AI and Data Privacy

Navigating Compliance in Africa



PECB REGIONAL WEBINARS

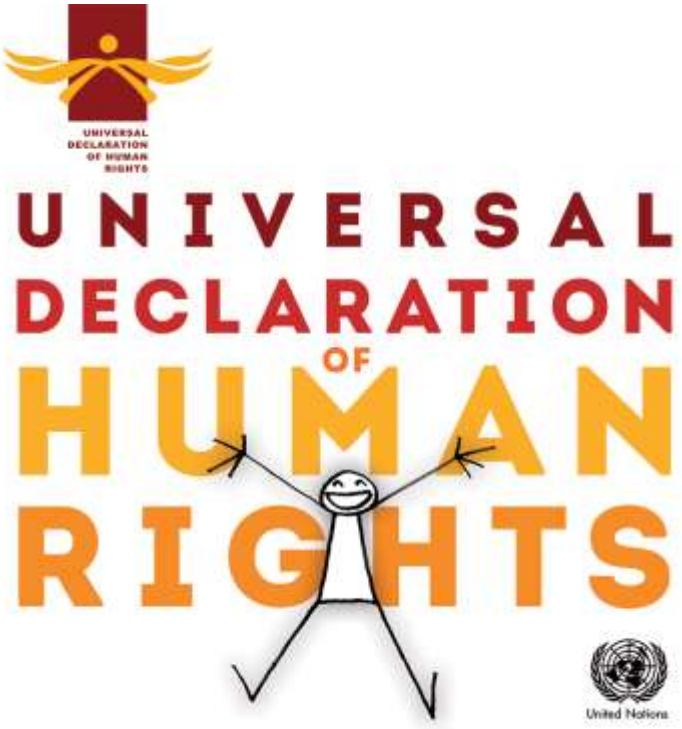
Agenda

1. Human Rights and Data Protection
2. Information Security versus Privacy/Data Protection
3. Legal and Regulatory Background
4. Privacy Implementation Controls (PIMS)
5. Transition of NDPA
6. Key Provisions of GAID 2025
7. Data Protection Roles & Responsibilities
8. National Data Architecture
9. Alignment with Global Standards
10. Maturity Roadmap and Next Steps
11. AI Overview
12. How does AI Work?
13. Why AI and Privacy Matter Now
14. AI and Privacy Intersection
15. Global Privacy and AI Regulation
16. Kenya's Data Protection Act
17. Why Traditional Compliance Falls Short
18. ISO/IEC 42001 – AI Management System
19. Best Practices Controls
20. Roadmap to Responsible AI
21. Q&A

UN Declaration of Human Rights

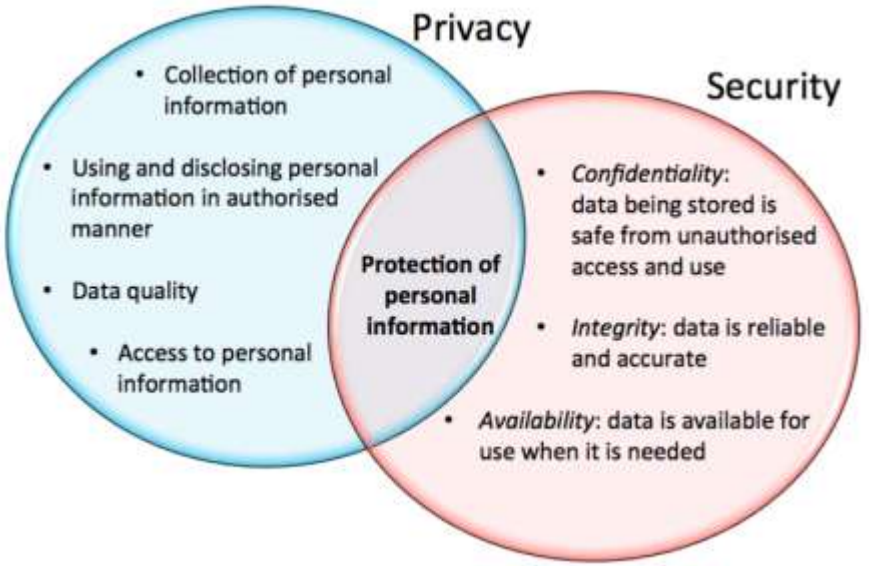
- **Article 12:** No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

- **Article 8:** Everyone has the right to an effective remedy by the competent national tribunals for acts violating the fundamental rights granted him by the constitution or by law.

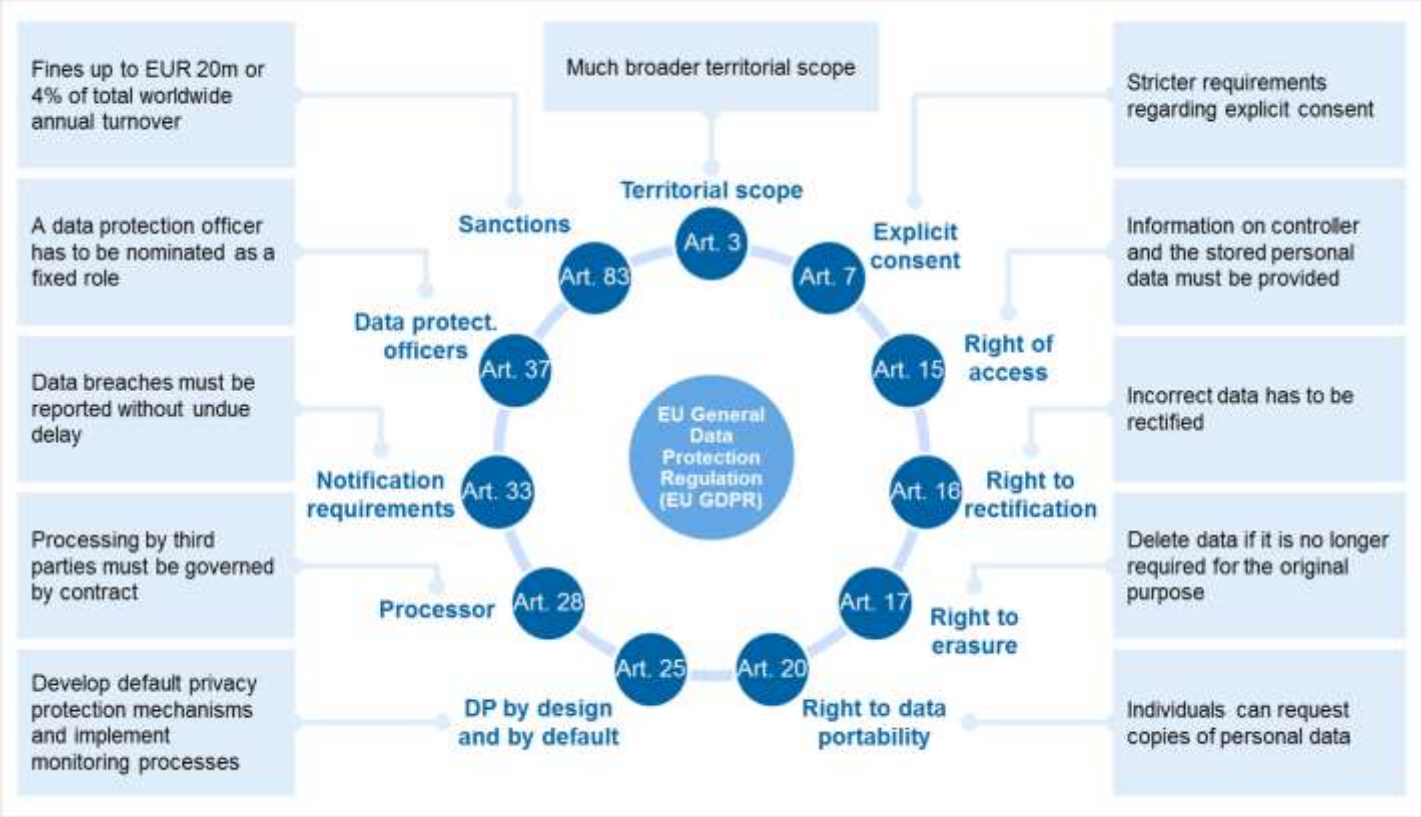


Information Security versus Privacy/Data Protection

SECURITY	PRIVACY
Security refers to protection against unauthorized access.	Privacy defines the ability to protect personally identifiable information.
Security provides protection for all types of data and information including the ones that are stored electronically.	Privacy means protecting sensitive information related to individuals and organizations.
Security can be achieved without privacy.	Privacy cannot be achieved without security.
Security program focuses on all sorts of information assets that an organization collects.	Privacy program focuses on personal information such as names, addresses, social security numbers, log in credentials, financial accounts information, etc.
It implements security protocols to	It refers to protection of privacy



