consultants, Institute of Certified Public Accountants of Uganda(ICPAU), Institute of Internal Auditors(IIA), Insurance Training College, Uganda Management Institute, East African School of Taxation, MAT Abacus as an ACCA training centre and Uganda Law Society.

b) Parameter Identification:

Parameters of success in data protection and delivery of related certifications are determined based on the practices of the identified best performers. These parameters included; the training modules covered, the course load, certification period and type, the topics covered, the accreditation framework and requirements for the participants to take up the courses. Clear criteria was established to evaluate the effectiveness and relevance of these parameters to the specific context of the curriculum development for the Personal Data Protection Office.

c) Emerging Best Practices:

During the analysis, emerging best practices and innovative approaches in data privacy and protection education were discovered. These practices were chosen based on the parameters identified earlier. By integrating these emerging practices into the curriculum development

process, cutting-edge strategies aligned with global trends were incorporated, fostering continuous improvement in data privacy education.

d) Reporting and Adoption

After integrating emerging best practices into the curriculum development process, the identified areas have been documented in this report and will be incorporated into the recommendations for adoption in the curriculum for data protection and privacy.

3. Bench Marking Findings

Benchmarking is an important tool for organizations to identify best practices, improve their processes, and enhance their performance and competitiveness. In this section, we present benchmarking findings on the summary of related programs, key lessons learned and information on accreditation bodies in the areas of Data Protection and Privacy as detailed in the table below.

3.1 Information about Data Protection and Privacy Training Accreditation bodies

Institutions	Course/ Certificate Level	Description	Training Mode	Course Load	Topics Covered	Accreditation	Certification Requirements
ISACA[1]	Certified Data Protection Solutions Engineer (CDPSE)	Designed for those experienced in the governance, architecture, and lifecycle of data privacy at a technical level.	Online In-person,	20hrs a week for several months	• Privacy Governance (34%) • Privacy architecture (36%) • Data Life Cycle (30%)	ISO/IEC 17024:2012	i. Passing the CDPSE exam and Applying for Certification ii. Three (3) or more years of experience in data privacy governance, privacy architecture, and/or data life cycle iii. This experience must be in at least Two CDPSE examination content outline domain areas. No experience waivers or substitutions.
	Certified Information Systems Auditor (CISA)	Designed for IT/IS auditors, control, assurance and information security professionals.	Online In-person,	20hrs a week for 4months	• Information System Auditing Process (21%) • Governance and Management of IT (17%) • Information		i. Passing the CISA exam and Applying for certification ii. Five (5) or more years of experience in IS/IT audit, control,

[1] https://www.isaca.org/training-and-events

					system Acquisition, Development and Implementation (12%) • Information Systems Operation and Business Resilience (23%) • Protection of Information Assets (27%)		assurance, or security. iii. Experience waivers are available for a maximum of three (3) years
	Certified in Risk and Information Systems Control (CRISC)	Designed for those experienced in the management of IT risk and the design, implementation, monitoring and maintenance of IS controls	Online In-person,	20hrs a week for 4months	• Governance (26%) • IT Risk Assessment (20%) • Risk Response and Reporting (32%) • Information Technology and Security(22%)		Three (3) or more years of experience in IT risk management and IS control. No experience waivers or substitutions
	Certified Information Security Manager (CISM)	Designed for those who manage, design, oversee and assess an enterprise's information security function.	Online In-person,	20hrs a week for 4months	• Information Security Governance (17%) • Information Security Risk Management(20%) • Information Security Program (33%) • Incident management(30%)		Five (5) or more years of experience in information security management. Experience waivers are available for a maximum of two (2) years

	Certified in Governance of Enterprise IT (CGEIT)	Recognizes a wide range of professionals for their knowledge and application of enterprise IT governance principles and practices.	Online In-person,	20hrs a week for 4months	• Governance of Enterprise IT (40%) • IT Resources (15%) • Benefits realization (26%) • Risk Optimization(19%)		Five (5) or more years of experience in an advisory or oversight role supporting the governance of the IT-related contribution to an enterprise. Experience waivers are available for a maximum of one (1) year.
PECB[2]	Privacy Information Management System	Foundation (Best practices of privacy Information Management Systems)	self-paced online course, instructor-led workshop	8hours per day for 3days	• Introduction to PIMS concepts as specified in ISO/IEC 27701 • PIMS and certification exam	ISO/IEC 27701	
		Lead Implementer		8hours per day for 5 days	• Fundamental principles and concepts of a PIMS • PIMS controls and best practices • Planning a PIMS implementation based on ISO/IEC 27701 • Implementing a PIMS based on ISO/IEC 27701 • Performance evaluation, monitoring and measurement of an ISMS based on ISO/IEC • 27001 • Continuous improvement of a	ISO/IEC 27701	Two years of work experience in Privacy Information Management Project activities: a total of 300 hours Signing the PECB Code of Ethics

[2] https://pecb.com/en/education-and-certification-for-individuals/gdpr/gdpr-foundation

					PIMS based on ISO/IEC 27701 • Preparing for a PIMS certification audit		
		Lead Auditor	self-paced online course, instructor-led workshop	8hours per day for 5days	• Introduction to PIMS • Audit principles, preparation and launching of an audit • On-site audit activities • Closing the audit	ISO/IEC 27701	Two years of work experience in Privacy Information Management Project activities: a total of 300 hours Signing the PECB Code of Ethics
	General Data Protection Regulation	Foundation Certified Data Protection Officer	self-paced online course, instructor-led workshop	8hours per day for 3days	• Introduction to the GDPR concepts and principles • Designation of the DPO and analysis of the GDPR compliance program • DPO operations • Monitoring and continual improvement of GDPR compliance	ISO/IEC 27701	Participants attending this training course are required to have a fundamental understanding of the GDPR and comprehensive knowledge of data protection requirements.
The International Association of Privacy Professionals (IAPP)[3]	• Certified Information Privacy Professional(CIPP)[4]	CIPP designations verifies your understanding of data protection laws, regulations and standards in	Online self-paced In-person,	8hrs per day for 7days	• Privacy Laws, Regulations, Practices • Use effective strategies for developing and	ANSI/ISO/IEC Standard 17024	At least 2 years' experience in projects, activities, tasks related to the missions of the DPO. Have at least two years of professional experience,

[3] https://iapp.org
[4] https://iapp.org/search/#!?q=cipp

	• Certified Information Privacy Manager (CIPM)[5] • Certified Information Privacy Technologist (CIPT)	your jurisdiction or discipline. CIPM certification attests to your understanding of how to implement data privacy regulations into day-to-day operations. CIPT endorses your understanding of the use of technology in building data protection practices into products and services.			implementing a privacy program. • Integrate privacy requirements into organizational policies and procedures. • Create a culture of privacy awareness. • Effectively plan for and respond to a data security breach. • Monitor, measure, analyze and audit privacy program performance. • Define key concepts of data protection. • Describe data protection laws and regulatory bodies. • Explain the application of the GDPR and other compliance obligations to European and international entities		as well as at least 35 hours in personal data protection given by a training establishment. Achieve 75% score on an exam. Score at least 50% on each of the three blueprint domains
The Privacy and Electronic	• Data Protection and PECR		online	8hrs a day for	• GDPR Principles • Data protection	IAPP	Attendance at training sessions

5

Communications Regulations (PECR)[6]				7days	impact assessments • Data breaches • Privacy and Electronic Communications Regulations		Completion of required assessments/exams Payment of course fees
EC Council[7]	• Certified Ethical Hacker -Entry-level	It covers many different technologies, but systematically applying the methodologies taught to evaluate any infrastructure.	Live, online, In-person,	8hrs a day for 7days	• Ethical hacking • Penetrating testing • Networking security • Information security laws and standards	ANAB(ANSI) 17024	A minimum of 2years IT Security experience before attempting the course. If you do not have the experience it is recommended to take the free cyber security essentials series.
	Certified Hacking Forensic Investigator • Intermediate-level	This program prepares cyber security professionals with the knowledge and skills to perform effective digital forensic investigations and bring their organizations into a state of forensic readiness.	Online Hands on labs	8hrs a day for 7days	• Computer forensics in today's world • Investigation process • Understanding hard disks and file systems • Data acquisition and duplication • Windows forensics • Network forensics • Email and social media • etc	ANAB(ANSI) 17024	An IT/ Forensic professional with basic knowledge of IT/Cybersecurity, computer forensics, incident response and threat vectors
Cousera	Data Privacy Fundamentals	Provides foundational	Online, self paced	2hrs a week for	• Privacy in the Digital age	Coursera Inc	Individuals in related field

[6] https://www.legislation.gov.uk/uksi/2003/2426
[7] https://www.eccouncil.org/train-certify/certified-ethical-hacker-ceh/

		understanding of digital age privacy concepts and theories.		3weeks	• Risk in Data Privacy • Framework of Data Privacy Law		
	Privacy Law and Data Protection	Provide methods for protecting privacy using the fair information principles and identify laws and regulations that pertain to data protection	Online, self paced	12hrs	• Privacy: Legal Issues, Landscape and Chronology • HIPAA • Security and Breach Notification • Other Ways that Privacy is Regulated	Coursera Inc	Individuals in related field
	Privacy Fundamentals Specializations	Introduces learners to fundamental privacy concepts, frameworks and laws.	Online , self paced	5hrs a day for 3-6months	• Introduction to Privacy, part 1, 2 and part 3. • Fundamental Privacy Acts and Laws	Coursera Inc	Individuals in related field
	Regulatory Compliance Specialization	Teaches learners to create a thorough risk profile, tailor a comprehensive compliance program and develop strategies for implementing the technologies, policies, monitoring and training an effective privacy compliance program.	Online, self-paced	5hrs a day for 6months	• What is Compliance • Effective Compliance Programs • Privacy Law and Data Protection • What is Corruption: Anti-Corruption and Compliance	Coursera Inc	Individuals in related field
	Privacy and Standardization	Introduces	Online ,	10hrs a	• Privacy in the	Coursera Inc	Individuals in related

	Specialization	learners to the huge societal role of standards and value the development and fundamentals of good standards	self-paced	week for 2months	Western World • Privacy in the USA • Privacy in the Europe • Standardization and Technology • Privacy and Standardization Capstone		field

3.2 Information about Other certifying Institutions

Institutions	Course/ Certificate Level	Description	Training Mode	Course Load	Topics Covered	Accreditation	Admission Requirements
Institute of Certified Public Accountant of Uganda (ICPAU)[8]	Certified Public Accountant	The CPA(U) course is designed to produce competent professional accountants, capable of making a positive contribution to the profession and the national economy in general, It has 4 levels.	Physical Online Self-Study	Varies	• Financial accounting • Management accounting • Auditing, Taxation • Business law, • Ethics, Business environment and concepts.	ICPAU	A diploma pursued in a period of at least two years from a recognized university or Institution of Higher Learning. At least two principal passes at A-Level with at least 5 credits at O-Level including English Language and Mathematics Recommendation letter from either an employer, A training institution, a person in position of responsibility.
	ACCA	A global professional accounting body offering the Chartered Certified Accountant qualification.	In-person, Online	Varies	• Financial accounting, Management accounting, Audit and assurance, Taxation, • Corporate business law, • Taxation, Strategic Financial reporting, Strategic business analysis	ICPAU	2 Passes at Uganda Advanced Certificate of Education (UACE) / GCE A Level 3 Passes at Uganda Certificate of Education (UCE). In 5 separate subjects including English and Mathematics. Degree A degree from a recognized university

[8] https://www.icpau.co.ug/

MAT ABACUS Business School[9]	ACCA, CPA, CISA, PMP, CIM, CIPS, CFA, CIA and Bespoke courses	The School provides consulting support to institutions to assist them in their quest to achieve management excellence through professional courses.	Physical In-Person Online	Varies on the course	• For Bespoke courses; Family Business. Finance for Non Finance Managers, Customer Experience, Leadership in Turbulent Times, Risk Management, Managing SME's.	An approved learning partner that works with several accrediting institutions	Varies on the particular course but general requirements cut across a diploma/Degree from a recognized university and evidence of professional work experience.
Institute of Internal Auditors(IIA)[10]	Internal Audit Practitioner Certified Internal Auditor Certification in Risk Management Assurance	The IIA's Certificate Programs are designed to enable highly accessible, and flexible, regardless of job level, title, or years of experience.	Instructor-Led Training In-Person Online	2yrs	• Internal Control Frameworks (e.g., COSO) • Risk Assessment and Management • Audit Planning and Execution • Conducting Internal Audit Consultations • Business Processes and Management • Information Technology (IT) Auditing	**IIA**	A copy of your degree or official transcripts. (If your name has changed since you earned your degree, you must also include your legal name change document.) • A letter from your college or university confirming your degree. • A letter from an academic evaluation service confirming your degree level.

