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 Identity, Biometrics and Electronic Authentication Law 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 Identity, Biometrics and Electronic Authentication Law Training Course

Legal Institute • 5 Days Intensive • Accredited Certification

Course Overview

Digital Identity, Biometrics and Electronic Authentication Law Training Course is designed to equip legal professionals, policymakers, regulators, cybersecurity specialists and technology leaders with the legal, regulatory and technical knowledge required to govern digital identity systems and electronic authentication frameworks.

Key Skills & Software Tools Covered

Digital Identity Management • Biometric Data Protection • Electronic Authentication • Privacy Compliance

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 Identity, Biometrics and Electronic Authentication Law Training Course

Introduction

Digital Identity, Biometrics and Electronic Authentication Law Training Course is designed to equip legal professionals, policymakers, regulators, cybersecurity specialists and technology leaders with the legal, regulatory and technical knowledge required to govern digital identity systems and electronic authentication frameworks. As governments, financial institutions, businesses and public agencies increasingly adopt digital transformation strategies, the use of electronic identification, biometric recognition, digital credentials and electronic signatures has become central to modern service delivery. However, these developments introduce complex legal considerations relating to digital identity governance, data protection, biometric privacy, identity verification, electronic transactions, cybersecurity, digital trust and regulatory compliance. This course explores the legal foundations of digital identity management, including identity registration, authentication standards, consent management, personal data processing, cross-border data transfers and the legal recognition of electronic signatures and digital credentials. Participants will examine international legal frameworks, emerging regulatory trends and best practices for establishing secure, inclusive and legally compliant digital identity ecosystems.

The training also addresses the growing legal and ethical implications of biometric technologies, including facial recognition, fingerprint scanning, iris recognition, voice biometrics and behavioural authentication. Participants will develop practical skills in evaluating biometric data protection risks, managing identity fraud, addressing algorithmic bias, ensuring transparency and accountability, and responding to digital identity breaches. Particular attention will be given to electronic authentication laws, digital identity assurance, identity theft prevention, biometric data security, AI-powered identity verification, digital evidence admissibility and cybersecurity risk management. Through practical exercises, regulatory analysis and international case studies, participants will learn how to develop effective digital identity policies, assess technology-provider compliance, strengthen authentication controls and manage legal disputes involving electronic identity systems. The course provides a comprehensive understanding of how law, technology, privacy and institutional governance intersect in the rapidly evolving digital identity landscape.

Course Duration

5 days

Course Objectives

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

- Understand the legal foundations, principles and regulatory frameworks governing digital identity management and electronic identification systems.
- Interpret international and national legislation relating to digital identity, electronic transactions and digital authentication.
- Evaluate biometric data protection requirements and legal safeguards for processing sensitive personal information.
- Understand the legal recognition, validity and enforceability of electronic signatures and digital contracts.
- Apply data privacy, consent management and lawful processing principles to biometric identity systems.
- Assess the legal implications of facial recognition, fingerprint scanning, iris recognition and voice authentication technologies.
- Strengthen digital identity verification, identity assurance and authentication governance frameworks.
- Identify and mitigate identity theft, impersonation, deepfake fraud and synthetic identity risks.
- Evaluate cybersecurity obligations and legal responsibilities associated with digital identity breaches.
- Apply AI governance, algorithmic accountability and fairness principles to automated biometric identification.
- Understand cross-border digital identity recognition, interoperability and international data transfer requirements.
- Develop effective compliance strategies for electronic authentication service providers and digital identity operators.
- Strengthen legal risk management, regulatory reporting and dispute resolution involving digital identity and biometric technologies.

Target Audience

- Legal practitioners, corporate lawyers and legal advisers handling technology-related legal matters.
- Government officials and policymakers responsible for digital transformation and national identification programmes.
- Data protection officers and privacy compliance professionals.
- Cybersecurity professionals, information security managers and IT governance specialists.
- Banking, financial services and fintech professionals responsible for digital onboarding and customer authentication.
- Regulatory authorities and compliance officers overseeing electronic transactions and digital identity services.
- Identity management specialists, biometric technology professionals and digital authentication providers.
- Risk managers, auditors, forensic investigators and fraud prevention specialists.