GDPR


Fines up to EUR 20m or 4% of total worldwide annual turnover
A data protection officer has to be nominated as a fixed role
Data breaches must be reported without undue delay
Processing by third parties must be governed by contract
Develop default privacy protection mechanisms and implement monitoring processes
Much broader territorial scope
Territorial scope
Art. 3
Sanctions
Art. 83
Explicit consent
Art. 7
Data protect. officers
Art. 37
Right of access
Art. 15
EU General Data Protection Regulation (EU GDPR)
Notification requirements
Art. 33
Art. 16
Right to rectification
Processor
Art. 28
Art. 17
Right to erasure
Art. 25
DP by design and by default
Art. 20
Right to data portability
Stricter requirements regarding explicit consent
Information on controller and the stored personal data must be provided
Incorrect data has to be rectified
Delete data if it is no longer required for the original purpose
Individuals can request copies of personal data

The Republic of Kenya – Data Protection Act (DPA): 2019 = 53 Key Considerations (Excluding Parts 1, 2 and 9)

Part 3 (7) Registration of DC & DP	1. Registration of DCs and DPs. 2. Application for Regis.	3. Duration of Registration Certificate	4. Register of DCs and DPs.	5. Cancellation of Variation of the Certificate.	6. Compliance and Audit 7. Designation of the DPO
Part 4 (19) Principles and Obligations of Personal Data Protection 19 Key Requirements	1. Principles of Data Protection	2. Rights of a Data Subject	3. Exercise of Rights of Data Subjects	4. Collection of Personal Data	5. Duty to Notify
	6. Lawful Processing of Personal Data	7. Data Protection Impact Assessment	8. Conditions of Consent	9. Processing of Personal data relating to Child	10. Restrictions on Processing
	11. Automated Individual Decision Making	12. Objecting to Processing	13. Commercial Use of Data	14. Right to data Portability	15. Limitation to Retention of Personal Data
	16. Right of Recertification and Erasure	17. Data Protection by Design or by Default	18. Particulars of determining Organizational Measures		19. Notification and Communication of Breach
Part 5 (4) Grounds for Processing Sensitive Personal Data (SPD)	1. Processing of Sensitive Personal Data (SPD)	2. Permitted grounds for processing Sensitive Personal Data (SPD)		3. Personal Data relating to Health	4. Further categories of Sensitive Personal Data (SPD)
Part 6 (3) Transfer of Personal Data Outside Kenya	1. Conditions for Transfer out of Kenya	2. Safeguards prior to transfer of personal data out of Kenya		3. Processing through a Data Server of data Center in Kenya	
Part 7 (5) Exemptions	1. General Exemptions	2. Journalism, Literature and Art	3. Research, History and Statistics	4. Exemptions by the Data Commissioner	5. Data-sharing Code
Part 8 (10) Enforcement Provisions	1. Complaints to the Data Commissioner	2. Investigation of Complaints	3. Enforcement Notices	4. Power to seek Assistance	5. Obstruction of Data Commissioner
	6. Penalty Notices	7. Administrative Fines	8. Right of Appeal	9. Compensation to a Data Subject	10. Preservation Order
Part 10 (1): Provision of Delegated Powers Regulations	Part 11 (4): Miscellaneous Provisions	1. Offences of Unlawful Disclosure of Personal Data	2. General Penalty	3. Codes, Guidelines and Certification	4. Consequential Amendments

Transition of NDPA



NDPA 2023



GAID 2025

Nigeria Data Protection Act (NDPA) 2023 – 20 Requirements

Part 5: Principles and Lawful Basis Governing Processing of Personal Data – 10 Requirements	Part 6: Rights of a Data Subject – 5 Requirements
1. Principles of personal data processing	1. Rights of a data subject
2. Lawful basis of personal data processing	2. Withdrawal of consent
3. Consent	3. Right to object
4. Provision of information to the data subject	4. Automated decision making
5. Data privacy impact assessment	5. Data portability
6. Obligation of the data controller and data processor	Part 7: Data Security – 2 Requirements
7. Sensitive personal data	1. Security, integrity and confidentiality
8. Children of persons lacking the legal capacity to consent	2. Personal data breaches
9. Data Protection Officers	Part 8: Cross Border – 3 Requirements
10. Data protection compliance services	1. Basis for cross-border transfer of personal data
	2. Adequacy of protection
	3. Other bases for transfer of person data outside Nigeria

NDPC – NDPA 2023: General Application and Implementation Directive (GAID) 2025 – 52 Articles					
1. The Objectives and Application	2. Material Context of Data Processing and Priority of the NDPA	3. Statutory Remedy in Respect of Double or Multiple Regulatory Framework on DP	4. Cooperation between the Commission and a Public Authority	5. Evaluation of Exemptions to the NDPA	6. Data Processing by Individuals for Household or Personal Purposes
7. General NDPA Compliance Measures by data Controllers and Data Processors	8. Designation of Data Controllers and Data Processors of Major Importance	9. Registration as Data Controller or Data Processor of Major Importance	10. Filing of NDPA Compliance Audit Returns with the Commission	11. Designation of a Data Protection Officer	12. Position of the Data Protection Officer
13. Submission of Internal Semi-Annual Data Protection Report by a Data Protection Officer	14. Credential Assessment of a Data Protection Officer	15. Principles of Personal Data Protection	16. Lawful Bases of Data Processing	17. Reliance on Consent	18. Data Processing which requires Consent
19. Consent to Cookies and other Tracking Tools	20. Lawfulness of Purpose and Reliance on Consent and other Lawful Bases	21. Reliance on Contract	22. Reliance on Legal Obligation	23. Evaluation of Lawful Bases of data Processing	24. Reliance on Vital Interest
25. Reliance on Public Interest	26. Reliance on Legitimate Interest	27. Consideration regarding Information to Data Subjects	28. Data Privacy Impact Assessment	29. Monitoring, Evaluation and Maintenance of Data Security System	30. Schedule of Internal Sensitization and Training on Privacy.

NDPC – NDPA 2023: General Application and Implementation Directive (GAID) 2025 – 52 Articles					
31. Deployment of a data Processing Software by a Data Controller or Data Processor	32. Measures Against Privacy Breach Abetment	33. Data Breach Notification	34. Data Processing Agreement	35. Benchmarking with Interoperable Data Privacy Measures	36. Exercise of Right to Recertification
37. Exercise of Right to Data Portability	38. Exercise of Right to be Forgotten	39. Exercise of Right to Lodge a Complaint with NDPC	40. Data Subject's Standard Notice to Address Grievance	41. Data Ethics, privacy and Dignity of the Human Person	42. Application of Global Best Practice on Data Ethics
43. Emerging Technologies	44. Parameters for Assessing Privacy and Public Interest in Emerging Technologies	45. Cross-Border Data Transfer	46. Capacity Building in Data Protection and Professional Development Credits	47. Jurisdiction of Court and Access to Justice	48. Evidence of Compliance with the NDPA
49. Consideration of Time-Bound and Non-Time-Bound Obligations		50. Supplementary	51. Review of Administrative and Financial Obligations under Special Grounds		52. Definitions
Schedules	1. Principles of Data Protection	2. NDPA Compliance Audits Returns	3. Data Protection Officer's Assessment	4. Data Privacy Impact Assessment	5. Guidance on Cross-border Data Transfer
	6. Data Subject's Vulnerability Index	7. Guidance Notice on Registration DC	8. Legitimate Interest Assessment Template	9. Data Subject's Standard Notice to Address Grievance	10. NDPA Compliance Audit Returns filing Fee

ISO 27701:2025 - Dependent on ISO 27001



ISO/IEC FDIS 27701

Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance

Under development (Edition 2, 2025)

This draft is in the approval phase.