[9] https://matabacus.ac.ug/our-story/
[10] https://www.theiia.org/en/certifications/

					• Enterprise Risk Management (ERM) Frameworks (e.g., COSO ERM) • Risk Assessment and Control Techniques • Compliance Management		
Insurance Training College of Uganda (ITC)[11]	Certificate of proficiency Certificate of Insurance	It is designed to equip students with an understanding of the insurance industry and the types of products insurance that individuals or organizations might buy	Instructor-Led Training Online	2hrs per day for 3weeks 5hrs per day for 6months	• Introduction to Insurance, Policies and Coverage • Risk Management • Legal & Regulatory Framework • Ethics Professionalism • Insurance Industry Trends • Sales and Marketing	NCHE	Uganda Certificate of Education (UCE) with a minimum of three passes. Possession of appropriate or relevant professional qualifications
East African School of Taxation[12]	The Diploma in Tax and Revenue Administration.	The school also offers training in in income tax and revenue administration tax planning processes, salary, and benefits tax consultancy, tax management systems and tax audits.	In person online		Tax Law, VAT Law & practices, tax practice, public finance, international taxation, financial accounting, customs law & practice, Research & projects	NCHE	Applicants for the DITRA course must be either holders of a degree from a recognizable university or members of professional bodies such as ACCA, CIMA, CPA, ICS, ICSA or ICAE & W.

[11] https://itc.ac.ug/certified-courses
[12] https://eastaxation.com/store/Compendium-of-Domestic-Tax-Laws-p624611205

Civil Service College	The college is dedicated to building capacities of Public Service Institutions and Human Resources for improved performance in Public Service delivery.	The College is responsible for in-service training, strengthening public policy research, providing advisory services and supporting innovations for improved service delivery	In person Online	Varies	• GBV responsive planning and budgeting • Corporate governance • Strategic Leadership and management • Gender Based Violence Response • Among others	Ministry of Public Service	Members in public services

3.2 Conclusions and Lessons Learned

In reviewing the diverse array of institutions offering training and certification programs in data protection and privacy, several standout practices and considerations emerge. These insights can inform decisions and considerations for enhancing our curriculum in this critical area:

Flexibility and Accessibility: Many institutions offer online training modes alongside in-person sessions, providing flexibility to learners. Adopting a blended approach to training delivery could enhance accessibility and accommodate diverse learner preferences.

Comprehensive Coverage of Topics: Training programs cover a broad spectrum of topics relevant to data protection and privacy, including governance, risk assessment, compliance, and incident management. Ensuring the curriculum encompasses a comprehensive range of topics will equip learners with the knowledge and skills needed to address complex privacy challenges.

Hands-on Learning and Practical Application: Some programs include hands-on labs, workshops, or project activities to reinforce learning and facilitate practical application of concepts. Integrating experiential learning opportunities into our curriculum can enhance consultation and skill development among learners.

Specialization and Customization: Institutions offer specialized certifications tailored to different roles and expertise levels within the field of data protection and privacy. Consideration should be given to offering specialized tracks or certifications within the curriculum to cater to the diverse needs and career paths of learners.

Continuous Improvement and Adaptation: The dynamic nature of data protection and privacy requires ongoing updates and adaptations to curriculum content. Establishing mechanisms for continuous review and improvement of the curriculum will ensure it remains relevant and responsive to evolving industry trends and regulatory requirements.

Accreditation for Credibility and Recognition: Institutions such as ISACA and PECB prioritize accreditation from recognized bodies like ISO/IEC and ANSI/ISO/IEC. It is worth noting that institutions providing data protection training are mainly accredited by international bodies while local institutions providing other types of certifications are leveraging on the national bodies. Hence for the development of the PDPO curriculum for data protection and privacy training, there is need to seek accreditation from recognized international accreditation bodies inorder to deliver an all-round certification.

Course Load and Experience Requirements: Institutions such as ISACA and PECB offer flexibility in course load, allowing learners to choose from various training modes and durations based on their schedules and learning preferences. In Uganda, we can adopt a similar approach by offering flexible course structures that accommodate the diverse needs of learners, including part-time options for working professionals. Additionally, by considering experience requirements for enrollment, we can ensure that the curriculum is tailored to the skill levels and career stages of participants. Aligning experience requirements with local industry standards and job market demands will enhance the relevance and effectiveness of the training programs, ultimately empowering learners to succeed in their respective fields.

Based on the findings from the desk review and bench marking, it is clear that there is a diverse range of options available, each with its own focus and requirements. To inform the development of DPO training curriculum in Uganda, it is recommended to tailor the curriculum to address specific local needs and challenges. This could include incorporating modules on the local data protection laws and regulations, as well as practical case studies relevant to Ugandan organizations. Additionally, considering the varying levels of experience and education required for different courses, offering a range of certification levels could help accommodate individuals at different stages of their careers. Collaborating with international accreditation bodies such as ISACA, PECB, and IAPP could also enhance the credibility and recognition of the training courses in Uganda. It is recommended that the courses emphasize not only legal and regulatory aspects but also the practical implementation of data protection principles. Moreover, the training should be accessible and affordable, potentially leveraging online platforms to reach a wider audience. Ongoing monitoring and evaluation should be conducted to ensure the courses remain relevant and impactful in Uganda's evolving data protection landscape.

4. Stakeholder Consultation Key Findings

The section below details the stakeholder consultation findings.

4.1 Respondent Demographics

The study engaged a total of 94 respondents, comprising of 68 males and 26 females of which 60% were from the public sector and 40% from the private sector. Among the respondents, the highest number came from CSO/NGO; ICT/Cyber Security Officials; Legal and lowest from PDPO, Financial Institutions, Utility and Telecommunication Industry respectively as described in the figure 2. Information extracted from the respondents indicated that there were more certificate holders with 71.3% as compared with those who did not have (28.7%). Also, amongst the respondents it was found that those who had a Cyber Security Certificate were 21 (25.6%), Data Protection and Privacy were 15 (18.3%) and the highest number of respondents (46 – 56.1%) were found to have other certificates such as ACCA, CPA among others. It should be noted that the respondents who indicated to have certificates, several of them had multiple of them in the different areas as illustrated in the figure below.

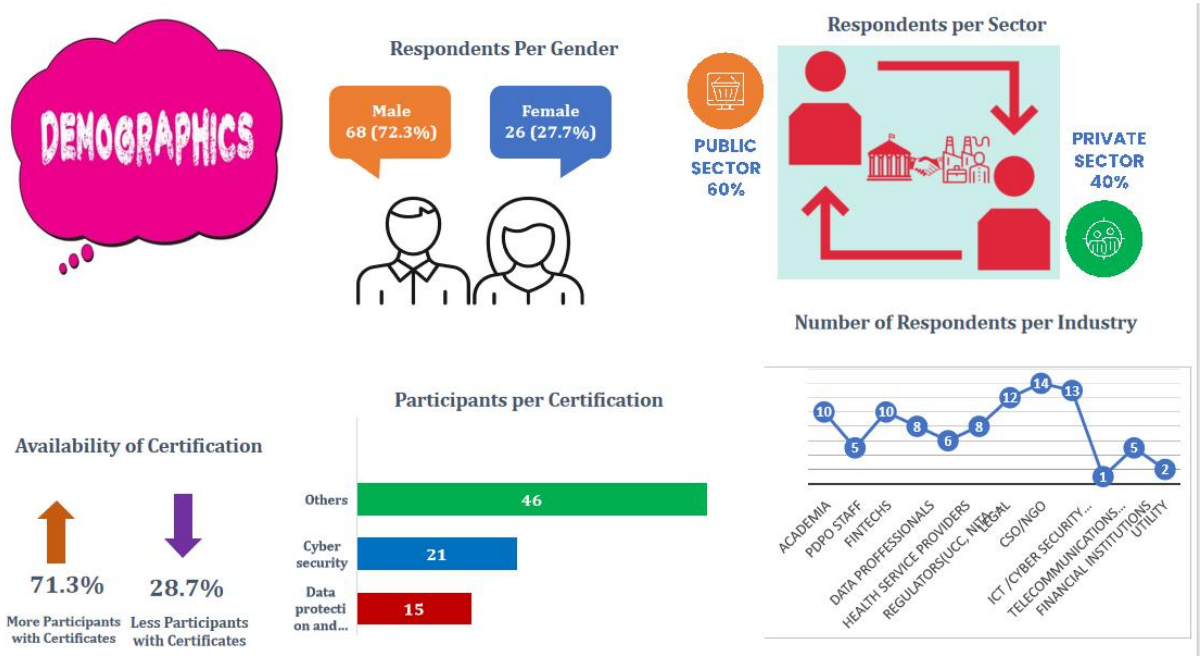

Figure 2: Summary Demographics of the Respondents

4.2 Key Policy Legal and Regulatory Environment Governing Data Protection Nationally and Internally

This section delves into the key policy, legal, and regulatory frameworks shaping the data protection landscape on both Nationally and Internationally level. From foundational principles enshrined in national laws to intricate agreements forged across international boundaries, understanding the complex web of regulations governing data protection is essential for navigating the complexities of the digital age. Through comprehensive analysis and exploration, the following are discussed; a) the awareness of national data protection legal and regulatory frameworks, b) awareness of existing international laws and regulations that serve as the

foundation for data protection on a global scale, c) The key roles of the Data Protection Officer (DPO) within organizations.

a) Awareness of National Data Protection Legal and Regulatory Frameworks

There are several laws and frameworks that streamline the undertakings within the Data Protection and Privacy life cycle ecosystem. Nationally, the public has been made aware of the existence of such frameworks as depicted in the figure 3 below. As depicted in the figure 3, the level of awareness from the respondents was lower (39.4%) as compared to those who were not aware (60.6%). Further still, the highest number of respondents who indicated to be aware of the legal and regulatory frameworks were from ICT Industry Professional (23.4%), Fin techs & Financial Institutions (16%), CSO/NGO (14.9%) and the lowest were PDPO Staff (5.3%), Health Service Providers (6.4%) respectively. The research team further sought to find out which of the National Legal and regulatory Frameworks were known by the respondents and the following was noted. The majority of the respondents were aware of the Data Protection and Privacy Act, 2019[13] with (26.1%), followed by the Computer Misuse Act, 2011[14] with (21.8%) and the lowest were Access to Information Act of Uganda 2005[15] with (5.6%) and Registration of Persons Act ,2015[16] with (1.4%) respectively as illustrated below.

