



# TRAINING OF TRAINERS TO DELIVER THE DATA PROTECTION CURRICULUM FOR THE PERSONAL DATA PROTECTION OFFICE TRAINING CENTER.

19th November, 2025

**Prepared by:**

**Eight Tech Consults Limited**

Email: [info@8technologies.net](mailto:info@8technologies.net)

Website: [www.8technologies.net](http://www.8technologies.net)

**With Support From:**

**Financial Sector Deepening Uganda (FSD Uganda)**

Email: [info@fsduganda.org.ug](mailto:info@fsduganda.org.ug)

[www.fsduganda.or.ug](http://www.fsduganda.or.ug)





# Eight tech profile/back ground

1. In operation **since 2007**
2. Core competencies: **ICT & Mgt Consultancy(policy dev't, Curriculum development), cyber security and data protection, Content development and digitization, E-Learning, ICT Innovation development, system integration, mobile and web technologies, research & data science, human capacity development**, among others.  
Hence the tag line:

***People, Innovation, Technology and Services***

3. 8Tech has over 15 years of experience implementing related assignments
4. **Over 100 year combined expert** experience in developing strategies and master plans.





# Eight tech profile-our clients



International Organisations



National Organisations



# About the facilitator

## About Me

**Dr. Drake Patrick Mirembe**

**<https://drakemirembe.org/>**

## Areas of Expertise

- Information Systems Security & Cybersecurity
- Specialized in secure systems design, digital trust, and cyber risk management.
- ICT for Development (ICT4D)
- Expertise in e-Governance, e-Health, e-Agriculture, mobile computing, and web-based systems.
- Instructional Design & E-learning
- Data Protection & Privacy Governance
- Strategic ICT Planning & Management
- Experienced in designing and implementing ICT strategies across sectors.



## Work Experience

- Founder & Manager – Microsoft Innovation Center–Uganda; Makerere’s Centre for Innovations and Professional Skills Development.
- Senior Lecturer & Supervisor – Supervised 14 PhD, 40+ Master’s, and 50+ Bachelor’s students to completion.
- Consultant & Trainer – World Bank and others
- Delivered ICT and cybersecurity programs for government, academia, and industry.

## Others

- Publications – Over 80 peer-reviewed journal and conference papers.
- Innovation Champion – Established multiple ICT hubs and incubation centers in Uganda.
- Mentorship & Capacity Building – Passionate about developing local talent for Uganda’s digital transformation.





# Curriculum BackGround

1

The importance of safeguarding personal data and upholding privacy rights has become paramount. With the proliferation of data breaches and privacy concerns, organizations worldwide are recognizing the critical need to implement robust personal data protection measures to safe guard the privacy of data owners.

2

The training program aims to empower participants to become proficient practitioners in the fields of data protection and privacy, but more importantly enforce the compliance with the provisions of the Data Protection and Privacy Law.

3

It is designed for ***privacy professionals, data stewards, and cybersecurity practitioners***, the program enhances their capabilities and helps enforce compliance with data protection laws, contributing to a secure digital environment.





# Objectives

**01**

Equip participants with knowledge to understand and comply with relevant data protection laws and regulations enabling them to navigate legal complexities and mitigate risks associated with non-compliance.

**04**

Raise awareness among participants about the importance of privacy protection and ethical considerations in handling personal data empowering them to champion privacy rights within their organizations and communities.

**02**

Equip participants with the skills to identify, assess, and mitigate risks to data security and privacy fostering a proactive approach to protecting sensitive information and minimizing potential vulnerabilities.

**05**

Prepare participants to effectively respond to data breaches and privacy incidents by developing incident response plans, conducting breach assessments and implementing remediation measures to mitigate harm and restore trust.

**03**

Promote effective data governance practices including data classification, access control, and data lifecycle management to maintain the integrity, confidentiality, and availability of data assets.

**06**

Equip participants with knowledge and ability to develop and implement effective privacy governance frameworks





# Program Regulations

## 2.1 Entry Requirements

In order to partake this course, participants will not need any prior knowledge within data protection and regulatory. However prior knowledge within the areas of ICT, Law, Business Management can facilitate effective undertaking of the course.

## 2.2 Load and Duration

01

The program will have a total load of 13 modules

Undertaken at the different levels of beginners, intermediate and advanced

02

03

A total of 178 hours will be used as learning hours for all the modules

28 hours for examination

04

05

The hours are distributed across the modules based on the content to be taught.

A participant shall be required to have completed it within one (1) year or else they start afresh.