← Will replace ISO/IEC 27701:2019

ISO 27701 – Privacy Information Management System (PIMS): 2025

Clauses	Sub Clauses				
4.0 – Context of the Organization	4.1 – Understanding the Organization and its context	4.2 – Understanding the needs and expectations of Interested parties.	4.3 – Determining the Scope of the ISMS	4.4 – Privacy Information Management System	
5.0 – Leadership	5.1 – Leadership and Commitment	5.2 Privacy Policy	5.3 – Roles, Responsibilities and Authorities		
6.0 – Planning	6.1 – Actions to address Risks and Opportunities 6.1.2 – Privacy Risk Assessment 6.1.3 – Privacy Risk Treatment	6.2 – Privacy Objectives and Plans to achieve them	6.3 - Planning of Changes		
7.0 – Support	7.1 – Resources	7.2 – Competence	7.3 Awareness	7.4 – Communication	7.5 – Documented Information
8.0 – Operation	8.1 – Operational Planning and Control	8.2 – Privacy Risk Assessment	8.3 – Privacy Risk Treatment		
9.0 – Performance Evaluation	9.1 – Monitoring, Measurement, Analysis and Evaluation (MMAE)	9.2- Internal Audit	9.3 – Management Review		
10. Improvement	10.1 – Continual Improvement	10.2 – Nonconformity and Corrective Action			
	Annex - A - F				

PIMS - 27701

1. Controller/Processor
2. Policies and Procedures
3. PIIs (Merchants + Customers + Employees + Suppliers/Vendors)
4. Sensitive PIIs
5. RoPA
6. Purpose and Legitimacy of Collection/Processing
7. DPIAs (Departmental/Product)
8. Forms (Physical and Electronic)
9. Data Minimization and Collection
10. Consent and Choice
11. Data Mapping across Applications and Databases
12. Data Protection in New App. Development Projects/Products
13. Pseudonymization, Anonymization, Masking, Tokenization and Encryption
14. Automation and Reporting Dashboards
15. Privacy by Design and by Default
16. Incident Management and Breach Management Process
17. Alignment to NDPR/A, Ghana DPA and other Countries DPR/A
18. Independent Audit Reports and Business Review Reports
19. Communication, Staff Awareness and DP Champions and DPO Training/Certification
20. Improvement/Maturity Plans



Read sample

ISO/IEC 29100:2024

Information technology — Security techniques — Privacy framework

Published (Edition 2, 2024)

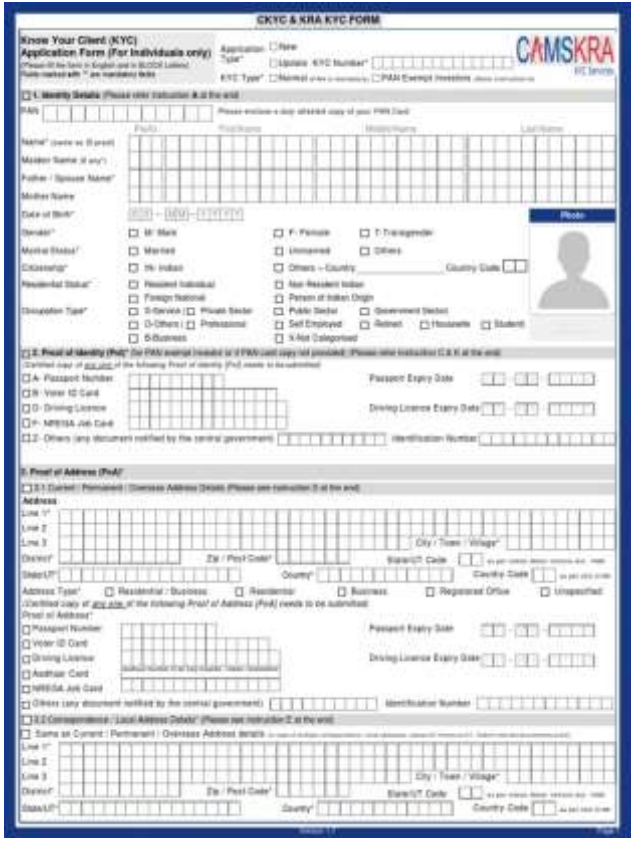
ISO 29100: 2024 – Privacy Framework						
5.1 – Overview of Privacy Framework						
5.2 – Actors and Roles		5.2.1 – General	5.2.2 – PII Principals	5.2.3 – PII Controllers	5.2.4 – PII Processors	5.2.5 – Third Parties
5.3 Interactions						
5.4 – Recognizing PII	5.4.1 – General	5.4.2 – Identifiers	5.4 3 - Other distinguishing characteristics	5.4.4 – Information which is or can be linked to a PII principal		
	5.4.5 – Pseudonymous data	5.4.6 – Metadata	5.4.7 – Unsolicited PII	5.4.8 – Sensitive PII		
5.5 – Privacy safeguarding requirements	5.5.1 – General	5.5.2 – Legal and regulatory factors	5.5.3 – Contractual factors	5.5.4 – Business factors	5.5.5 – Other factors	
5.6 – Privacy policies			5.7 – Privacy controls			
6. The privacy principles of ISO 29100	6.1 – Overview of privacy principles	6.2 – Consent and choice	6.3 – Purpose, legitimacy and specification	6.4 – Collection limitation	6.5 – Data minimization	6.6 – Use, retention and disclosure limitation
	6.7 – Accuracy and quality	6.8 – Openness, transparency and notice.	6.9 – Individual participation and access	6.10 – Accountability	6.11 – Information security	6.12 – Privacy compliance

36 Attributes that can be used to identify natural persons (attributes of Personally Identifiable information)
A privacy project means you ensure and attest to the protection of all the datasets below as applicable to customers, employees and suppliers (end to end data and information flows in physical and electronic formats).

1. Age or special needs of vulnerable natural persons
2. Allegations of criminal conduct
3. Any information collected during health services
4. Bank account or credit card number
5. Biometric identifier
6. Credit card statements
7. Criminal convictions or committed offences
8. Criminal investigation reports
9. Customer number
10. Date of birth
11. Diagnostic health information
12. Disabilities
13. Doctor bills
14. Employees' salaries and human resources files
15. Financial profile
16. Gender
17. GPS position
18. GPS trajectories
19. Home address
20. IP address
21. Location derived from telecommunications systems
22. Medical history
23. Name
24. National identifiers (e.g. passport number)
25. Personal e-mail address
26. Personal identification numbers (PIN) or passwords
27. Personal interests derived from tracking use of internet websites
28. Personal or behavioural profile
29. Personal telephone number
30. Photograph or video identifiable to a natural person
31. Product and service preferences
32. Racial or ethnic origin
33. Religious or philosophical beliefs
34. Sexual orientation
35. Trade-union membership
36. Utility bills

Various Business Forms

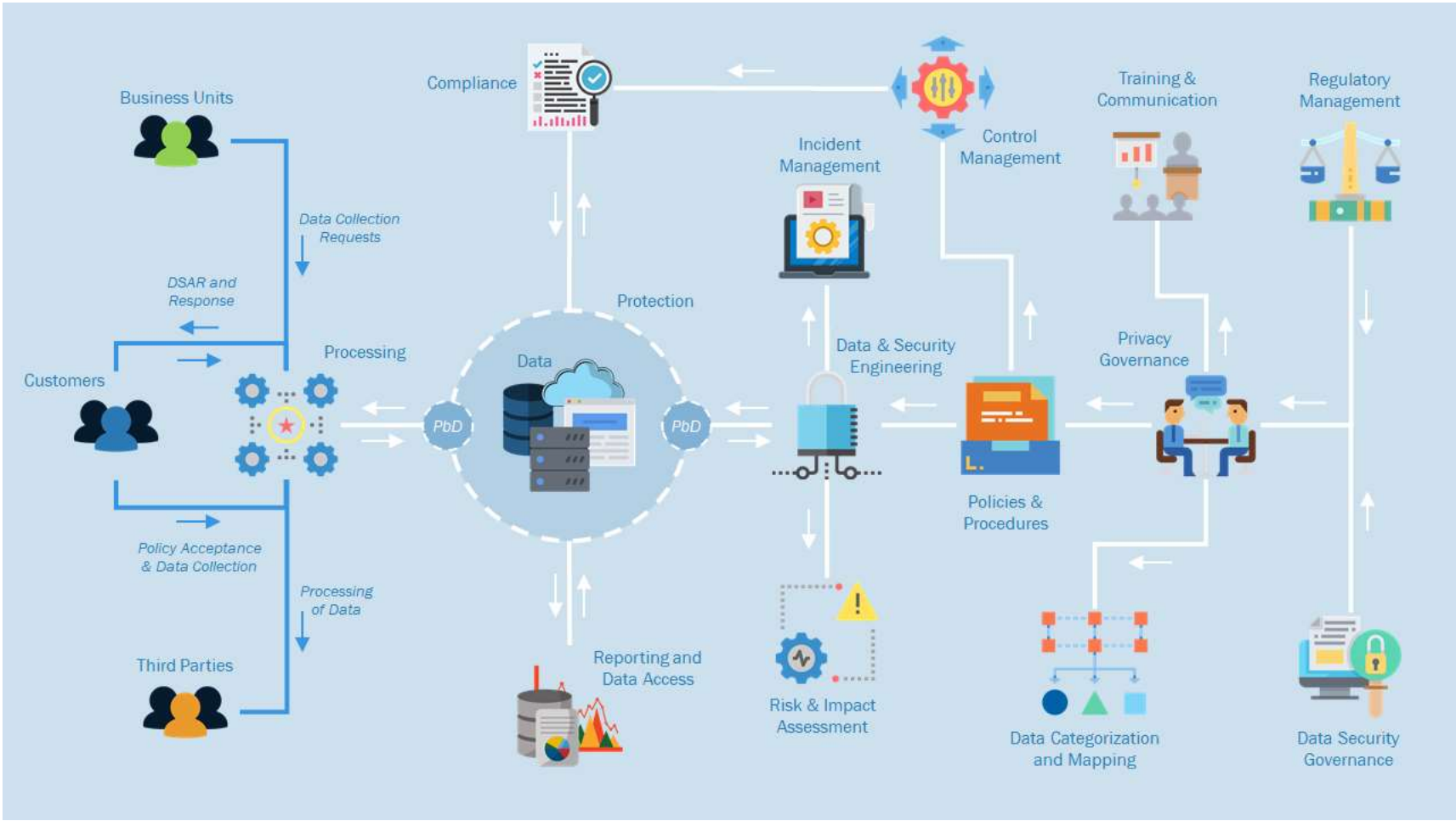
- Account Opening forms
- Bio Data forms
- Vendor Registration forms
- KYC forms
- Customer Compliant forms
- Conference forms