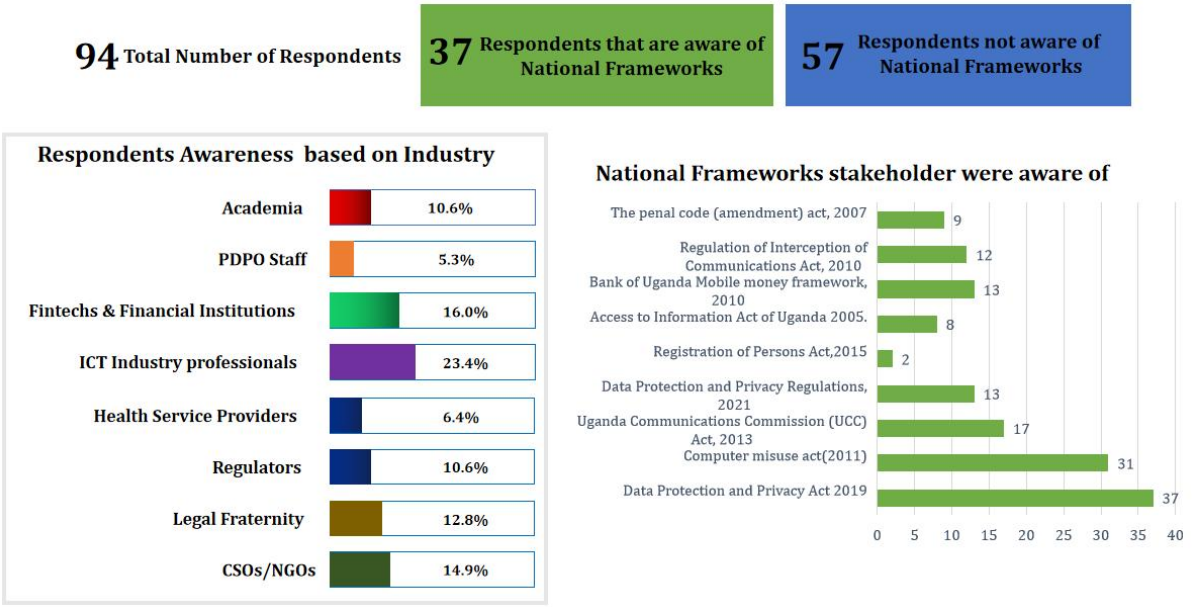

Figure 3: Awareness of the National data protection legal and regulatory frameworks

The National Data Protection and Privacy Lifecycle Ecosystem has already multiple legal and regulatory frameworks geared to streamlining the undertaking. It was clear that some respondents were aware of more than one legal and regulatory framework. This indicates that there are some efforts from the different organizations to create awareness of the existing

[13] https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://ict.go.ug/wp-content/uploads/2019/03/Data-Protection-and-Privacy-Act-2019.
[14] https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://ict.go.ug/wp-content/uploads/2019/12/UGANDA-Computer-Misuse-Act-No.-2-of-2011-1.pdf
[15] https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=http://judiciary.go.ug/files/downloads/access%2520to%2520informatioinformation%2520Act2005.pdf
[16] https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.ict.go.ug/wp-content/uploads/2018/06/Registration-of-Person-Act-2015.pdf

national legal and regulatory frameworks. One of the respondents from academia indicated the following during the study;

"These legal and regulatory frameworks guide our work and have been applied in the following ways: They outline specific requirements that we must adhere to when handling personal data, they enable us identify and mitigate risks associated with data processing activities. In conclusion, the legal and regulatory frameworks provide a comprehensive framework for guiding organizations in managing personal data responsibly, ethically, and lawfully."

b) Awareness of International Laws and Regulations in data protection and privacy

In regards to awareness of international Data Protection Legal and Regulatory Frameworks, of the 94 respondents for the study only 28 (29.8%) indicated to be aware and 66 (70.2%) were not aware of these frameworks.

Figure 4: Awareness of international data protection legal and regulatory frameworks

Out of the 28 respondents who acknowledged familiarity with certain international legal and regulatory frameworks, 26 provided details about the specific frameworks they knew. The largest portion (15 respondents, comprising 53.6% of the total) mentioned awareness of the General Data Protection Regulation (GDPR), followed by the ISO 27000 Series at 10.7%. Other frameworks were also cited which included; NIST Cyber Security Framework, ISO 27000 series, COBIT 2019, California Consumer Privacy Act (CCPA), China's Personal Information Protection Law, Personal Information Protection and Electronic Documents Act (PIPEDA), IOM Data Protection Policy, OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data as depicted in Figure 5.

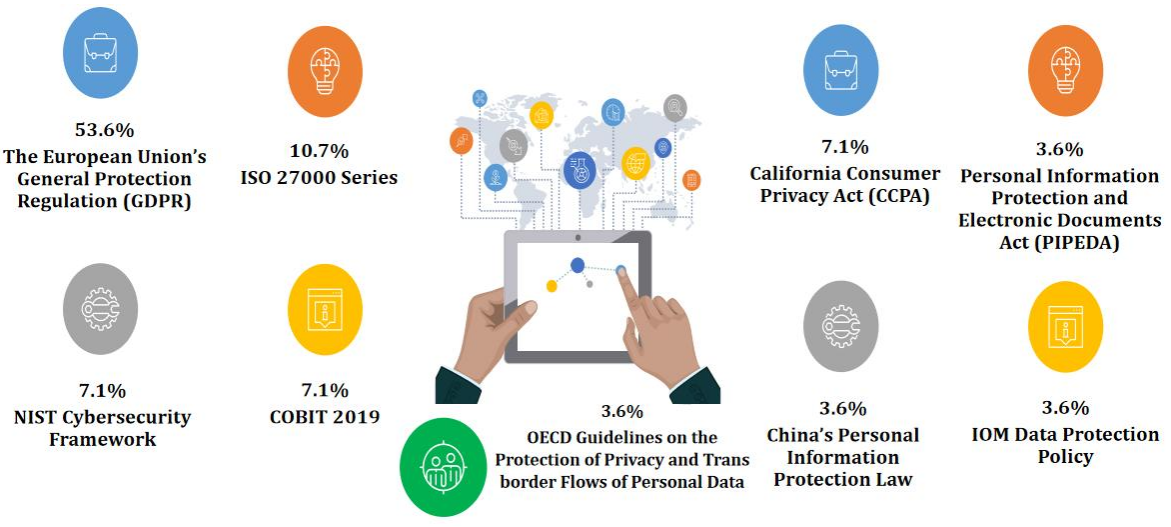

Figure 5: List of international data protection legal and regulatory frameworks that the respondents were aware of.

c) Guidance of the application of the frameworks in the work environment

Understanding how the data protection and privacy legal and regulatory frameworks influence the work environment was crucial. The following represent the responses provided by the respondents in regards to the ways the above identified frameworks guide their operations

i) Compliance Management at work: There's need of a clear understanding of the legal and regulatory frameworks in order to comply to the laws. For example, compliance management specifies requirements that must be adhered to in handling personal data responsibly, ethically, and lawfully.
ii) Safeguarding personal data collected from clients/customers/stakeholders,
iii) Guides the development of the data protection impact assessment,
iv) They enable identify and mitigate risks associated with data processing activities,
v) They promote transparency and accountability in a work environment,
vi) Development of internal data protection policies covering data collection, processing, storage, and security measures in regards to data subject rights, consent management, security measures, data breach response, data processing impact assessments,
vii) Providing training and awareness programs to employees to ensure they understand their responsibilities regarding data protection.

The above responses were further grounded by some key respondents from a regulator and Fintech who indicated that;

"Our Data Privacy Impact Assessments which are undertaken regularly are drafted and informed around the Personal Data Protection and Privacy Act 2019 and to some extent the GDPR as such we are always compliant with both laws in our activities." (Respondent from an ICT regulatory body)

"We ask clients for their consent when collecting any personal information, our data doesn't infringe on the privacy of our clients, we always let people know about the intended purposes of the collected data, we have measures in place to avoid abuse of this data." (respondent from a Fintech)

d) Level of awareness of Roles of Data Protection Personnel in the organization

Respondents were asked to mention key roles of a data protection personnel in their respective organizations and the table below summarizes their responses.

Industry	Roles of Data Protection Personnel
Academia	i. Safe guard sensitive personal information held by the organization ii. Act as a contact point for PDPO iii. Provide guidance on Data Protection Impact Assessments iv. Develop and implement procedures for responding to data privacy breaches v. Conducting regular audits of data processing activities to ensure compliance with the Law.

Legal Fraternity	i. Enforce Compliance of the law ii. Policy Development and Implementation iii. Conduct Training and Awareness and awareness of the Law iv. Risk Assessment and Management v. Data Subject Rights Management vi. Data Breach Management vii. Data Protection Impact Assessments (DPIAs)
CSOs / NGOs	i. Provide guidance on data collection, designing tools used, supervise data collection, regulate and set standards in data collection, audit, engage in further research ii. Guide in the implementation of the regulatory frameworks iii. Data Collection, Data Entry, Data Cleaning, Data Transformation, Data Storage, Data Analysis, Data Visualization, Data Interpretation, Data Reporting,
ICT Industry professionals	i. Training and awareness on compliance with data protection and privacy regulations, risks and threats. ii. Training staff on internal laws of data protection policy, iii. Monitor implementation of data protection systems iv. Maintaining the breach procedure.
Regulators (UCC, NITA-U, NSSF)	i. Defining what personal data is and its protection in this way it is well implemented. ii. Information security. iii. The Data Protection Officer is responsible for ensuring that an organization complies with data protection laws and regulations. iv. Monitors internal compliance to the PDPA Act 2018 v. Informs and advises on our data protection obligations considering all the relevant regulations vi. Act as a contact point/liaison for us and the PDPO Office.
Fin Techs and Financial Institutions	i. Defining what personal data is and its protection in this way it is well implemented. ii. Promoting a culture of privacy within the organization through training and awareness programs. iii. Ensuring that data processing activities are conducted in accordance with the principles of privacy by design and default.
ICT Industry Professionals	iv. Ensuring Information security v. Advising and guiding the organization on compliance with Uganda's Data Protection and Privacy laws. vi. Monitoring and ensuring compliance with data protection regulations within the organization. vii. Handling data subject requests, including access, rectification, and erasure requests. viii. Coordinating with supervisory authorities, ix. Conducting Data Protection Impact Assessments (DPIAs) where necessary. x. Managing data breach incidents, including investigation, notification, and mitigation. xi. Training employees on data protection laws and best practices. xii. They also serve as the point of contact for regulatory authorities

		in case of data breaches or other issues.
	xiii.	Manages risks related to data processing activities, and regularly reviews and updates data protection policies to reflect changes in laws, regulations, and business processes.