Course Modules

Module 1: Legal Foundations of Digital Identity and Electronic Identification

- Concepts, principles and evolution of digital identity systems.
- Legal definitions of digital identity, identification and authentication.
- National digital identity frameworks and regulatory governance.
- Legal recognition of electronic identification credentials.
- Rights, responsibilities and accountability of digital identity stakeholders.
- Case Study: Examining the legal and governance challenges arising from the implementation of a national digital identity programme, including concerns about inclusion, privacy and institutional accountability.

Module 2: International Digital Identity Laws and Regulatory Frameworks

- International standards and legal principles governing digital identity.
- UNCITRAL Model Law on Electronic Commerce and Electronic Signatures.
- Electronic identification and trust services regulatory frameworks.
- Comparative analysis of digital identity legislation across jurisdictions.
- Cross-border recognition of electronic identification credentials.

• Case Study: Comparing the European Union's eIDAS framework with digital identity regulatory approaches in other jurisdictions and evaluating their implications for international transactions.

Module 3: Biometrics Law, Privacy and Data Protection Compliance

• Legal classification and protection of biometric personal data.

• Fingerprint, facial, iris, voice and behavioural biometric technologies.

• Lawful processing, informed consent and purpose limitation.

• Data minimisation, retention and secure biometric storage.

• Data protection impact assessments for biometric systems.

• Case Study: Assessing a financial institution's deployment of facial recognition technology and determining whether its collection, processing and storage of biometric information comply with applicable privacy laws.

Module 4: Electronic Authentication, Digital Signatures and Trust Services

• Legal principles of electronic authentication and identity assurance.

• Electronic signatures, advanced electronic signatures and digital signatures.

• Digital certificates, public key infrastructure and cryptographic authentication.

• Legal validity and enforceability of electronic agreements.

• Responsibilities of trust service providers and certification authorities.

• Case Study: Evaluating a commercial contract executed through electronic signatures, focusing on authentication reliability, consent, evidentiary value and enforceability.

Module 5: Digital Identity Fraud, Cybersecurity and Legal Liability

• Identity theft, impersonation and synthetic identity fraud.

• Deepfake-enabled identity manipulation and authentication attacks.

• Biometric spoofing, presentation attacks and liveness detection.

• Cybersecurity obligations for digital identity service providers.

• Legal liability, breach notification and incident response.

• Case Study: Investigating a biometric authentication breach involving fraudulent account access and examining the liability of the service provider, technology vendor and affected institution.

Module 6: Artificial Intelligence, Automated Biometrics and Algorithmic Accountability

• AI-powered facial recognition and automated identity verification.

• Algorithmic bias, discrimination and biometric accuracy.

• Explainability, transparency and accountability in AI authentication.

• Legal implications of automated decision-making and profiling.

• AI governance, human oversight and responsible biometric innovation.

• Case Study: Reviewing a facial recognition system that produces disproportionately high false rejection rates for certain demographic groups and identifying the relevant legal, ethical and regulatory concerns.

Module 7: Digital Identity Governance, Interoperability and Cross-Border Compliance

• Digital identity governance structures and institutional responsibilities.

• Interoperability standards and federated identity management.

• Single sign-on, identity federation and authentication protocols.

• Cross-border identity verification and international data transfers.

• Digital identity inclusion, accessibility and consumer protection.

• Case Study: Examining a regional digital identity verification initiative that enables financial institutions to authenticate customers across national borders while complying with different data protection laws.

Module 8: Regulatory Compliance, Digital Evidence and Dispute Resolution

• Digital identity audits and regulatory compliance assessments.

• Electronic authentication records and audit trail management.

• Admissibility and evidentiary value of biometric and electronic records.

• Legal disputes involving identity verification and electronic signatures.

• Development of digital identity policies and compliance programmes.

• Case Study: Analysing a court dispute involving an electronically authenticated transaction where the customer denies authorising the transaction, focusing on digital evidence, authentication logs and burden of proof.

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-identity-biometrics-and-electronic-authentication-law-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.