				PRE-TREATMENT						
RIS Ref	Personal Data Asset	Risk Scenario	Risk Owner	Existing Controls	Likelihood	Likelihood Rationale	Impact	Impact Rationale	Risk Score	Risk Level
1	Employee name and address	Data is stolen by an unauthorised person	IT Manager	Firewall and access control	2	No breaches have happened to date.	2	This is generally publicly-available data.	4	LOW
2	Employee name and address	Data is lost during the system conversion	Conversion Manager	Pre-conversion backups	2	There is in-house experience with similar data conversions.	2	Employee will need to provide details again.	4	LOW
3	Employee name and address	Data is corrupted during the system conversion	Conversion Manager	Testing of conversion programs	2	There is in-house experience with similar data conversions.	3	May affect tax situation of employee.	6	MEDIUM
4	Employee name and address	Data becomes viewable by other employees	HR Manager	Access control	3	Relies upon correct configuration which can be complicated.	4	Invasion of employee's privacy.	12	HIGH
5	Employee bank details	Data is stolen by an unauthorised person	IT Manager	Firewall and access control	2	No breaches have happened to date.	4	May expose the employee to fraud.	8	MEDIUM

	TREATMENT		POST-TREATMENT						
Risk Level	Treatment Option Chosen	Treatment Action(s)	Post-Treatment Likelihood	Post-Treatment Likelihood Rationale	Post-Treatment Impact	Post-Treatment Impact Rationale	Post-Treatment Risk Score	Post-Treatment Risk Level	Comments
LOW	Accept		2		2		4	LOW	
LOW	Accept		2		2		4	LOW	
MEDIUM	Accept		2		3		6	MEDIUM	
HIGH	Modify	Involve external specialist with configuration and thorough testing.	2	Likelihood of incorrect configuration reduced.	4	No change.	8	MEDIUM	
MEDIUM	Accept		2		4		8	MEDIUM	


Business Units
Compliance
Training & Communication
Regulatory Management
Incident Management
Control Management
Data Collection Requests
DSAR and Response
Protection
Processing
Customers
Data
Data & Security Engineering
Privacy Governance
PbD
PbD
Policies & Procedures
Policy Acceptance & Data Collection
Processing of Data
Third Parties
Reporting and Data Access
Risk & Impact Assessment
Data Categorization and Mapping
Data Security Governance

Tips For Protecting PII

1. Encryption
2. Use Strong Passwords
3. Two Factor Authentication
4. Backup Data
5. Safely Destroy Old Media with Personal Data
6. Install All Updates
7. Use a Secure Wireless Network
8. Use a VPN Service
9. Lock Your Device When Away
10. Do not upload confidential documents to the cloud
11. Use Security Questions
12. Use a Firewall
13. Use Anti-Virus
14. Use Anti-Malware
15. Check your privacy settings
16. Use a Secondary or Disposable Email Account

Source: wallarm

DATA PROTECTION & PRIVACY POLICY

1. **PURPOSE:** The purpose of this Data Protection and Privacy Policy is to establish the principles and practices for the protection of personal and sensitive data collected and processed by [COMPANY NAME]. This Policy ensures compliance with data protection laws and regulations and outlines our commitment to safeguarding the privacy and confidentiality of individuals' data.

2. **SCOPE:** This Policy applies to all employees, contractors, vendors, and authorized users who handle or have access to personal and sensitive data within [COMPANY NAME]. It encompasses data collected from customers, employees, partners, and other stakeholders.

3. **POLICY STATEMENTS**

Data Protection Principles

- **Lawful Processing:** [COMPANY NAME] will only collect, process, and use personal and sensitive data when there is a lawful basis for doing so, such as consent, contract necessity, legal obligation, legitimate interests, or the protection of vital interests.
- **Transparency:** Individuals will be informed about the purpose, use, and processing of their data at the time of collection or as soon as practicable thereafter.
- **Data Minimization:** [COMPANY NAME] will only collect data that is necessary for the specified purpose and will retain it only for as long as required.
- **Data Accuracy:** Reasonable efforts will be made to ensure the accuracy of data, and individuals have the right to request correction of inaccuracies.
- **Security:** Appropriate security measures, including encryption, access controls, and data breach response plans, will be implemented to protect data from unauthorized access, disclosure, alteration, or destruction.

Data Collection and Consent

- **Consent: Wherever** required by law, [COMPANY NAME] will obtain clear and unambiguous consent from individuals before collecting or processing their personal data.
- **Children's Data:** Special care will be taken to protect the data of children and minors, and parental or guardian consent will be obtained when necessary.

Data Subject Rights

- **Access and Rectification:** Data subjects have the right to access their data and request corrections, updates, or deletions.
- **Data Portability:** Data subjects may request their data in a structured, commonly used, and machine-readable format for portability.
- **Objection and Restriction:** Data subjects have the right to object to the processing of their data and request restriction under certain circumstances.

- **Withdrawal of Consent:** Data subjects have the right to withdraw their consent at any time where processing is based on consent.

Data Breach Response

- **Notification:** [COMPANY NAME] will promptly investigate and report data breaches to the appropriate regulatory authorities and affected individuals, as required by law.
- **Mitigation:** Steps will be taken to mitigate the impact of data breaches, prevent recurrence, and address vulnerabilities.

Third-Party Data Processors

- **Third-Party Contracts:** When [COMPANY NAME] engages third-party data processors, contracts will be established to ensure they comply with data protection regulations and safeguard the data in their custody.

Training and Awareness

- **Training:** Employees, contractors, and authorized users will receive regular training and awareness programs on data protection and privacy to ensure compliance and awareness of data protection principles.

4. **RESPONSIBILITIES**

- **Data Protection Officer (if applicable):** Responsible for overseeing data protection compliance, monitoring data security, and acting as the point of contact for data subjects and regulatory authorities.
- **Employees and Users:** Responsible for adhering to this Policy, understanding data protection principles, and reporting any data protection concerns or breaches.

5. **COMPLIANCE AND CONSEQUENCES**

Non-compliance with this Data Protection and Privacy Policy may result in disciplinary actions in accordance with [COMPANY NAME]'s policies and procedures. Violations may also lead to legal and regulatory penalties.

6. **POLICY REVIEW**

This Data Protection and Privacy Policy will be reviewed annually or more frequently if necessary. Updates or changes to the Policy will be communicated to all relevant personnel to ensure continued adherence to data protection and privacy guidelines.

Data Protection Job Description

Our growing company is hiring for a data protection. Thank you in advance for taking a look at the list of responsibilities and qualifications. We look forward to reviewing your resume.

Responsibilities for data protection

- Advise on compliance with relevant national and European law, EDPB, ICO (and other applicable Data Protection Authority) guidance, codes and best practice
- Advise on and identify data protection risks relating to all major projects proposed or undertaken by the business, including but not confined to risks around supplier relationships, transfer of data to third parties and the completion of PIAs
- Oversee the management and maintenance of all Data Protection-related policies, guidelines and materials
- Manage, participate in and sign off data protection projects and support the wider GDPR assessment stages across the UK and Ireland
- Develop relationships with other Data Protection Officers and provide advice and mentorship to the same across the Group to share knowledge and best practices
- Be seen as a reference point by most colleagues across the organization on data protection issues and best practice
- Relevant Data Protection qualification (ISEB / PDP / CIPPe)
- Daily interactions with government clients related to meeting technical requirements for ESOC initiatives, and weekly reporting requirements
- Manage product management artefacts and deliverables such as roadmaps, product overviews, reports, backlog and documentation
- Collect, synthesize and analyze product related data

Qualifications for data protection

- Minimum Bachelors or Degree from a University
- Lead business and technical conversations
- Experience with online tools (JIRA, GIT, Confluence)
- Experience utilizing agile methodologies – Kanban and/or Scrum
- Strong influence and negotiating skills, and the ability to overcome barriers and resistance to execute
- Expertise in data-protection mechanisms including an in understanding of cryptographic algorithms such as AES, 3DES, RSA, ECC, SHA