Table 1: Key Roles of Data Protection Officer in the organization

As we explore the findings from this section, it is worth noting that majority of the stakeholders that participated in the study stated that most organizations do not have/hire Data protection officers as a specific role. However, other roles within the organizations such as data analysts, cyber security experts, business development officers, research personnel's, among others were designated the roles of the data protection Officers. Respondents from an NGO, health sector, cyber security and ICT industry professional indicated the following;

"Yes, I know some but we don't have a DPO, we have data managers and they are responsible for data confidentiality in the organization, collecting cleaning and presenting or storing data" (Respondent from an NGO)

"We don't have a DPO at case hospital but we have a data manager who does some of these roles like ensuring data safety and security, organizing and analyzing data, training staff on how to manage the data," (Respondent from a health service provider)

"The Data Protection Officer (DPO) is responsible for advising organizations on data protection laws and regulations, monitoring compliance, conducting Data Protection Impact Assessments, and training employees on data protection laws and best practices. They also serve as the point of contact for regulatory authorities in case of data breaches or other issues. The DPO manages data subject requests, communicates about data protection matters internally and externally, ensures data security, promotes privacy by design and Default, manages risks related to data processing activities, and regularly reviews and updates data protection policies to reflect changes in laws, regulations, and business processes. However most organizations don't have DPOs" (Says a cyber-security expert)

"To secure organization information from loss, and any malicious attacks." (says an ICT Industry Professionals)

In summary, the findings emphasize critical aspects, outlining the requisite roles for data protection personnel to effectively carry out roles such as *Compliance Management, Data Protection Impact Assessment, Transparency and Accountability, and the formulation of Internal Data Protection Policies along with conducting Training and Awareness Programs*. Furthermore, the multifaceted responsibilities of Data Protection personnel across diverse organizations encompass *defining personal data, ensuring information security, overseeing compliance, developing policies, conducting training, assessing risks, and managing data breaches*. It is imperative for Data Protection Personnel to possess comprehensive knowledge of both national and international frameworks governing data protection and privacy.

4.3 Key capacity building needs for stakeholders involved in data collection, processing and data protection and Privacy

The sub section below details the capacity building areas for the data protection personnel in the following key areas; a) Knowledge and skills areas, b) Background Education/Profession c) Existing institutions providing data protection and privacy programmmes d) Future skills anticipated to be possessed by some data protection personnel.

a) Education Background for Data Protection Personnel

The study revealed that individuals executing the mandate of data protection personnel within organizations have diverse professional background majority being associated with responsibilities around information system management, records management, transaction processing among others. According to the DPO's Training Needs Assessment Report,2022, majority of the DPO's had backgrounds in IT/Computer Science courses or a related field making up nearly a third (32.5%) of all. The least proportion (3.3%) accounts for those professionals 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. Therefore, the design of the curriculum must take into the unique considerations of the professional backgrounds of individuals executing roles of data protection.

Furthermore, it emerged through this study that data protection and privacy role is largely delegated to technical staff (front line staff) yet it is also critical for decision makers within the organization. In order to establish an enabling environment and ensuring compliance with the law, as such the curriculum to be developed should provide opportunities for capacity building of a variety of stakeholders within the organizations including the key decision makers. Some of the respondent further grounded the issue by saying;

"I think we can give consideration to professions like ICT professionals, lawyers, business related individuals, statisticians, data scientists and among others since they have knowledge of some of the aspects to be covered in data protection like laws, Cyber security etc which will make the course beneficial to them and easy for them to grow in their roles." (respondent from the ICT industry professionals)

"The course should be open to everyone who is interested in being a data protection personnel provided it could be given sort of levels for people with a diploma, degree and others" (respondent from health service providers)

b) Level of Awareness of existing data protection and privacy training providers in Uganda

In the stakeholder consultations it was important to understand the level of awareness of data protection and privacy training providers in Uganda and majority of the respondents (65 out of 94) indicated that they were not aware of any institutions offering such training services, while the 29 respondents indicated to be aware of some of these institutions. Furthermore, it was important to establish the level of awareness of these institutions per industry of the respondents and it was established that the ICT industry professionals (15) were more aware followed by the respondents from the Regulators (5), Fin tech & Financial Institutions (5),

Academia (4) and PDPO (3) staff. The least level of awareness was noted from the CSO/NGO respondents (3), Health Providers (1) and the legal fraternity (1).

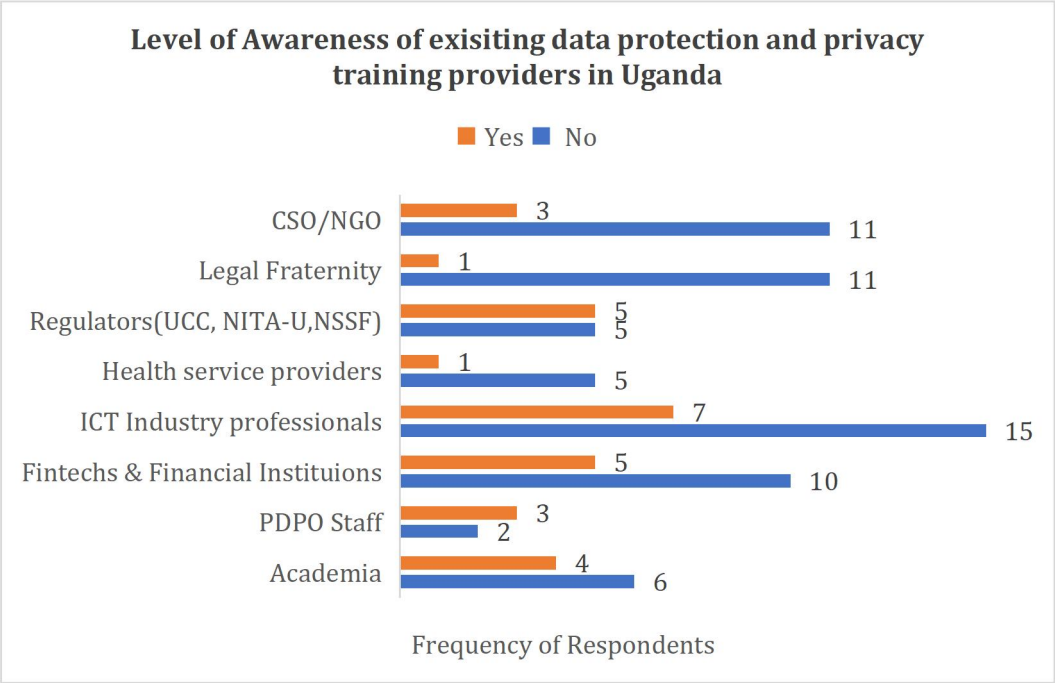

Figure 6: Level of Awareness of existing data protection and privacy training providers in Uganda

Some institutions mentioned to be providing data protection and privacy training in Uganda and their nature include;

Name of training service provider	Nature of programs	Training delivery mode	Certification	No. of responses
National Information Technology Authority (NITA-U)	Workshops	Online and physical.	Sometimes Certificates of attendance are given.	3
Personal Data Protection Office (PDPO)	Webinars Workshops	Online Physical	None	4
ISACA Kampala Chapter[17]	Various professional certifications e.g. (CISA and CISM)	Online	Various professional certifications (CISA and CISM)	6
Makerere University	Makerere University teaches modules in program of BRAM, BLIS, BIST and others about data management. In addition, the CIPSD offers a number of professional certifications related to	Physical	Offer professional certifications for the courses and other modules are embedded in their academic programmes	4

[17] https://engage.isaca.org/kampalachapter/home

	cyber security including; Ethical hacking, Data analysis and visualisation among others.			
Uganda Institute of Information and Communications Technology (UICT).	Some course Modules are embedded in programs such as RAM, DCT, DIST and also offer on demand customised training programs. Delivered by industry professionals.	Physical	Modules are in the academic programmes	3
Unwanted Witness	Free awareness and knowledge sharing workshops on data protection.	In-person sessions, workshops	Certificates of attendance	4
WOUGNET	Workshops for members and other organizations on Cyber security, data protection and privacy laws and best practices	Physical	None	5
Total				29

Table 2: Institutions providing data protection and privacy programmes in Uganda that stakeholders were aware of.

From the table above, the ISACA Kampala Chapter was noted for its provision of professional certifications such as CISA and CISM that are related to data protection and privacy, additionally. WOUGNET, UNWANTED WITNESS, PDPO and National Information Technology Authority (NITA-U) stood out with few responses for offering awareness workshops focused on providing guidelines and knowledge of data protection and privacy to other individuals and organizations.

Furthermore, it was noted from some academic stakeholders that institutions such as Makerere University and Uganda Institute of Information and Communications Technology (UICT) offered degree and certificate courses that contained data protection and privacy modules.

The above results are further backed up by some an academic respondent who indicted that;

"Makerere University. In the schools of computing and Information technology teaches modules in program of BRAM AND BLIS" (Response from the ICT Industry Professional)

It is worth noting that; the six institutions listed in table 3 primarily focus on raising awareness about data protection and privacy rather than offering certification training in these areas. This underscores the pressing need for the establishment of a dedicated data protection and privacy certification center within the country.

c) Knowledge and Skills desired to be possessed by data protection personnel

Respondents provided diverse responses to the question on what knowledge and skills are desired by data protection personnel since there was no limit to the number of suggestions. However, the majority **33%** emphasized the importance of Legal and Regulatory Knowledge, citing the need to understand data protection laws and regulations and interpret legal requirements accurately, **22%** of respondents highlighted the significance of Technical

Expertise. Furthermore, **19%** of respondents emphasized the importance of Risk Management and Assessment indicating a recognition of the importance of identifying and mitigating potential threats to data security, **16%** of respondents emphasized the value of general skills and knowledge, including analytical and problem-solving skills, ethical conduct, and understanding of data security principles. Lastly, only **10%** of respondents indicated a preference for communication and interpersonal skills highlighting the need for effective communication with different stakeholders regarding data privacy matters. Results are further demonstrated in the figure 6 below;

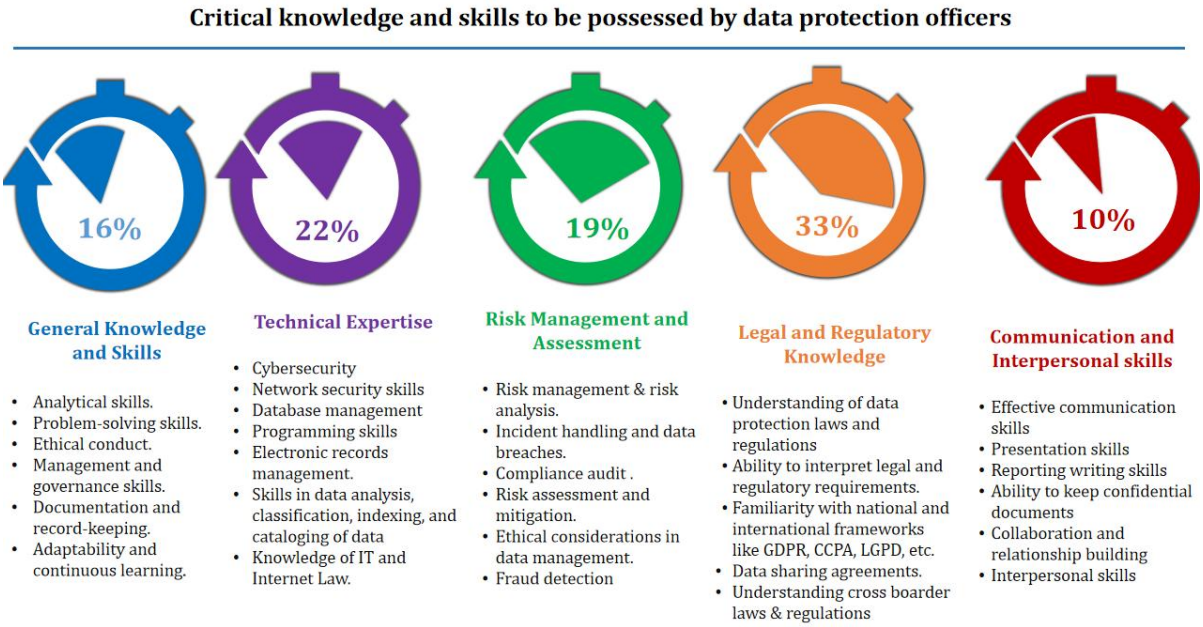

Figure 7: Critical knowledge and skills to be possessed by data protection personnel

In summary, respondents highlighted the critical importance of possessing Knowledge on the Legal and regulatory framework, risk management and assessment skills and IT Technical expertise emphasizing the need for Data Protection Personnel to adeptly identify and mitigate potential threats to data security. Regarding the preferred background education and professions for Data Protection Personnel, the majority of participants recommended backgrounds in Information Technology (IT), Audit, and Legal disciplines.