06



# Program Organisation

The program will be organized as described in the table below;

**Level 1: Beginner**

**Level 2: Intermediary**

**Level 3: Advanced**

| Status                                                                                 | Course name                                                          | Learning Hours (LH) | Assessment Hours (AH) |
|----------------------------------------------------------------------------------------|----------------------------------------------------------------------|---------------------|-----------------------|
| <b>Data Protection Regulatory Environment and Professional Ethics (Beginner Level)</b> |                                                                      |                     |                       |
| Mandatory                                                                              | Fundamentals of Data Privacy (The History of Privacy)                | 6                   | 1                     |
| Mandatory                                                                              | Data Protection and Privacy Policy, Legal and Regulatory Frameworks. | 24                  | 3                     |
| Mandatory                                                                              | Cross-border Data Transfer Mechanisms.                               | 3                   | 1                     |
| Mandatory                                                                              | Ethical Principles, National Values and Multicultural Awareness.     | 6                   | 1                     |
| Total                                                                                  |                                                                      | 39                  | 6                     |
| <b>Data Privacy Governance &amp; Management (Intermediate Level)</b>                   |                                                                      |                     |                       |
| Mandatory                                                                              | Emerging Technological Trends and Data Protection.                   | 12                  | 2                     |
| Mandatory                                                                              | Privacy Governance (Governance, Management & Risk Management)        | 16                  | 2                     |
| Mandatory                                                                              | Data Lifecycle (Records Management, Retention and Disposal)          | 18                  | 2                     |
| Mandatory                                                                              | Data Protection and Privacy Awareness and Training Programs.         | 13                  | 2                     |
| Mandatory                                                                              | Personal Data Security Breaches and Complaints Management.           | 18                  | 3                     |
| Total                                                                                  |                                                                      | 77                  | 11                    |
| <b>Cyber Security Fundamentals for Data Protection (Advanced Level)</b>                |                                                                      |                     |                       |
| Mandatory                                                                              | Information Security Fundamentals and Basic Security tools.          | 20                  | 3                     |
| Mandatory                                                                              | Data Protection and Privacy Audits.                                  | 15                  | 3                     |
| Mandatory                                                                              | Cyber Security Maturity Assessment.                                  | 18                  | 3                     |
| Mandatory                                                                              | Data Protection Impact Assessments.                                  | 9                   | 2                     |
| Total                                                                                  |                                                                      | 62                  | 11                    |
| Grand Total                                                                            |                                                                      | 178                 | 28                    |



# Assessment, Grading and Certification

This training program encompasses three key courses.

01

Assessment for the program will be undertaken at two levels; **Continuous assessment shall cover 40% , examination 60% of the total marks.**

02

Any participant who achieves 60% and above of the total marks will have passed the module. Any participant who achieves more than 60% on average in all modules for a specific level shall be issued a certificate.

03

The participant will be considered to have completed the course and all the three certificates are issued to them.





# M1. Data Protection, Regulatory Environment and Professional Ethics

The course module on Data Protection Regulatory Environment and Professional Ethics delves into the complexities of data protection laws, regulations and ethical considerations guiding responsible data handling practices. Participants will gain insights on four Topics

**01**

## Fundamentals of Data Privacy (The History of Privacy)



### Detailing;

1. Introduction to Privacy: Definitions and Concepts
2. Historical Foundations of Privacy
3. Emergence of Legal Frameworks
4. Case Studies and Reflections

**03**

## Cross-border Data Transfer Mechanisms



### Detailing;

1. Understanding Cross-Border Data Transfer (1hrs)
2. Standard Contractual Clauses (SCCs), Contractual Safeguards and Binding Corporate Rules (BCRs) (2hrs)

**02**

## Data Protection and Privacy Policy, Legal and Regulatory Frameworks



### Detailing;

1. Understanding Uganda's Data Protection Legal and Regulatory Framework
2. Overview of Trans-Border Data Flow Regulation
3. Regional Instruments - International Instruments
4. Issues and Analysis

**04**

## Ethical Principles, National Values and Multicultural Awareness



### Detailing;

1. Ethical Principles in Data Protection
2. National Values and Cultural Diversity
3. Multicultural Awareness and Inclusive Practices
4. Ethical Decision-Making in Data Protection



# Mode of delivery and Assessment

## ❖ **Module 1**

- ❖ Use real-world Ugandan examples to contextualize laws and ethics.
- ❖ Encourage discussion and reflection—especially around ethical dilemmas and multicultural values.
- ❖ Apply adult learning principles: self-direction, relevance, experience-sharing.
- ❖ Integrate participatory methods: case studies, role plays, breakout groups, and quizzes.
- ❖ Ensure accessibility: use visual aids, plain language, and inclusive facilitation.