Data Protection Officer TASKS

- Create data protection policies, guidelines and strategies
- Educate all members of staff on topics related to data compliance
- Implement policies throughout the organisation
- Ensure all staff members adhere to data compliance
- Conduct regular audits
- Maintain all records of data processing
- Mentor the company's data processors
- Create documents and reports for senior management

MONITOR COMPLIANCE

- Collect information to identify and analyze processing activities
- Conduct audits to ensure GDPR compliance and address potential issues

INFORM AND ADVISE

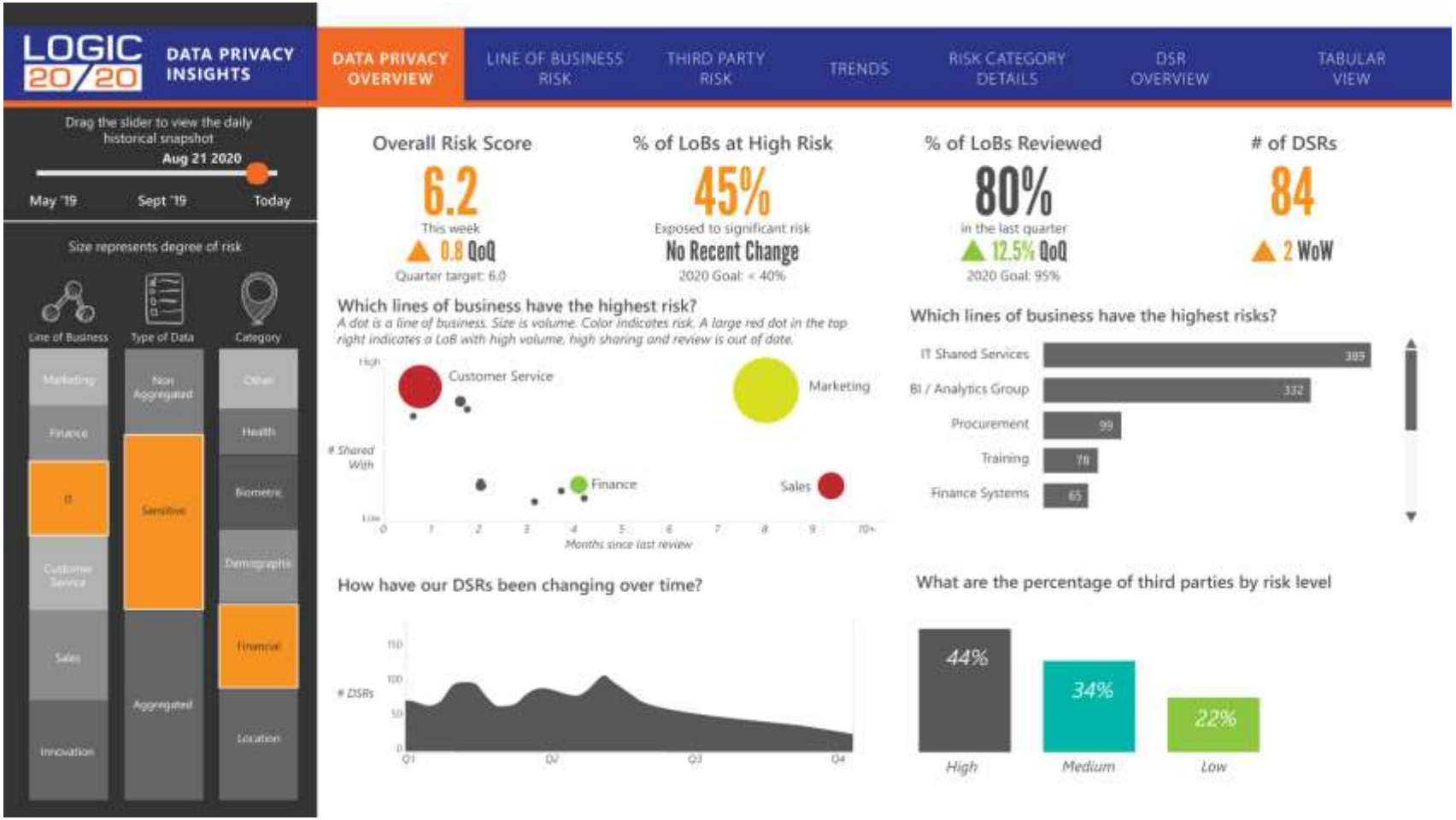
- Inform, advise and issue recommendations on data handling, e.g. for performing PIAs
- Educate the company and employees on compliance and train data handling staff

COOPERATE WITH SUPERVISOR

- Cooperate with the supervisory authority and make records available on request
- Proactively report issues with data processing, such as data breaches

ACT AS CONTACT POINT

- Act as single point of contact for inquiries by data subjects
- Provide information on data subjects' privacy related rights


LOGIC 20/20
DATA PRIVACY INSIGHTS
DATA PRIVACY OVERVIEW
LINE OF BUSINESS RISK
THIRD PARTY RISK
TRENDS
RISK CATEGORY DETAILS
DSR OVERVIEW
TABULAR VIEW
Drag the slider to view the daily historical snapshot
Aug 21 2020
May '19
Sept '19
Today
Size represents degree of risk
Line of Business
Type of Data
Category
Marketing
Finance
IT
Customer Service
Sales
Innovation
Non Aggregated
Sensitive
Aggregated
Other
Health
Biometric
Demographic
Financial
Location
Overall Risk Score
6.2
This week
0.8 QoQ
Quarter target: 6.0
% of LoBs at High Risk
45%
Exposed to significant risk
No Recent Change
2020 Goal: < 40%
% of LoBs Reviewed
80%
in the last quarter
12.5% QoQ
2020 Goal: 95%
# of DSRs
84
2 WoW
Which lines of business have the highest risk?
A dot is a line of business. Size is volume. Color indicates risk. A large red dot in the top right indicates a LoB with high volume, high sharing and review is out of date.
High
Low
Shared With
Customer Service
Marketing
Finance
Sales
0
1
2
3
4
5
6
7
8
9
10+
Months since last review
Which lines of business have the highest risks?
IT Shared Services
BI / Analytics Group
Procurement
Training
Finance Systems
389
332
99
78
65
How have our DSRs been changing over time?
DSRs
150
100
50
0
Q1
Q2
Q3
Q4
What are the percentage of third parties by risk level
44%
34%
22%
High
Medium
Low

Maturity Roadmap and Next Steps

1. Conduct periodic privacy audits Conduct periodic privacy audits
2. Define improvement and training milestones
3. Implement dashboards for real-time compliance
4. Certify DPOs and DP Champions

Artificial Intelligence - Overview

Artificial Intelligence (AI) emulates human intelligence by machines, enabling them to perform tasks such as problem-solving, learning, and decision-making. It involves algorithms, data processing, and adaptation to achieve human-like functionalities in various applications.