4.4 Stakeholder opinions on the establishment and Operationalization of the Data Protection and Privacy Training Center

Gauging stakeholder perspectives is crucial in understanding the feasibility and effectiveness of establishing and operationalizing a Data Protection and Privacy Training Center. In this section, we delve into the diverse perspectives of stakeholders regarding the establishment and operationalization of a dedicated center aimed at training and certifying individuals in data protection and privacy in terms of suggested topics to be covered, the proposed accreditation framework, Proposed Delivery Methods and the Target Audience for the data protection and privacy training course.

a) Suggested topics for the curriculum

The suggested topics for inclusion in the data protection curriculum were selected by a subset of the total respondents, with multiple options available for selection. Among these topics, ***"Data Protection Law"*** emerged as the most popular choice, with a significant 75 respondents selecting it. Following closely, ***"Fundamentals of Data Privacy"*** gained considerable attention, with 70 respondents indicating its importance. ***"Data Life Cycle Management"*** with 66 respondents suggesting for its inclusion in the curriculum. ***Cyber Security fundamental***s and ***Risk Management*** were highlighted by 50 and 47 respondents, respectively, underscoring their significance in comprehensive data protection education. Additionally, technical knowledge of IT systems, professional ethical considerations and integrity were considered essential by 29 and 28 respondents, respectively, "***Emerging Technologies***" and "***Electronic Records Management***" were also recognized as pertinent topics by 27 respondents each. Lastly, "Data ***Breach Response and Incident Management***" and "***International Data Protection Frameworks***" rounded, with 26 and 22 respondents selecting them, respectively. This diverse array of topics reflects the comprehensive approach necessary to equip individuals with the knowledge and skills required to navigate the evolving landscape of data protection effectively.

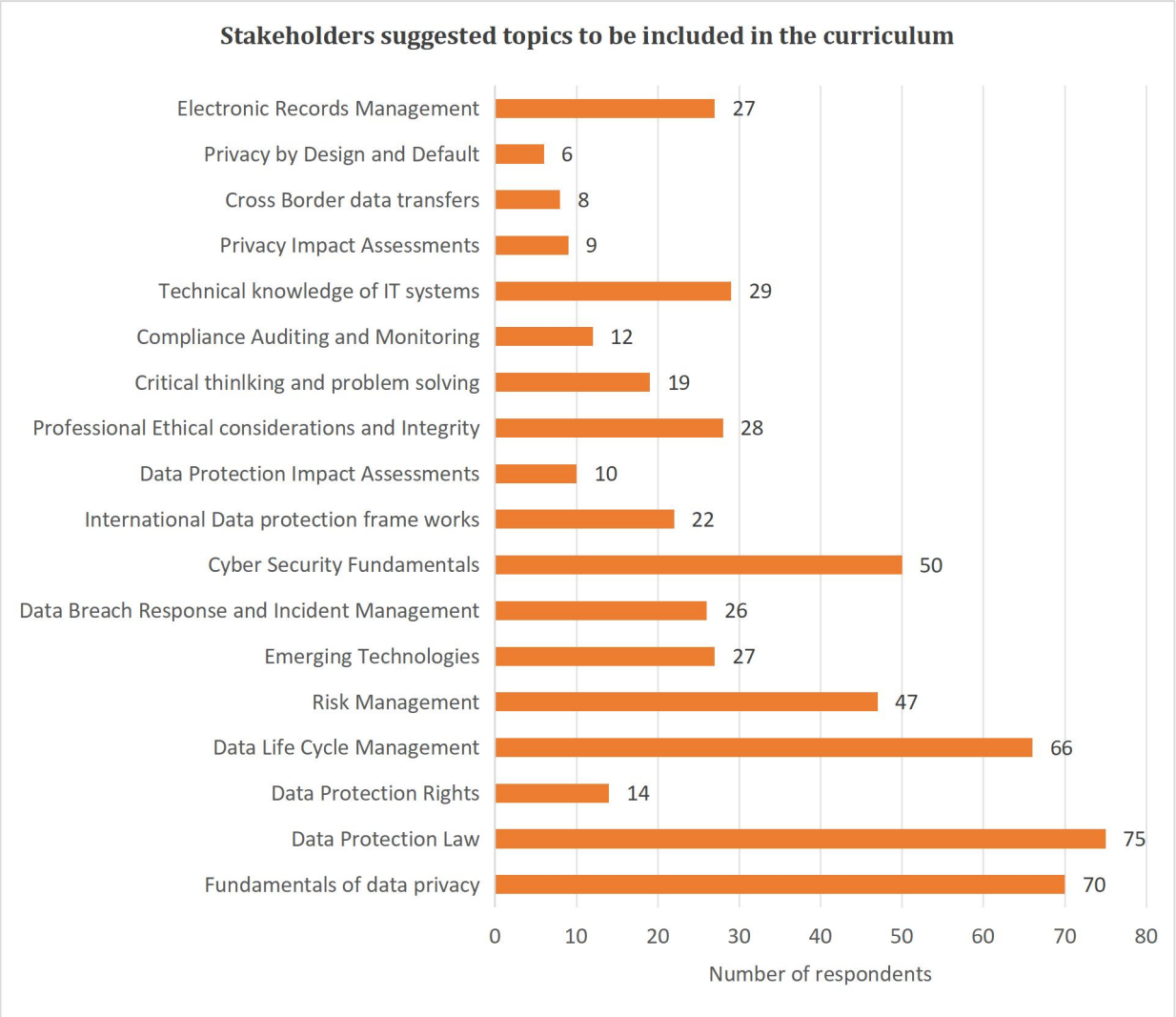

Figure 8: Suggested topics for the Data Protection and privacy Curriculum

Where for this context we interpret: Data Life Cycle Management to comprise of the different forms of data processing, Data Collection, Data Entry, Data Cleaning, Data Transformation, Data Storage, Data Analysis, Data Visualization, Data Interpretation, Data Reporting, Data Security)

b) Suggested topics based on the different industries

Suggested topics for inclusion in the data protection curriculum across various industries, with the number of respondents who selected each topic provided for each group. "Fundamentals of Data Privacy" emerged as a commonly recognized topic among several groups, with the legal fraternity and CSOs/NGOs. Similarly, "Data Protection Law" was mentioned frequently across most groups, indicating a widespread recognition of the importance of legal frameworks in data protection. Other notable topics include "Data Life Cycle Management," "Cyber Security Fundamentals," and "Risk Management," which received varying number of responses for support across different stakeholder groups. Interestingly, certain topics such as "Data Protection Rights" and "Privacy by Design and Default" received the least responses from respondents overall. Overall, the results highlight the diverse perspectives and priorities among stakeholders regarding the key components of a comprehensive data protection curriculum as illustrated in the figure below;

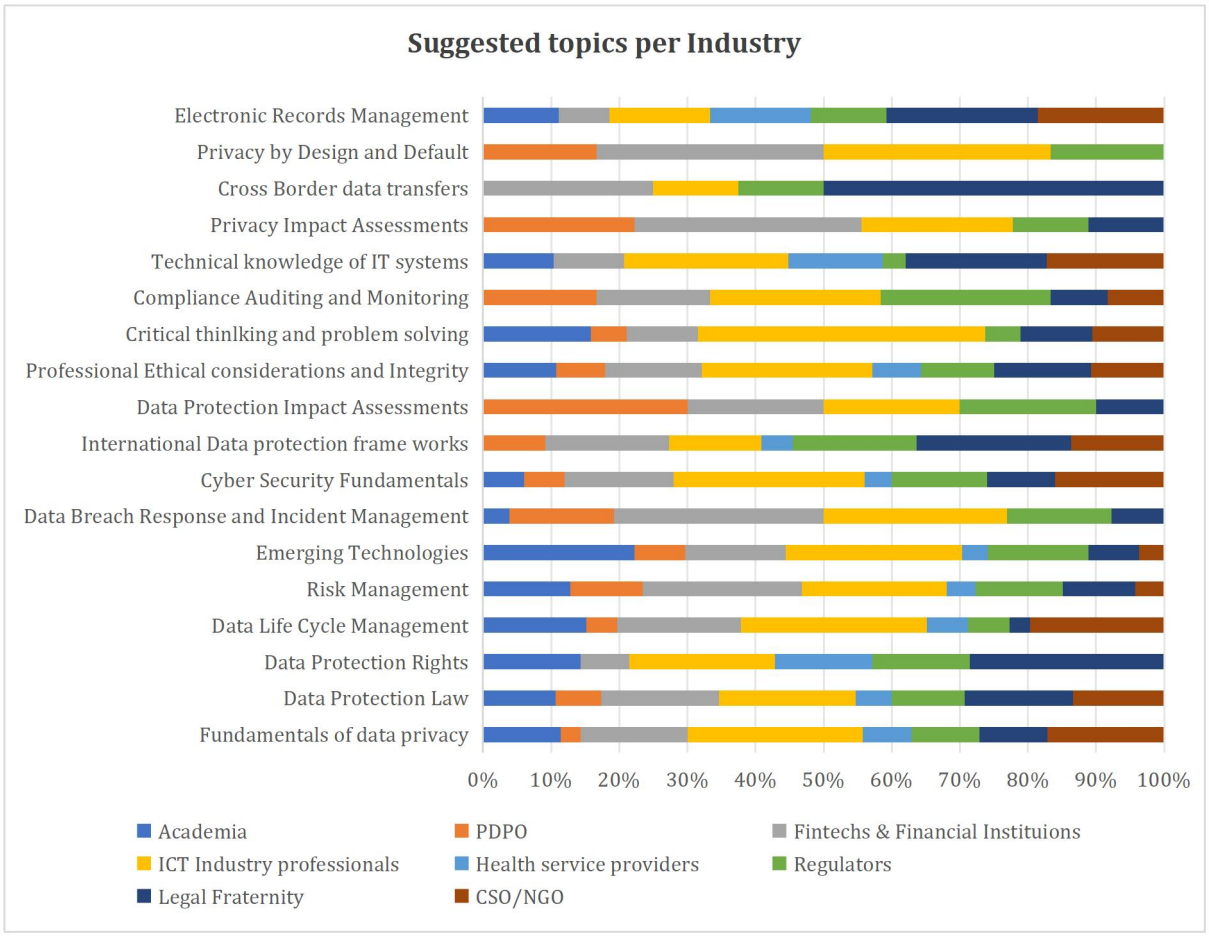

Figure 9: Suggested topics for the Data Protection and privacy Curriculum

These results are further backed up by some respondents who indicated that;

"I would suggest a topic on how to Communicate whereby people do not know when, what and how to communicate. and also a topic on critical thinking whereby people need to think about what they are doing, reading and etc" (Says a respondent from an NGO)
"Data and the right to privacy; rationale- this helps data handlers to understand the centrality of the right to privacy as a mechanism for full realization of the same right in data management." (Respondent from the legal fraternity)

"Legal Framework: Understanding the relevant data protection laws and regulations, such as GDPR, CCPA, or other applicable regulations depending on the jurisdiction. This provides a foundation for understanding compliance requirements and legal obligations.

