Datastat Research
Building Capacity in Training and Research

DATASTAT TRAINING IN

OFFICIAL COURSE PROSPECTUS

Center for Advanced Research & Professional Development

Nairobi Training Center • Global Virtual Academy • Corporate On-Site

LEGAL INSTITUTE

Digital Privacy Rights and Surveillance Regulation Training Course

Comprehensive Course Syllabus, Practical Modules & Upcoming Schedules

PROGRAM SPECIFICATIONS & HIGHLIGHTS

DURATION
5 Days Practical Hands-on

DELIVERY MODES
In-Person Class & Live Virtual

CERTIFICATION
Accredited Certificate of Completion

INTAKES / DATES
Multiple Cohort Schedules Included

PREPARED FOR:

Valued Participant

Email: training@datastatresearch.org | Issued: November 21, 2026

Academic & Professional Training Year: 2026

DATASTAT TRAINING INSTITUTE

P.O. Box 102802-00101, Nairobi, Kenya

Training Centers: Nairobi • Mombasa • Kigali • Dubai • Live Virtual Academy

Tel: +254 724 527 104 | +254 734 969 612

Email: training@datastatresearch.org

www.datastatresearch.org

Digital Privacy Rights and Surveillance Regulation Training Course

Legal Institute • 5 Days Intensive • Accredited Certification

Course Overview

Digital Privacy Rights and Surveillance Regulation Training Course is designed to equip professionals with the legal, regulatory, technological and institutional competencies required to protect personal data, uphold digital privacy rights and regulate surveillance activities in an increasingly interconnected digital environment.

Key Skills & Software Tools Covered

Digital Privacy Protection • Surveillance Law Compliance • Human Rights Advocacy • Data Governance

Upcoming Training Schedules

Confirmed cohort intakes and venues. Both physical in-person classroom and live virtual online seats are available.

TRAINING DATES	LOCATION / VENUE	FORMAT / DURATION	INVESTMENT (FEE)
23 Nov 2026 – 27 Nov 2026	Nairobi	Classroom / 5d	**$1,500 USD / KES 110,000**
23 Nov 2026 – 27 Nov 2026	Kigali	Classroom / 5d	**$3,000 USD / KES 110,000**
23 Nov 2026 – 27 Nov 2026	Dubai	Classroom / 5d	**$5,000 USD / KES 110,000**
23 Nov 2026 – 27 Nov 2026	Cape Town	Classroom / 5d	**$4,500 USD / KES 110,000**
23 Nov 2026 – 27 Nov 2026	Addis Ababa	Classroom / 5d	**$3,000 USD / KES 110,000**
23 Nov 2026 – 27 Nov 2026	Singapore	Classroom / 5d	**$5,000 USD / KES 110,000**
23 Nov 2026 – 27 Nov 2026	Istanbul	Classroom / 5d	**$5,000 USD / KES 110,000**
23 Nov 2026 – 27 Nov 2026	Bangkok	Classroom / 5d	**$5,000 USD / KES 110,000**
23 Nov 2026 – 27 Nov 2026	Accra	Classroom / 5d	**$4,000 USD / KES 110,000**
30 Nov 2026 – 4 Dec 2026	Nairobi	Classroom / 5d	**$1,500 USD / KES 110,000**
30 Nov 2026 – 4 Dec 2026	Kigali	Classroom / 5d	**$3,000 USD / KES 110,000**
30 Nov 2026 – 4 Dec 2026	Dubai	Classroom / 5d	**$5,000 USD / KES 110,000**

* Corporate discounts and customized cohort scheduling are available for teams of 3 or more participants.

Course Curriculum & Modules

Digital Privacy Rights and Surveillance Regulation Training Course

Introduction

Digital Privacy Rights and Surveillance Regulation Training Course is designed to equip professionals with the legal, regulatory, technological and institutional competencies required to protect personal data, uphold digital privacy rights and regulate surveillance activities in an increasingly interconnected digital environment. As governments, corporations, financial institutions, telecommunications providers and digital platforms expand their use of data-driven technologies, concerns surrounding data protection, online privacy, digital surveillance, biometric identification, artificial intelligence (AI), facial recognition, behavioural tracking and electronic communications monitoring continue to grow. This course explores the evolving legal frameworks governing digital privacy, including constitutional privacy protections, data protection legislation, international privacy standards, cross-border data transfers and regulatory compliance obligations. Participants will examine how emerging technologies affect individual freedoms, informational autonomy, confidentiality and the right to privacy while understanding the responsibilities of organisations that collect, process, store, share and monitor personal information.