Increased Efficiency



Innovation and New Discoveries

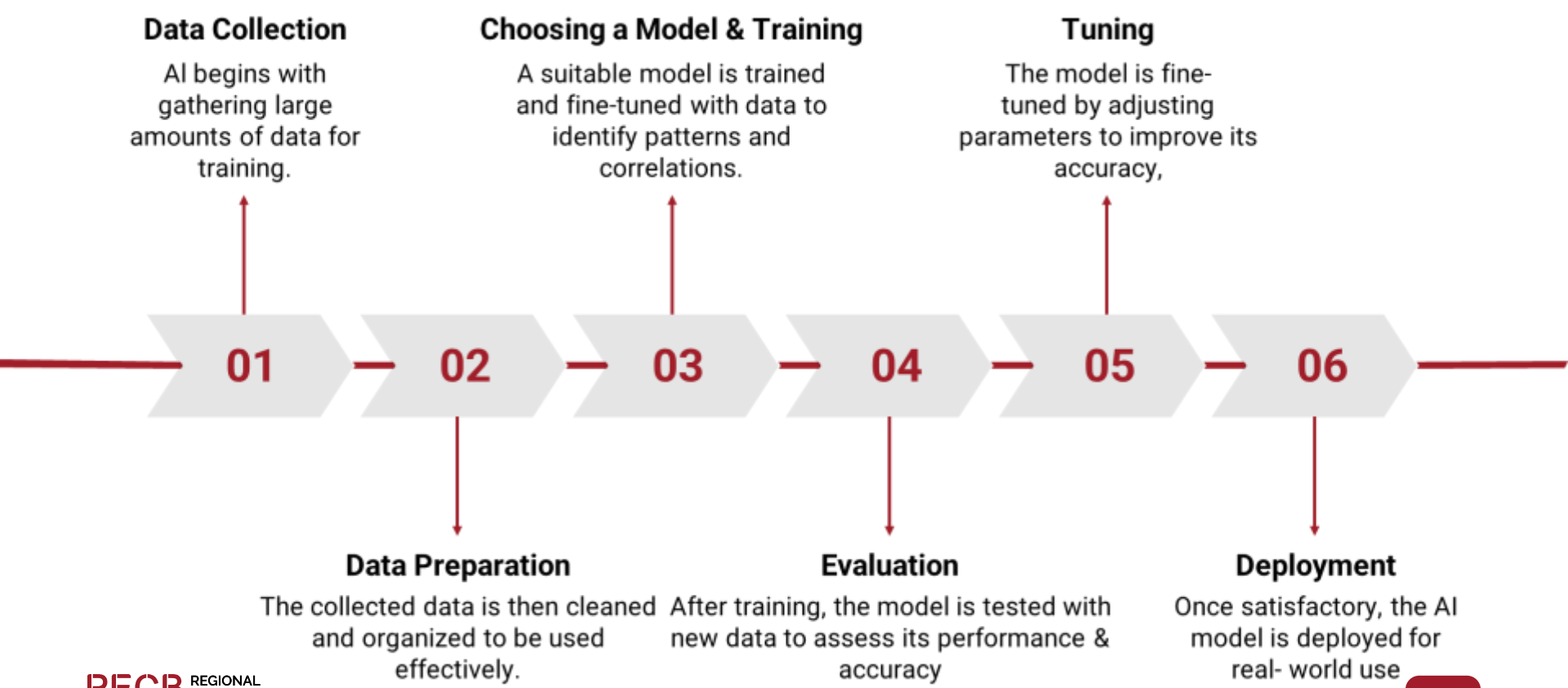


Improved Decision Making

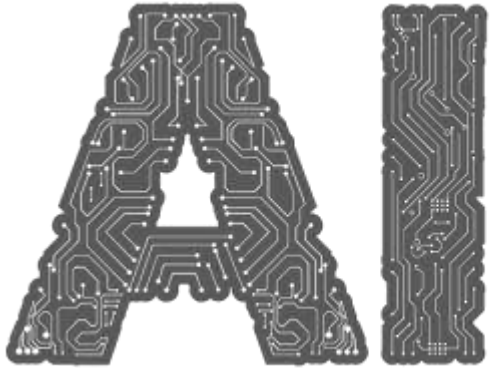


Enhanced Human Capabilities

How Does AI Work?



Why AI and Privacy Matters Now



ENGINEERING

The use of algorithms, neural networks, computers programming, and other technologies that help develop artificial intelligence (AI) applications and techniques

01 AI systems rely on vast, often personal, datasets to train models

02 Scale of data collection and inference capabilities is unprecedented

03 Traditional privacy tools (consent, anonymization) insufficient

04 Reputational, ethical, and legal risks are rising

AI and Privacy Intersection

- Privacy is no longer a passive compliance issue — it is central to AI governance.



AI and Privacy Intersection: Key Privacy Concerns

Privacy and artificial intelligence (AI) intersect at several critical points, primarily because AI relies heavily on data—often personal data—to function effectively. Here is how the two fields intersect:

Data Dependency and Personal Information

- AI relies on large datasets, often containing sensitive personal data, raising concerns about how this data is collected, used, and shared.

Risk of Re-identification

- Even anonymized data can be traced back to individuals when combined with other datasets, challenging traditional privacy measures.

Profiling and Automated Decision

- AI can analyze personal data to make predictions or decisions—such as in hiring, lending, or policing—which may affect rights and freedoms without adequate transparency or recourse.

Bias and Discrimination

- AI may reflect or amplify biases in training data, leading to unfair or discriminatory outcomes.

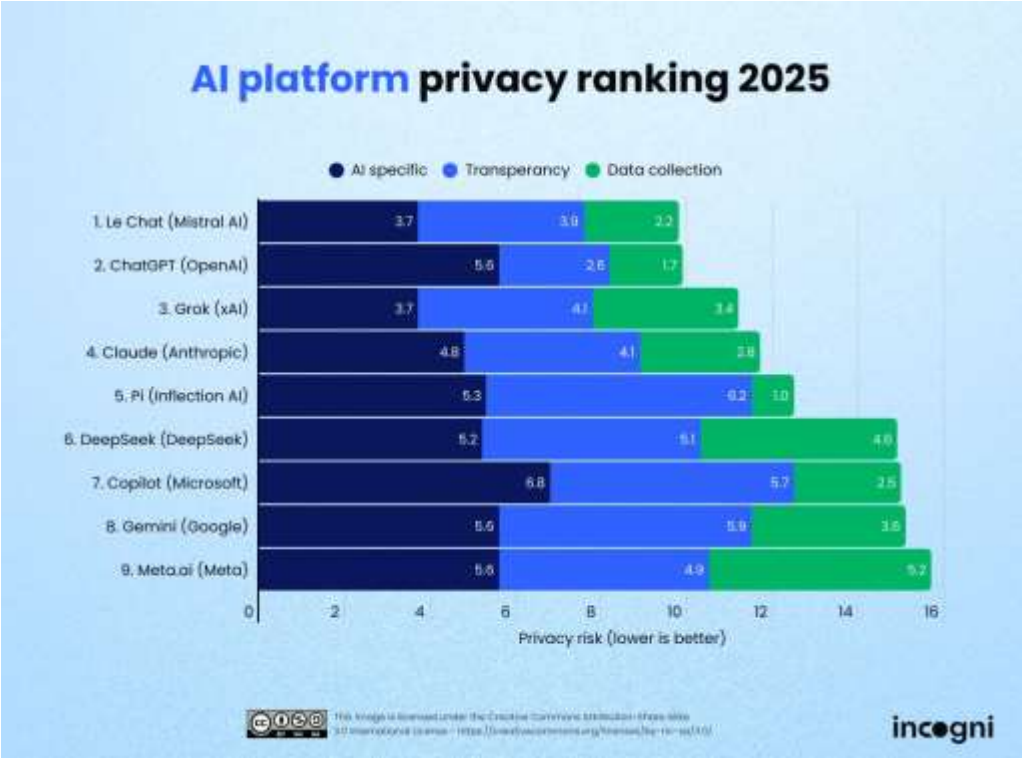
Consent and Transparency

- Due to AI's complexity, users may not fully understand how their data is used, making informed consent and data rights harder to uphold.

Legal and Ethical Frameworks

- Privacy laws increasingly regulate AI through requirements like DPIAs and human oversight, making privacy a core part of ethical AI development.

How Leading Gen AI and LLM Compare on Privacy in 2025



Source: incogni.com

Global AI & Privacy Regulation

1. **GDPR (EU):** Article 22 (automated decision-making), DPIAs, data minimization
2. **Global Shift:** OECD AI Principles, EU AI Act, U.S. Executive Orders on AI
3. **Kenya's Data Protection Act (2019):** Processing restrictions, consent, DPIA
4. **ISO/IEC 42001:2023**

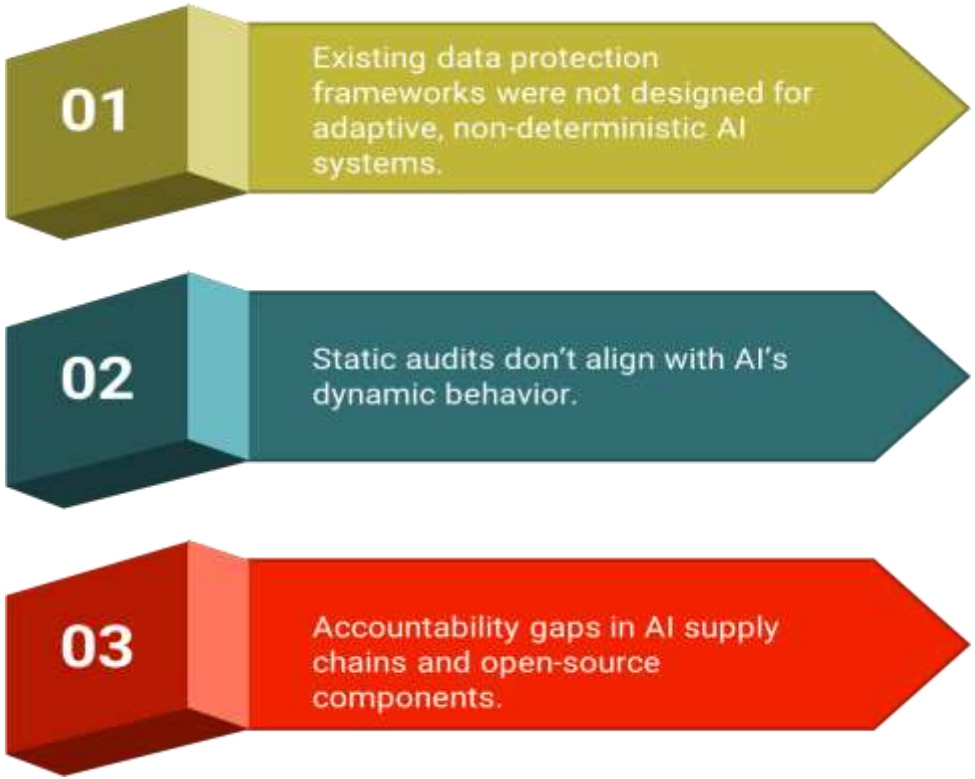
Kenya Data Protection Act (DPA)