Data Protection Principles: Explaining the core principles of data protection, including lawful processing, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality. Understanding these principles helps individuals ensure that personal data is processed in a compliant and ethical manner.

Data Security: Covering principles and techniques for ensuring the security of personal data, including measures to prevent unauthorized access, data breaches, and cyber attacks. This includes topics such as encryption, access controls, authentication mechanisms, and incident response procedures". (As indicated by a respondent from one Fintech)

In conclusion, the analysis revealed a clear hierarchy of topics based on respondent preferences, with ***Cyber Security, Legal and Regulatory Frameworks, Principles/ Fundamentals of Data Protection and professional Ethical considerations*** occupying the top positions. These topics should be given high priority in curriculum development, as they align with the predominant concerns and interests of the respondents. Additionally, attention should be paid to Understanding Data Processing Forms and Risk Management, Assessment, and Mitigation, which are deemed important by a significant portion of respondents. The curriculum should be structured to provide a well-rounded education, encompassing legal, ethical, and technical aspects while addressing the evolving challenges presented by emerging technologies.

c) Proposed Accreditation Framework

In establishing a robust and credible educational program in Data Protection and Privacy, the development and adherence to a comprehensive Accreditation Framework are paramount. The Accreditation Framework serves as the foundational structure that ensures the course meets rigorous standards, aligns with industry best practices, and is recognized for its quality and relevance.

It is significant that the findings from the consultations bring to light a noticeable lack of awareness regarding the accreditation framework among the respondents. Out of the total number 94 respondents, a third of them accounting for 66% of the respondents indicated that PDPO should work with entities such as; National Information Technology Authority (NITA-U) accounting for 14.9%, International Certification bodies and PDPO accounting for 12.8% each followed by National Council for Higher Education accounting for 8.5% of the respondents.

On the other hand, opinions were more divided regarding accreditation by higher education institutions (universities), the Uganda Business and Technical Examinations Board (UBTEB), and the Directorate of Industrial Training (DIT), with lower percentages of respondents accounting for 7.4%, 6.4% and 3.2% respectively supporting their accreditation roles. Notably, a

considerable portion of respondents, constituting 34%, expressed no opinion, indicating a degree of uncertainty or lack of preference regarding accreditation bodies for data protection training programs (Refer to figure 10).

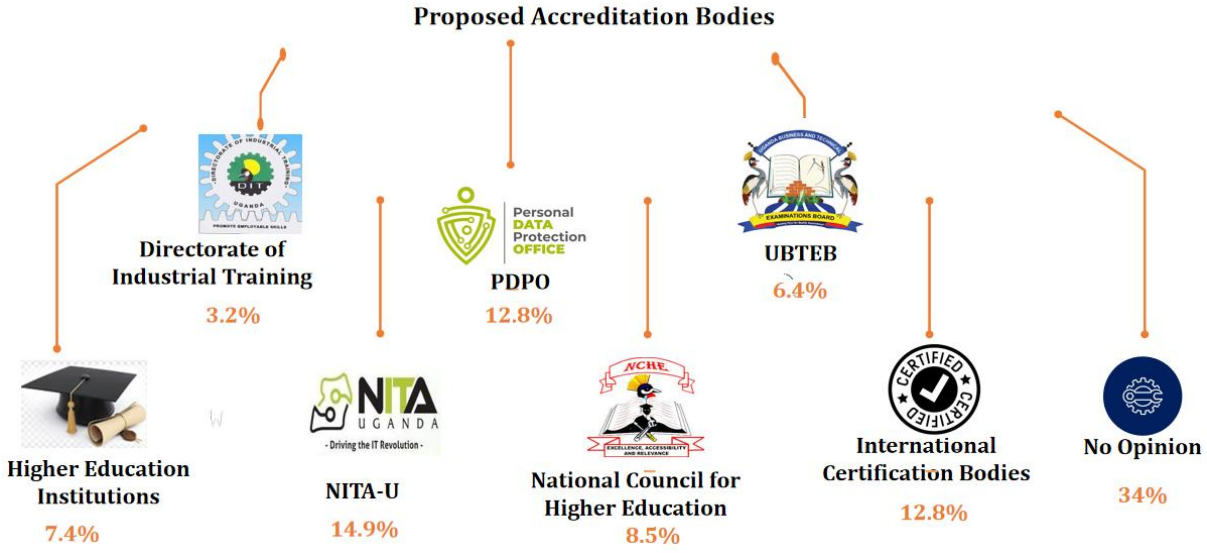

Figure 10: Proposed Accreditation Body

This diversity of opinions highlights the complexity of accreditation considerations and suggests the need for further dialogue and consensus-building among stakeholders in the data protection.

A key respondent from a telecommunication regulatory body indicated that;

"An ideal accreditation framework for data protection and privacy programs should ensure individuals possess a well-rounded understanding of the field and meet established standards. This framework should acknowledge global and local regulations, adopt a multi-disciplinary approach, include continuous learning requirements, emphasize practical application and case studies, align the curriculum with industry needs and trends, integrate ethical considerations, establish rigorous assessment mechanisms, designate reputable accreditation bodies, seek international recognition, be flexible to technological advancements, involve key stakeholders, ensure transparency and accessibility, promote quality assurance and continuous improvement, promote diversity and inclusion, and foster industry collaboration."

Other Respondents indicated that;

"Through a National Accreditation programme that aligns with leading industry standards and existing professional certifications. The accreditation should not seek to replace existing international certifications."

" Accreditation should be granted by a reputable and independent organization with expertise in data protection and privacy."

"Accredited programs should be delivered by instructors with demonstrable expertise in data protection and privacy law, regulations, and best practices."

Instructors should possess relevant academic qualifications and practical experience in the field.

d) Proposed Delivery Methods

The responses on proposed Delivery methods presents the percentages of respondents' preferences for online self-paced study with 25% of the respondents followed by instructor-led virtual classes 21% of the respondents. Blended learning, which combines online and in-person instruction, also received substantial responses, with 20% while Boot camps, characterized by intensive and immersive training sessions, were favored by 16% of respondents. Physical classes, were less favored compared to virtual and online options with 10% of respondents. Notably, 8% of respondents expressed no opinion. This diversity of preferences underscores the importance of offering a variety of training modalities to cater to the diverse learning needs and preferences of individuals seeking data protection training.

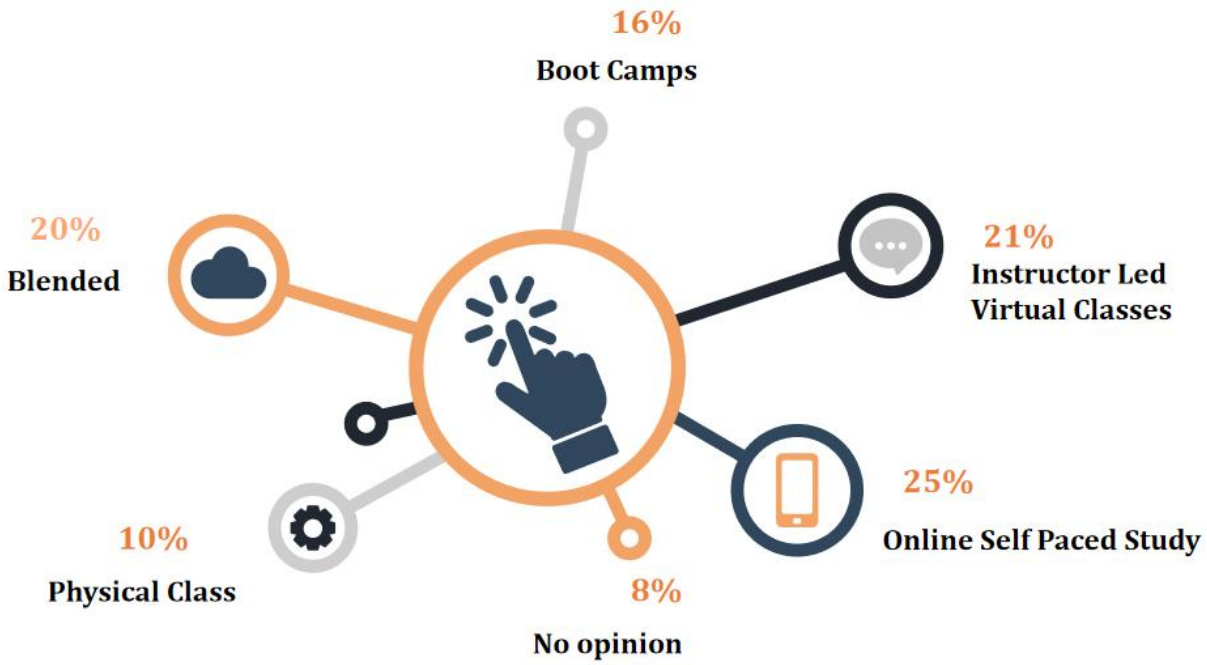

Figure 11: Proposed curriculum delivery methods

e) Target Audience for the data protection and privacy training course

Recognizing that individuals and professionals from various fields play unique roles in ensuring the secure handling of personal data, the respondents were asked to propose target beneficiaries for the course and the responses were categorized into distinct groups based on their responsibilities and expertise as detailed in the table below;

Category	%age	Target Audience
Core Implementers and Enforcers	63%	Data Protection Officers (DPOs)
		IT Professionals (System Administrators, Network Administrators, Cybersecurity Experts)
		Data Handlers, Processors and Researchers
		Compliance Officers and Auditors
Legal and Compliance Experts	22%	Legal Professionals
		Business and Compliance Professionals
		Government Officials

		Executives and Decision-Makers
Industry-Specific Professionals	9%	Healthcare Professionals
		Educational Institution Staff
		Nonprofit Organizations Staff
		Start-up Entrepreneurs
Workforce Awareness	6%	Human Resources Personnel
		General Workforce Awareness (All Employees)
		Consultants and Advisors

Table 3: Target Audience for the data protection and privacy training course

f) Suggestions on the Operationalization of the Data Protection Training Center

We engaged with the respondents to gather perceptions into the strategic aspects of operationalizing the Data Protection Training Center and this was aimed at harnessing collective wisdom and expertise. Some of the suggestions from the respondents are listed in the table below;

No.	Suggestion	Category
1.	a) Established as an Affiliate of a recognized industrial certification body. b) Established under NCHE Act and operated by PDPO. c) Established under a collaborative framework with universities d) Established through an instrument of parliament e) Established through a statutory Instrument by the minister.	Training center Establishment
2.	a) Use key industry players and professionals in the delivery of the courses. b) Duration of the program should be between 1week to 12weeks. c) It should also act as a licensing body for Data Protection Officers (DPO). d) The course itself should be introduced to the existing universities or institutions of higher learning. e) The course should be practical with relevant case studies.	Curriculum Delivery
3.	a) The course should be embedded in some of the diploma and bachelor programs b) The course should be mandatory for designated DPOs. c) The programme should be marketed using mass media and online channels d) The programme should seek international accreditation to increase it market appeal	Program marketing and promotion

Table 4: Suggestions on the Operationalization of the Data Protection Training Center

5. Conclusions and Recommendations

This section serves to digest the overarching conclusions derived from the research findings and to propose actionable recommendations aimed at addressing identified gaps and enhancing the effectiveness of data protection education initiatives in the country. Through an examination of awareness levels, desired knowledge and skills, suggested topics for curriculum development, and considerations for accreditation frameworks, this section endeavors to provide a comprehensive road map for the curriculum for data protection and privacy training for PDPO.