The training further examines the regulation of government surveillance, corporate monitoring, intelligence gathering, lawful interception, electronic communications surveillance and digital investigation practices. Participants will develop practical skills in conducting privacy impact assessments, evaluating surveillance authorisations, implementing privacy-by-design principles, managing consent, preventing unlawful data collection and responding to data breaches and privacy complaints. Particular attention will be given to the implications of artificial intelligence-powered surveillance, predictive analytics, Internet of Things (IoT) monitoring, geolocation tracking, social media surveillance and mass data collection. Through practical exercises, regulatory case studies and simulated compliance scenarios, participants will learn how to balance legitimate security and law enforcement objectives with fundamental human rights, transparency, accountability, proportionality and due process. The course provides actionable insights into building responsible digital governance systems, strengthening institutional privacy safeguards and ensuring compliance with evolving national, regional and international surveillance regulations.

Course Duration

5 days

Course Objectives

By the end of this training course, participants should be able to:

- Understand fundamental digital privacy rights, constitutional protections and international human rights standards governing personal information.
- Interpret national and international data protection laws, privacy regulations and electronic communications legislation.
- Evaluate legal requirements governing government surveillance, lawful interception and intelligence monitoring.
- Conduct effective Data Protection Impact Assessments (DPIAs) and privacy risk assessments.
- Apply privacy-by-design and privacy-by-default principles in digital systems and organisational processes.
- Assess the legality, necessity and proportionality of digital surveillance activities.
- Understand regulatory requirements for biometric data processing, facial recognition and AI-powered surveillance.
- Develop effective policies for data minimisation, consent management, data retention and information security.
- Identify and mitigate risks associated with mass surveillance, behavioural tracking and online profiling.
- Strengthen organisational accountability through privacy audits, compliance monitoring and regulatory reporting.
- Manage cross-border data transfers and international digital privacy compliance obligations.
- Investigate privacy violations, data breaches and unlawful surveillance complaints while preserving digital evidence.
- Develop responsible digital governance frameworks that balance national security, public safety, commercial interests and individual privacy rights.

Target Audience

- Data Protection Officers (DPOs), privacy officers and data governance professionals.
- Government regulators, policymakers and public sector administrators.
- Law enforcement officers, intelligence personnel and digital investigation specialists.
- Legal practitioners, corporate lawyers and human rights advocates.
- Cybersecurity professionals, information security managers and IT auditors.
- Telecommunications operators, internet service providers and digital platform administrators.
- Compliance officers, risk managers and corporate governance professionals.
- Technology executives, AI developers, digital transformation specialists and privacy consultants.

Course Modules

Module 1: Foundations of Digital Privacy Rights and Human Rights Protection

- Evolution of digital privacy rights in the modern information society.
- Constitutional protection of privacy, dignity and personal autonomy.
- International human rights instruments and digital rights standards.
- Principles of confidentiality, informational self-determination and data sovereignty.
- Balancing privacy rights against national security and public interest objectives.
- Case Study: Examining a constitutional privacy dispute involving government access to citizens' private communications and the implications for fundamental human rights.

Module 2: Data Protection Laws and International Privacy Regulatory Frameworks

- Overview of national data protection legislation and regulatory institutions.
- General Data Protection Regulation (GDPR) principles and compliance obligations.
- African Union data protection frameworks and regional privacy standards.
- Kenya's Data Protection Act, 2019, and the role of the Office of the Data Protection Commissioner.
- International data transfers, adequacy requirements and regulatory cooperation.
- Case Study: Assessing a multinational digital service provider's failure to comply with cross-border personal data transfer requirements and developing corrective compliance measures.