The Kenya Data Protection Act was enacted in 2019 to align Kenya with global privacy standards like GDPR

Key Requirements of the Kenya DPA (2019)

Lawful Processing	Processing must be fair, transparent and with consent or have a valid legal basis
Data Minimization	Only data that is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
DPIAs	Required for high-risk processing activities including AI & automation
Cross-Boarder Data Transfers	Subject to adequacy or safeguards
Security Measures	Both organizational and technical safeguards
Enforcement	ODPC may issue penalties, audits, and compliance orders

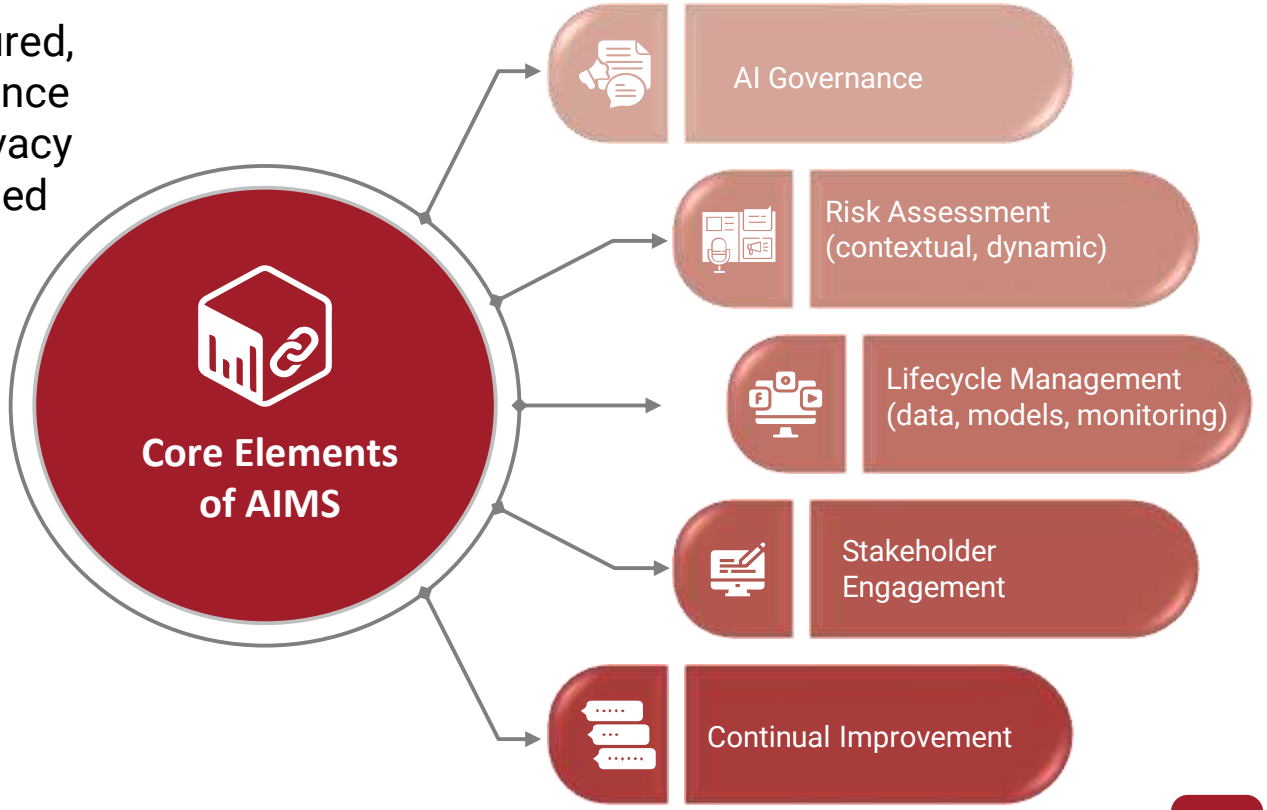
Why Traditional Compliance Falls Short



That is why a purpose-built framework like AIMS (ISO/IEC 42001) is essential.

ISO/IEC 42001– AI Management System

AIMS provides structured, lifecycle-wide governance for AI and ensures privacy principles are embedded from the ground up.



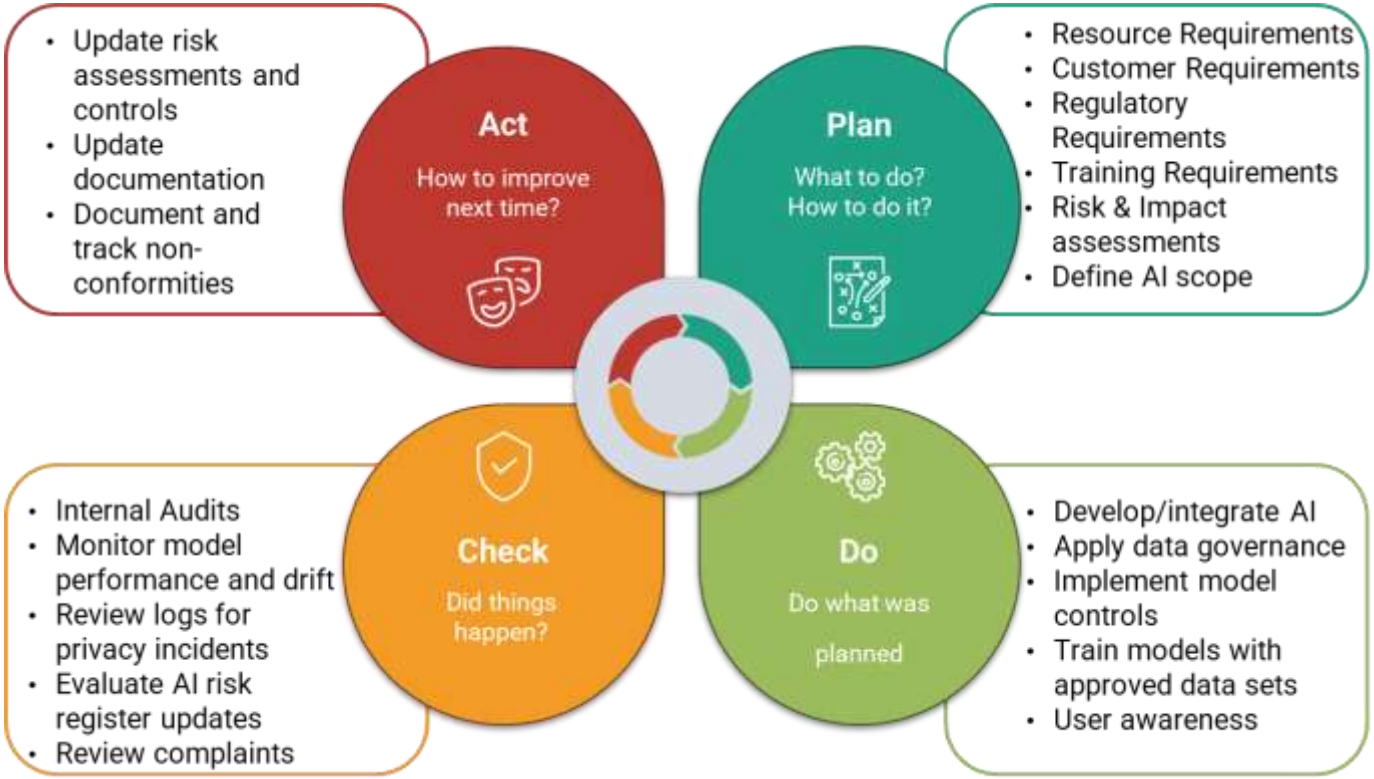
Key Benefits of Implementing AIMS



ISO/IEC 42001 Implementation Approach

1. **Establish Context**: Understand AI use cases and applicable regulations.
2. **Define Scope & Objectives**: Focus on AI systems that process personal data.
3. **Risk Assessment**: Map risks across lifecycle (data, model, outcome).
4. **Design Controls**: Ethical AI policies, bias mitigation, explainability techniques.
5. **Integrate with ISMS/DPMS**: Harmonize with existing ISO 27001/27701 controls.
6. **Monitor, Audit & Improve**: Periodic reviews, updates, and transparency reports.