5.1 Conclusions

a) Bench marking

Based on the findings from the desk review and bench marking, it is clear that there is a diverse range of options available, each with its own focus and requirements. To inform the development of DPO training curriculum in Uganda, it is recommended to tailor the curriculum to address specific local needs and challenges. This could include incorporating modules on the local data protection laws and regulations, as well as practical case studies relevant to Ugandan organizations. Additionally, considering the varying levels of experience and education required for different courses, offering a range of certification levels could help accommodate individuals at different stages of their careers. Collaborating with international accreditation bodies such as ISACA, PECB, and IAPP could also enhance the credibility and recognition of the training courses in Uganda. It is recommended that the courses emphasize not only legal and regulatory aspects but also the practical implementation of data protection principles. Moreover, the training should be accessible and affordable, potentially leveraging online platforms to reach a wider audience. Ongoing monitoring and evaluation should be conducted to ensure the courses remain relevant and impactful in Uganda's evolving data protection landscape.

b) Respondent Demographics

In this study, 94 respondents participated, with a majority being males (68) compared to females (26). Among the respondent categories, CSO/NGOs, ICT/Cyber Security Officials, and legal professionals were the most represented, while PDPO, financial institutions, and utility and telecommunication industries had the lowest representation. Interestingly, the majority of respondents (71.3%) held certificates, with Cyber Security and Data Protection and Privacy certificates being notable. However, a significant portion (56.1%) possessed other certificates such as ACCA and CPA.

c) Awareness of National and International Legal and Regulatory Frameworks

The study revealed varying levels of awareness among respondents regarding national data protection legal and regulatory frameworks. While 39.4% were aware, the majority (60.6%) were not. Notably, awareness levels varied across sectors, with ICT industry professionals, fintechs & financial institutions, and CSOs/NGOs showing the highest awareness. The Data Protection and Privacy Act, 2019, was the most recognized framework (26.1%), followed by the Computer Misuse Act, 2011. Regarding international data protection legal and regulatory frameworks, only 29.8% of respondents indicated awareness. Among them, the General Data Protection Regulation

(GDPR) stood out as the most recognized framework (53.6%), followed by the ISO 27000 Series. Other frameworks mentioned included NIST Cyber Security Framework, COBIT 2019, and various national laws such as the California Consumer Privacy Act. These findings highlight the need for enhanced awareness initiatives to ensure stakeholders are informed about National and global data protection standards and regulations, particularly given the increasingly interconnected nature of data management practices across borders.

d) Awareness of data protection training providers in Uganda

In the stakeholder consultations, it became evident that there was a significant lack of awareness regarding data protection and privacy training providers in Uganda. A majority of the respondents (65 out of 94) indicated that they were not aware of any institutions offering such training services, while only 29 respondents claimed awareness. Interestingly, awareness levels varied across industries, with ICT industry professionals exhibiting the highest level of awareness, followed by respondents from regulatory bodies, fintech & financial institutions, academia, and PDPO staff. Conversely, CSO/NGO respondents, health providers, and the legal fraternity demonstrated the lowest levels of awareness. Additionally, specific institutions such as the ISACA Kampala Chapter, WOUGNET, Unwanted Witness, PDPO, and NITA-U were noted for offering awareness workshops focused on data protection and privacy. Furthermore, some stakeholders highlighted institutions like Makerere University and Uganda Institute of Information and Communications Technology (UICT), which offer courses encompassing data management practices.

e) Desired Knowledge and skills to be possessed by Data Protection Personnel

Regarding the desired knowledge and skills for data protection personnel, respondents provided diverse responses, emphasizing the importance of legal and regulatory knowledge, technical expertise, risk management, general skills, and communication abilities. This underscores the multifaceted nature of data protection roles and the need for a comprehensive skill set among professionals in this field.

f) Proposed Accreditation Framework

In establishing a robust educational program in Data Protection and Privacy, the development and adherence to a comprehensive Accreditation Framework are crucial. However, the findings revealed a noticeable lack of awareness regarding accreditation frameworks among respondents. While some entities such as NITA-U, international certification bodies, and PDPO were recognized for their potential role in accreditation, opinions were divided regarding accreditation by higher education institutions and other regulatory bodies. A significant portion of respondents expressed no opinion, highlighting the complexity of accreditation considerations and the need for further dialogue and consensus-building among stakeholders in the data protection ecosystem.

5.2 Recommendations

In response to the findings derived from comprehensive stakeholder consultations and bench marking exercises, a set of strategic recommendations has been formulated to guide the development of a robust curriculum for data protection and privacy training under the Personal Data Protection Office (PDPO).

These recommendations encompass diverse aspects aimed at fostering an adaptive, industry-relevant, and globally competitive educational program. The section detail specific issues addressed, corresponding actions proposed, priority levels, and the designated bodies responsible for the implementation of these recommendations.

Issue	**Action**	**Priority**	**Person Responsible**
Limited awareness of laws, regulations and policies in regards to data protection and privacy	Conduct awareness campaigns and workshops to educate stakeholders on the different laws, policies and frameworks.	High	PDPO
Identified key topics for the curriculum are Cyber Security, Legal and Regulatory Frameworks, and Data Processing Forms	Develop a curriculum that prioritizes these key topics, ensuring a balanced coverage of legal, ethical, and technical aspects.	High	Curriculum Development Team
Lack of clarity on the accreditation bodies and process	Collaborate with recognized accreditation bodies during the delivery like NCHE, NITA-U, and DIT, ensuring adherence to regulatory standards.	High	PDPO
Preference for a blended curriculum delivery approach	Implement a curriculum delivery strategy that combines both physical and online methods to cater to diverse learning preferences.	High	Curriculum Development Team
Target audience diversity in roles and responsibilities	Customize the curriculum to meet the needs of diverse target audiences, including Core Implementers, Legal Experts, Industry Professionals, and Workforce.	High	Curriculum Development Team
Recommendations for operationalizing the Data Protection	Establish the center in collaboration with recognized institutions, ensuring inclusivity,	High	PDPO, NITA-U

Training Center	affordability, and practical relevance.		
Continuous Stakeholder Consultation	Establish regular channels for feedback and consultation with stakeholders.	Medium	PDPO
Regular Curriculum Review and Update	Implement a periodic review process to ensure the curriculum stays current with evolving technologies and regulatory changes.	Medium	Curriculum Development Team , PDPO
Internship and Practical Experience Integration	Collaborate with industry partners to incorporate internships or practical experiences into the curriculum.	Medium	PDPO
Cross-Disciplinary Collaboration	Encourage collaboration between different academic disciplines to provide a holistic approach to data protection and Privacy.	Medium	PDPO, NITA-U, MoES
Global Best Practices Incorporation	Integrate global best practices and case studies into the curriculum to provide a broader perspective.	High	Curriculum Development Team
Certification Exam Preparation	Develop resources and modules that help students prepare for relevant certification exams.	Medium	Curriculum Development Team
Research and Development Component	Introduce a research and development component to encourage innovation and contribute to the field's knowledge base.	Low	PDPO, NITA-U
Flexible Learning Paths	Allow for flexible learning paths to accommodate the varying levels of expertise and prior knowledge among participants.	High	Curriculum Development Team

6. Proposed Courses for the Curriculum

No.	Course	Knowledge Areas	Justification	Course Load
1.	Data protection regulatory environment and professional ethics **Or** Data Protection Legal and Regulatory Frameworks	Fundamentals of data privacy (The History of Privacy)	Data protection officers need a comprehensive understanding of the historical evolution of privacy to grasp the context and evolution of privacy laws and principles as evidenced in international certifications like CIPP and CIPM offered by IAPP. This knowledge provides a foundation for informed decision-making and compliance strategies within the contemporary landscape of data protection.	3hrs
		Data Protection and Privacy Policy, Legal and Regulatory Framework	This course is meticulously crafted to empower Data Protection Officers (DPOs) by enhancing their knowledge and skills necessary for interpretation and application of laws within the context of a diverse, multicultural society. The course covers laws with the national, regional and international context like SADC Model Law on Data Protection (2010), ECOWAS Supplementary Act (2010), EAC Framework for Cyberlaws (2008).[18] Emphasizing practical application, the course aligns with the Certified Information Privacy Professional (CIPP), accredited to ANSI/ISO Standard 17024:2012, ensuring a robust foundation in privacy laws. Additionally, it adheres to the design principles of the Certified in Data Protection (CDP), a program by the Identity Management Institute that delves into international security standards and data protection laws.	12hrs

[18] https://www.itu.int/en/ITU-D/Capacity-Building/Documents/IG_workshop_August2018/Presentations/Session%207_Verengai%20Mabika.pdf

		Ethical Principles, National Values and multicultural awareness	Codes of ethics are relevant in supporting competent multicultural counselling. [19] the course uniquely focuses on fostering the moral character and values of participants, recognizing the critical role these qualities play in the ethical execution of their duties. The course prioritizes ethical education, aiming to equip participants with the awareness and discernment to make ethically sound decisions, Furthermore, the course will incorporate assessment methods and feedback mechanisms designed to evaluate participants' ethical decision-making skills and ethical awareness throughout the program evaluate their moral character and values. This shall ensure that data protection officers understand the diverse cultural contexts in which they operate, adhere to ethical standards in their practices, and respect national values, fostering trust and compliance within the communities they serve.	3hrs
2.	Data Privacy Governance & Management	Emerging technological trends and data protection -	The module shall incorporate emerging technological trends to equip professionals with the knowledge and skills to navigate the complexities they bring, including understanding the implications of AI algorithms on data privacy, managing data collected from IoT devices, handling massive volumes of data in Big Data environments, ensuring security and privacy in Cloud Computing, and implementing data protection measures throughout these processes. This will focus on the technical, business, and regulatory aspects of IoT, Big Data, and AI, covering IoT technologies, standards, architectures, and policies; Big Data overview, ecosystem, technologies, and challenges; and AI applications in ICT/telecom, including Machine Learning for 5G, as well as business aspects, policies, and Internet governance related to these	3hrs

[19] https://files.eric.ed.gov/fulltext/EJ622696.pdf

			technologies.[20]	
		Privacy Governance (Governance, Management & Risk Management)	This is intended to cover the development and implementation of privacy policies and procedures, as well as the establishment of a privacy governance framework that aligns with applicable laws and regulations. Having a proper governance structure to oversee the efforts in organizations and to be aware of, and be able to mitigate, the risk involved will be an important aspect of the DPO's work.[21]	6hrs
		Privacy Architecture (privacy by design and default)	This shall help DPOs learn how to implement privacy by design in the organization or product, apply privacy in system design consistently, verify adherence to privacy by design, and assist with DPIAs and other GDPR requirements.[22]	6hrs
		Data Lifecycle (Records Management, Retention and Disposal)	This shall empower Data Protection Officers (DPOs) to establish a comprehensive records management system by defining accountability and responsibilities, implementing internationally accepted best practices, and governing the capture, classification, access, and management of records throughout their lifecycle. It will also encourage the automation and digitalization of business processes to align with strategic goals, enhance efficiency, and[23] minimize paper usage.	10hrs
		Data protection and privacy awareness and training program	This shall make sure DPOs receive appropriate training about the privacy program, including what its goals are, what it requires people to do and what responsibilities they have. The training must be relevant, accurate and up	4hrs