## **Module 2**

- ❖ Use real-world Ugandan case studies (e.g., NIRA, telecoms, hospitals, fintechs).
- ❖ Facilitate peer learning: Encourage trainers to share sector-specific practices.
- ❖ Incorporate simulations and role plays to build confidence in handling breaches, audits, and training delivery.
- ❖ Use visual tools: data lifecycle diagrams, risk matrices, breach response flowcharts.
- ❖ Encourage reflection on ethical dilemmas, organizational readiness, and personal biases.





# M.2 Data Privacy Governance and Management

In the Data Privacy Governance & Management course, participants will learn how to establish and maintain robust privacy governance frameworks within organizations. **Topics covered include;**



**Emerging  
Technological Trends  
and Data Protection**

1

## Sub topics Detailing;

1. Introduction to Technology Fundamentals
2. Introduction to Emerging Technologies and Data Privacy
3. Specific Emerging Technologies and their Data Privacy Implications
4. Legal and Ethical Frameworks for Data Protection in a Technological Era
5. Strategies for Mitigating Data Privacy Risks

## Sub topics Detailing;

1. Introduction to Privacy Governance
2. Establishing a Privacy Governance Framework
3. Data Privacy Risk Management
4. Implementing Privacy Controls and Processes
5. Monitoring and Continuous Improvement



**Privacy Governance  
(Governance, Management  
& Risk Management)**

2



**Data Lifecycle (Records  
Management, Retention  
and Disposal)**

3

## Sub topics Detailing;

1. Introduction to Data Lifecycle Management
2. Data Collection and Storage
3. Data Retention and Scheduling
4. Data Disposal and Destruction
5. Legal and Regulatory Considerations



# M.2 Data Privacy Governance and Management

In the Data Privacy Governance & Management course, participants will learn how to establish and maintain robust privacy governance frameworks within organizations. **Topics covered include;**



## Data Protection and Privacy Awareness and Training Programs

4

### Sub topics Detailing;

1. Introduction to Data Protection and Privacy Programs
2. Goals and Objectives of Privacy Programs
3. Requirements and Responsibilities of Data Protection Officer
4. Privacy Best Practices, Regulations, and Compliance Standards
5. Training Delivery Techniques and Strategies
6. Designing Effective Privacy Training Sessions
7. Practical Exercises and Case Studies

### Sub topics Detailing;

1. Overview of Data Security Breaches
2. Incident Identification and Investigation
3. Data Breach Notification Requirements
4. Complaint Management Process
5. Communication and Reporting



## Personal Data Security Breaches and Complaints Management

4



# M.3 Cyber Security Fundamentals

The Cyber Security Fundamentals course provides participants with essential knowledge and skills to mitigate cybersecurity risks and safeguard data from cyber threats

***Modules covered include;***

## **Information Security Fundamentals and Basic Security tools**

**Sub topics Detailing;**

1. Introduction to Information Security fundamentals
2. Cryptography and the Public Key Infrastructure
3. Attacks and Incident Response Handling

## **Data Protection Impact Assessments**

**Sub topics Detailing;**

1. Introduction to Data Protection Impact Assessments (DPIAs)
2. DPIA Methodologies and Tools
3. Identifying Privacy Risks in Data Processing Activities
4. Developing DPIA Reports: Documentation and Reporting Requirements

**01**

**02**

## **Data Protection and Privacy Audits**

**Sub topics Detailing;**

1. Introduction to Data Protection and Privacy Audits.
2. Privacy Audit Principles and Standards.
3. Audit Planning and Execution)
4. Third-Party Assessments and Vendor Management
5. Documentation and Reporting

**04**

## **Cyber Security Maturity Assessment**

**Sub topics Detailing;**

1. Introduction to Cyber Security Maturity Assessment.
2. Asset Management, risk Assessment and Policies
3. Technical Controls and Cyber Security Training Awareness
4. Incident Response and Recovery
5. Reporting and Communication

**03**





# Mode of delivery and Assessment

## E.Mode of Delivery

The modules will be delivered by experienced professionals with expertise in the corresponding fields. Using a combination of

- Interactive lectures
- Group discussions,
- Lab assessments
- Scenario case studies
- Guest speaker presentations.

Online learning resources, including readings, videos and quizzes will be available to facilitate independent learning.

## F.Module Assessment:

Each module will be assessed over **40% continuous assessment** and a **comprehensive 3hour examination** and contribute 60% towards the overall grade. To pass the course, students must achieve a combined score of at least 60% in both the continuous assessment and exam.



# Profile of Human Resource

The person shall have a minimum of a degree within one of the following disciplines;

01

**Law:** A Bachelor degree coupled with adequate working experience of at least 5 years of practice, an LLM (Master of Laws), or equivalent with a focus on privacy and data protection law.

02

**Information Technology:** A minimum of a degree in Computer Science, Information Systems, or Cybersecurity, preferably with experience related to data protection coupled with adequate working experience of at least 5 years in practice.