Module 3: Government Surveillance and Lawful Interception Regulation

- Legal foundations of government surveillance and intelligence gathering.
- Regulation of lawful interception of electronic communications.
- Surveillance warrants, judicial authorisation and oversight mechanisms.
- Necessity, proportionality and legitimate purpose requirements.

• Accountability, transparency and safeguards against arbitrary surveillance.

• Case Study: Evaluating a government agency's request to intercept private communications during a national security investigation and determining the applicable legal safeguards.

Module 4: Corporate Surveillance, Employee Monitoring and Digital Workplace Privacy

• Legal boundaries of employee monitoring and workplace surveillance.

• Monitoring corporate emails, internet usage and digital communications.

• CCTV surveillance, location tracking and employee productivity analytics.

• Employee consent, transparency and legitimate monitoring interests.

• Developing workplace privacy policies and acceptable-use frameworks.

• Case Study: Reviewing a corporation's implementation of employee monitoring software that tracks computer activity, location and electronic communications without adequate transparency.

Module 5: Artificial Intelligence, Biometrics and Emerging Surveillance Technologies

• AI-powered surveillance systems and automated decision-making.

• Facial recognition, biometric identification and behavioural analytics.

• Predictive policing, algorithmic profiling and automated risk assessment.

• Internet of Things (IoT), smart devices and continuous data collection.

• Ethical AI governance, algorithmic accountability and privacy safeguards.

• Case Study: Assessing the privacy and discrimination risks associated with a city's deployment of facial recognition technology in public spaces.

Module 6: Privacy Compliance, Data Governance and Risk Management

• Developing organisational privacy policies and governance structures.

• Conducting Data Protection Impact Assessments (DPIAs).

• Privacy-by-design, privacy-by-default and data minimisation strategies.

• Data retention, consent management and lawful processing requirements.

• Privacy audits, compliance reporting and regulatory enforcement readiness.

• Case Study: Designing a privacy compliance programme for a financial institution introducing a new digital customer identification and monitoring platform.

Module 7: Digital Privacy Violations, Cybersecurity and Regulatory Enforcement

• Identifying unlawful data collection, disclosure and surveillance practices.

• Data breach investigation, notification and incident response procedures.

• Digital evidence preservation and forensic investigation requirements.

• Individual rights, privacy complaints and regulatory enforcement mechanisms.

• Civil liabilities, administrative penalties and institutional accountability.

• Case Study: Investigating a data breach involving unauthorised access to customer records and determining the organisation's notification, remediation and regulatory reporting obligations.

Module 8: Responsible Surveillance Governance and Future Regulatory Developments

• Developing responsible surveillance policies and institutional oversight mechanisms.

• Independent regulatory supervision and parliamentary accountability.

• Human rights impact assessments for surveillance technologies.

• Emerging challenges involving big data, cloud computing and cross-border monitoring.

• Building sustainable digital privacy and surveillance compliance frameworks.

• Case Study: Developing a regulatory oversight framework for a national digital surveillance programme that incorporates judicial supervision, independent audits, transparency and effective remedies for affected individuals.

Training Methodology

• Interactive lectures and presentations.

• Group discussions and brainstorming sessions.

• Hands-on exercises using real-world datasets.

• Role-playing and scenario-based simulations.

• Analysis of case studies to bridge theory and practice.

• Peer-to-peer learning and networking.

- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@datastatresearch.org or call +254724527104

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to DATASTAT CONSULTANCY LTD account, as indicated in the invoice so as to enable us prepare better for you.

Certification & Learning Methodology

- Hands-on practical delivery with real-world datasets, case studies, and lab exercises.
- Post-training mentorship, access to class resources, and customized follow-up support.
- Participants who successfully complete the course receive an accredited Datastat Certificate of Completion.

How to Enroll & Reserve Your Seat

1. Online Registration: Visit https://datastatresearch.org/courses/digital-privacy-rights-and-surveillance-regulation-training-course to register online.
2. Email Booking: Send participant details to training@datastatresearch.org for official invoice & reservation.
3. Support & Assistance: Inquire via phone +254 724 527 104 | +254 734 969 612.