[20] https://academy.itu.int/training-courses/full-catalogue/key-technologies-and-governance-internet-things-big-data-and-artificial-intelligence
[21] https://ace.nus.edu.sg/course/data-protection-governance-risk-management/
[22] https://www.dp-institute.eu/en/courses/privacy-by-design/
[23] https://www.bstdb.org/Records_Management_Policy.pdf

			to date. Training and awareness is key to actually putting into practice data protection policies and procedures.[24] This will further equip them with skills on how to deliver similar trainings to other stakeholders.	
		Personal data security breaches and complaints Management	DPOs shall be able to have consistent and effective control arrangements to protect personal data they hold. They will be able to clearly define what entails data breach, and the course of action to be followed by all staff in the event of a real or potential data protection breach.	6hrs
	Cyber Security Fundamentals	Information Security Fundamentals and Basic Security tools	This course shall show DPOs the basics to set up, manage and measure threat and vulnerability processes. It will demonstrate how security events are identified and addressed. The module is further aligned to international certifications such as Privacy Trust, Certified Ethical Hacker, Certified Hacking Forensic Investigator, Certified Information Privacy Auditor, Certified Information Systems Auditor, Certified Information Security Manager, and Certified Information Systems Security Professional.	10hrs
		Data Protection and Privacy Audits	This shall enable DPOs evaluate the current state of privacy and data protection actions in the organization. The cover shall train DPOs to offer audit services to measure compliance, identify gaps and offer recommendations.[25]	10hrs
		Cyber Security Maturity Assessment	The purpose of this course is to train DPOs on how to evaluate an organization's cyber security capabilities and readiness. The DPO shall be able to provide a comprehensive view of an organization's overall cyber security posture including policies, procedures and technologies.[26]	10hrs

[24] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/accountability-framework/training-and-awareness/
[25] https://privaon.com/services/data-protection-audits/
[26] https://www.linkedin.com/pulse/cybersecurity-maturity-assessment-why-its-important-kuppannagari/

		Cross-border data transfer mechanisms	This course shall learn about Binding Corporate Rules (BCR), which are internal rules for data transfers within multinational organization designed to allow transfer personal data internationally within the same corporate group. DPOs shall know to choose the right method, implement safeguards, keep records of data transfers including data types and reviewing the processes.[27]	3hrs
		Data Protection Impact Assessments	This is designed for DPOs to learn how to plan and conduct a data protection impact assessment. DPOs will acquire a comprehensive understanding of how to minimize potential risks and vulnerabilities of data protection.[28]	4hrs

[27] https://www.dpocentre.com/binding-corporate-rules-an-improvement-on-cross-border-data-transfer/
[28] https://data-privacy-office.eu/services/data-protection-impact-assessment/

7. Annexes

Annex I: List of Documents Reviewed

1. The Data Protection and Privacy Act, 2019
1. The DPO training needs assessment report by the Personal Data Protection Office 2022
2. National IT Survey Report, 2022
3. PDPO Strategic plan
4. The Computer Misuse (Amended) Act, 2022
5. Data Protection and Privacy regulations 2021
6. Data Protection and Privacy legal frameworks for Uganda
7. The AU Data Policy Framework
8. Uganda Cyber Security Policy Legal and Regulatory instruments
9. ISACA Certification guide
10. International association of privacy practitioner's certification guidelines
11. Access to Information Act, 2005

Annex II: Data Collection Tools

KEY INDUSTRY PRACTITIONERS KII TOOL FOR THE DESIGN AND DEVELOPMENT OF CURRICULUM FOR THE PERSONAL DATA PROTECTION OFFICE.

The Personal Data Protection Office (PDPO) through National Information Technology Authority – Uganda (NITA-U) is establishing a Data Protection Academy as a mechanism of enhancing compliance to the data protection and privacy act 2019. This initiative will involve the development of training programs to address knowledge and skill gaps of designated data protection officers as identified in the needs assessment report of 2022.

Therefore, the purpose of this tool is to seek stakeholders input in the design of the proposed academy and its associated programs.

Disclaimer: In line with the Data Protection and Privacy Act,2019, the information provided shall be strictly used for purposes of informing the nature of courses the academy can run, means of course delivery, course load and ideal course certification pathways. Any personal identifiable information shall be held with utmost confidentiality and shall only be used for verification of facts by the Consultant, and at the end of the assignment, the personal data shall be destroyed.

Consent form signed : ……Date : ……Location: ……

A. Personal and Professional Information:

1) Name
2) Education background
3) Position and department
4) Organization
5) Email address
6) Have you taken any professional certification: Yes/No
7) If yes, please specify
    a. Describe your experience in terms of training requirements and duration, mode of delivery, quality and convenience.

B. Awareness of the policy legal and regulatory environment

1) Are you aware of any National data protection legal and regulatory frameworks? If yes, please mention them
    a. Briefly share how these legal and regulatory frameworks guide your work and how you have applied them?
2) Are you aware of any international data protection legal and regulatory frameworks? If yes, please mention them
3) Are you involved in data processing in any form? Yes/No. If yes, describe your role.
4) Are you aware of the roles of a Data Protection Officer? If yes, please mention them

C. Key capacity building areas for data protection officers

1) In your opinion, what critical knowledge and skills should be possessed by data protection officers?
2) Mention some of the institutions providing data protection and privacy training programmes in Uganda. (provide more details on the nature of programs, training delivery, accreditations/certification)

D. Suggestions on data protection academy operations

i) Which topics would you recommend to be included in a curriculum for data protection and privacy and why?
ii) Share your thoughts on the ideal accreditation framework for such programmes
iii) How should these trainings be delivered: Online, virtual, blended?

iv) Kindly share any thoughts on how the data protection academy should be established and operationalized?

PDPO STAFF KII TOOL FOR THE DESIGN AND DEVELOPMENT OF CURRICULUM FOR A DATA PROTECTION ACADEMY UNDER THE PERSONAL DATA PROTECTION OFFICE.

The Personal Data Protection Office (PDPO) through National Information Technology Authority – Uganda (NITA-U) is establishing a Data Protection Academy as a mechanism of enhancing compliance to the data protection and privacy act 2019. This initiative will involve the development of training programs to address knowledge and skill gaps of designated data protection officers as identified in the needs assessment report of 2022.

Therefore, the purpose of this tool is to seek stakeholders' input in the design of the proposed academy and its associated programs.

Disclaimer: In line with the Data Protection and Privacy Act,2019, the information provided shall be strictly used for purposes of informing the nature of courses the academy can run, means of course delivery, course load and ideal course certification pathways. Any personal identifiable information shall be held with utmost confidentiality and shall only be used for verification of facts by the Consultant, and at the end of the assignment, the personal data shall be destroyed.

Consent form signed : ……Date : ……Location: ……

A. Personal and Professional Information:

- Name
- Education background
- Position and department
- Role in data protection and privacy management
- Email address

B. Awareness of the policy legal and regulatory environment

i) Are you involved in data processing in any form?

ii) Are you aware of any international data protection legal and regulatory frameworks? If yes, please mention them

iii) Briefly share how these legal and regulatory frameworks guide your work

C. Key capacity building areas for data protection officers

i) In your opinion, what critical knowledge and skills should be posed by a data protection officer?

ii) Mention some of the institutions providing data protection and privacy training programmes in Uganda. (provide more details on the nature of programs, training delivery, accreditations/certification)

iii) What specific legal requirements should the curriculum address?

iv) What technology infrastructure is available to support the delivery of the curriculum? (e.g., learning management systems, online platforms)

D. Suggestions on data protection academy operations

i) Which topics would you recommend to be included in a curriculum for data protection and privacy?

ii) Share your thoughts on the ideal accreditation framework for such programmes

iii) How should these trainings be delivered: Online, virtual, blended?

iv) Kindly share any thoughts on how the data protection academy should be established and operationalized?

Annex III: List of Stakeholders Consulted

Organisation	Number
DFCU	1
Ntinda Medical Centre	1
MTN	1
National Water and Sewerage Cooperation (NWSC)	1
National Social Security Fund (NSSF)	1
AFRI FOODS	1
Centre for Multi lateral Affairs	1
Tenda Africa	1
Kabale University	2
Soroti University	1
Kayunga Hospital	1
African Renewal University	1
Gulu University	1
Uganda Institute of Information and Communication Technology (UICT)	2
African Field Epidemiology Networt	1
Huawei	1
Clinic Master	1
National Information Technology Authority Uganda (NITA-U)	5
UCC /UCUSAF	3
UNWANTED WITNESS	1
Uganda National Farmers Federation (UNFFE)	1
NUDIPU	1
Makerere University	5
Makerere University Business School (MUBS)	5
Nkumba University	5
MOUNTAINS OF THE MOON	1
ISACA	1
Personal Data Protection Office (PDPO)	5
FITSPA	10
Fleet Monitoring Systems Ltd	1
Case Hospital	1
CEHURD	2
IRA	1
ABSA Bank	1
UMEME	1
Centenary bank	1
UTCL	1
Radix Consulting	1

MAT ABACUS	1
Kyambogo University	1
RUFORUM	1
NARO	1
Mutabingwa & Co. Advocates	1
NCHE	1
Mugani & Nanteza Company Associates	1
UNFFE	1
Barungi Baingana & Co. Advocates	1
Uganda AIDS Commission	1
Post Bank	1
Ortus Advocates	1
Divine Dental Clinic	1
Ministry of Health	1
Sports Uganda	1
PWC	2
CISP	2
WOUGNET	2
NCHE	1
	94

Annex IV: Consultation Letter

Personal DATA Protection OFFICE

PDPO/DO/001-ADM

7th February 2024

.....

.....

.....

INTRODUCTION OF EIGHT TECH CONSULTS LTD

The Personal Data Protection Office (PDPO) with support from Financial Sector Deepening Uganda (FSDU) is undertaking a project for the design and development of curriculum for Data Protection and Privacy Training. The primary objective of this initiative is to bridge knowledge and skill gaps among designated Data Protection Officers and increase the number of Data Protection and Privacy trained personnel in Uganda.

To do the design and development of the curriculum, Financial Sector Deepening Uganda (FSD Uganda) has contracted Eight Tech Consults an ICT services and Management consultancy firm. The Eight Tech Consults team shall conduct explorative interviews and engage with selected stakeholders to inform the development of the curriculum.

The purpose of this letter, therefore, is to introduce to you Eight Tech Consults Ltd and request that you kindly provide them all the necessary support they need to accomplish this assignment.

For more information on this initiative you can contact Mr. Stephen Mugabe Manager Data Protection Affairs at the Personal Data Protection Office (PDPO), 0776 577213 stephen.mugabe@pdpo.go.ug, or Ms. Fiona Nyanzi Project Coordinator Eight Tech, +256 778 167775 fiona@8technologies.net

We look forward to your cooperation.

Yours Sincerely,

Alibateese

Stella Alibateese

NATIONAL PERSONAL DATA PROTECTION DIRECTOR

Personal Data Protection Office (PDPO)
Palm Courts, Plot 7A Rotary Avenue (Lugogo Bypass)
Office: +256 759 848 259
E-mail: info@pdpo.go.ug
website: www.pdpo.go.ug