03

**Business Administration:** An MBA with a concentration in compliance, risk management, or information management coupled with adequate working experience of at least 5 years in practice.

1. Professional Certifications for the trainers from any of the following areas shall be required:
  - Privacy and Data Protection (Certified Information Privacy Professional (CIPP), Certified Information Privacy Manager (CIPM), Certified Information Privacy Technologist (CIPT)); Certified Data Privacy Solutions Engineer (CDPSE), Certified Information Systems Auditor (CISA), Cybersecurity (Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM)) and Compliance and Governance (Certified in Governance, Risk and Compliance (CGRC)).
2. Adequate Practical Experience from the industry, teaching and training will be required for all trainers. Several years of experience working in data protection roles, such as Data Protection Officer (DPO), compliance manager, or privacy consultant.
3. Hands-on experience with implementing data protection frameworks and ensuring regulatory compliance within organizations and will also provide experience.
4. Previous experience in teaching at a university or institute level or having conducted professional training programs.
5. Having developed educational materials related to data protection and privacy laws.
6. Membership in Professional Bodies: Active membership in professional organizations such as the International Association of Privacy Professionals (IAPP), Information Systems Audit and Control Association (ISACA), International Information System Security Certification Consortium (ISC)2 or similar.

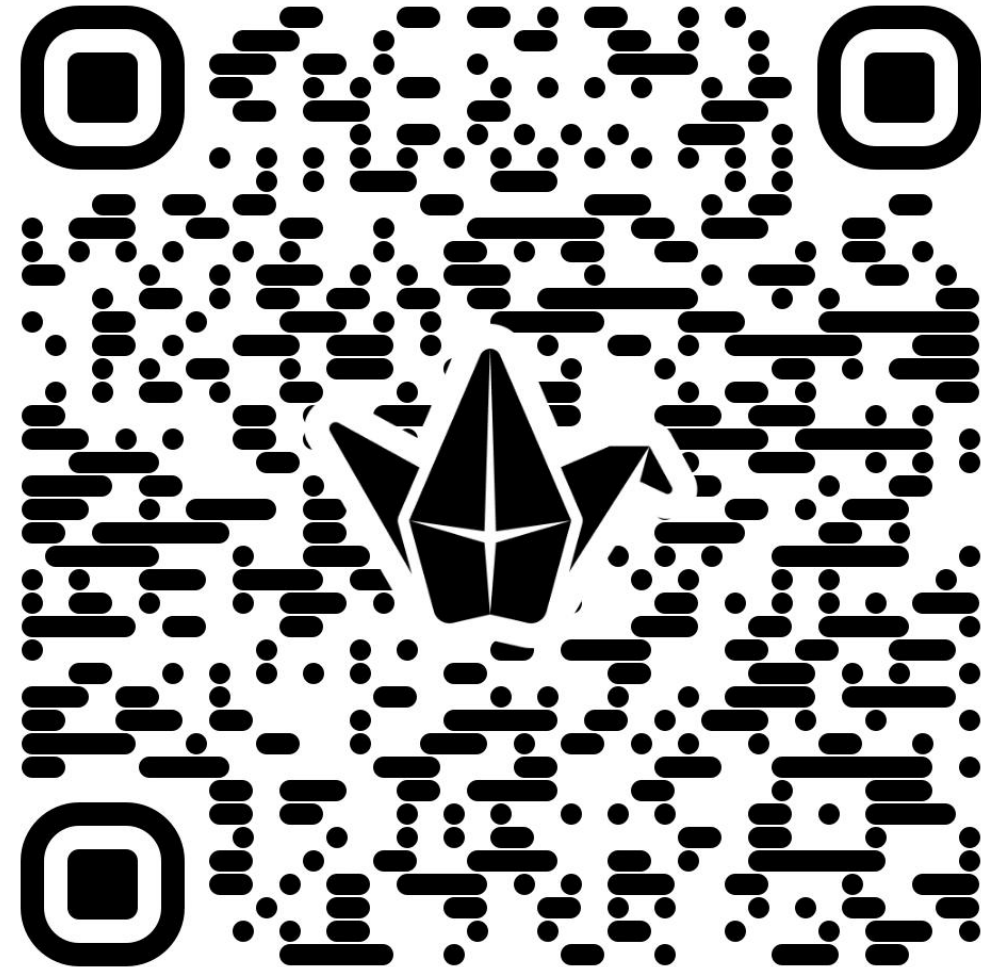


# Feedback on the curriculum and suggestions on the curriculum delivery

Access link:

<https://shorturl.at/Y0Ea4>

Scan QR CODE





Personal  
**DATA**  
Protection  
**OFFICE**

# Thank You



## Team work!