ISO/IEC 42001 Implementation Approach

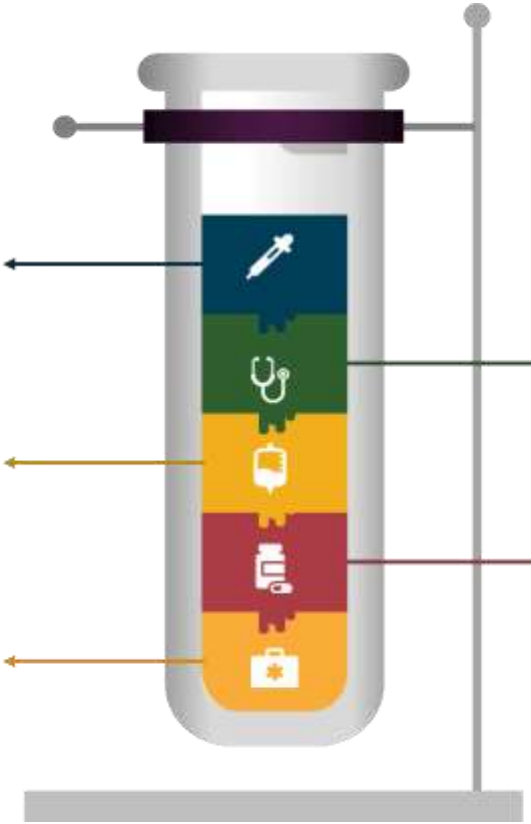


Best Practice Controls

Privacy-by-Design
Embedding privacy principles into the design and architecture of systems and business processes from the outset.

Central AI Inventory and Risk Registry
Maintain a centralized record of all AI systems, models, data sets, and their use cases.

Employee training
Ongoing role-based training on:
AI ethics, Data protection laws, Responsible data practices, Emerging regulatory frameworks



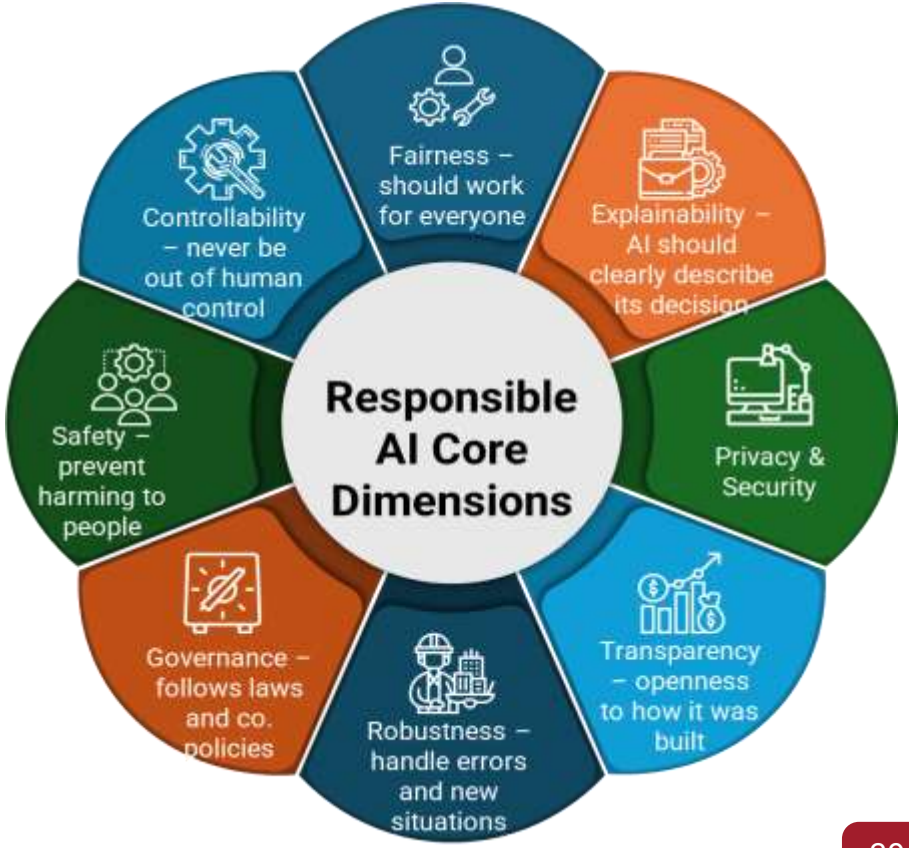
Data Protection Impact Assessments
Evaluate risks to personal data before initiating high-risk processing activities (e.g., facial recognition, profiling, automated decision-making).

Consent & Purpose Limitation Tracking Tools
Monitor whether data used in AI systems is collected with valid user consent.
Ensure data processing aligns strictly with the original stated purpose.

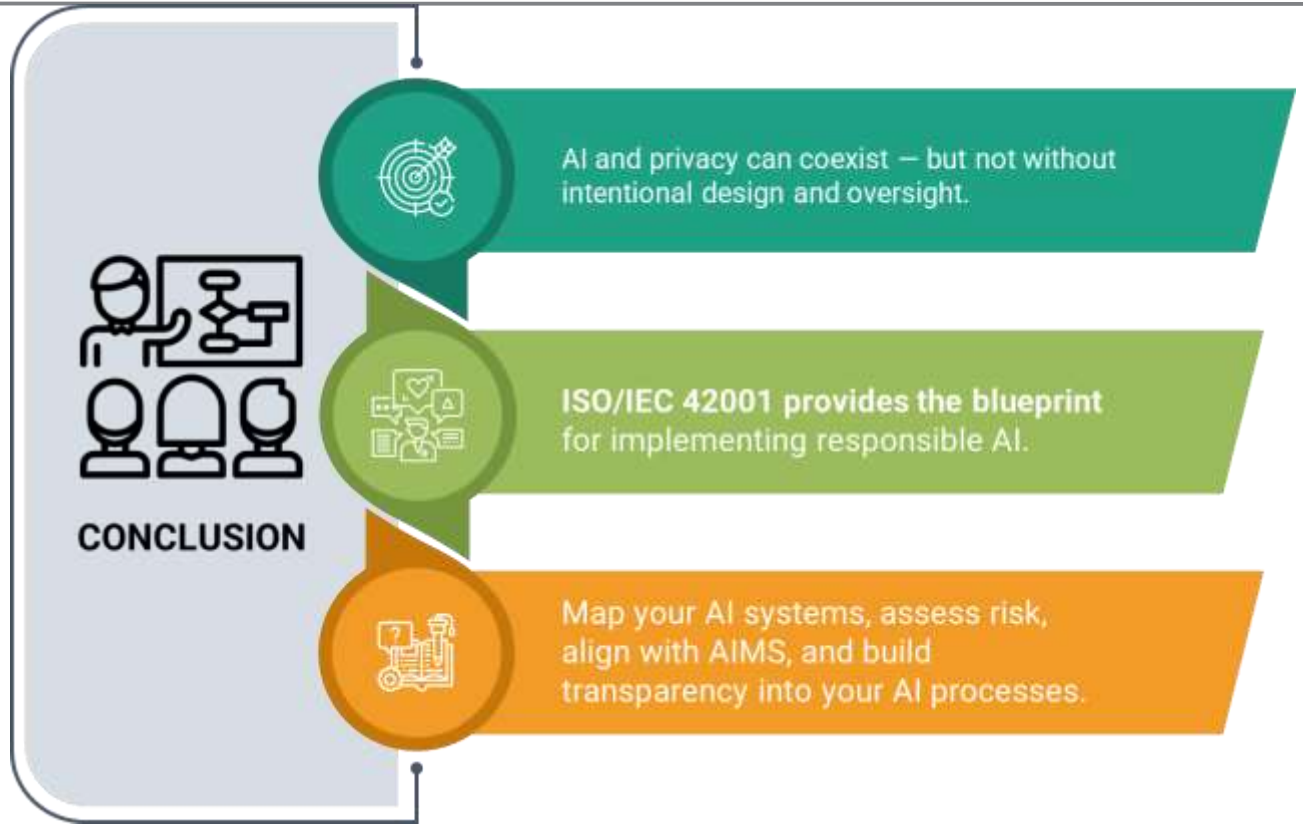
Roadmap to Responsible AI

- As AI aims to learn like humans, attention must be paid to AI Ethics, which include:
  - What computers learn, and
  - How do they learn it?

- Ensuring AI is fair, unbiased, and respects human rights, equity, and **privacy** is crucial for societal benefit.



A Forward-Looking AI Governance Strategy



Q&A Session



Contact

- Website: https://a4sonline.com/
- Phone: +234 916 820 3693
- Email: orlando@a4sonline.com

- Website: www.sentinelafricaconsulting.com
- Phone: +254 715 484888
- Email: info@sentinelafricatraining.com

For any questions or comments you can contact us below:

- support@pecb.com