Project AIDA: An Open-Source AI Governance Framework for Kenyan SMEs

Empowering Kenyan SMEs to innovate responsibly under the Data Protection Act

By
Obed M. Nyandiri
Founder & CEO, AI For Us
Independent Researcher in AI Governance and Data Protection

Date

October 13 2025

Version 1.0

Abstract

The rapid uptake of accessible artificial intelligence (AI) tools by Kenyan small and medium-sized enterprises (SMEs) presents both a generational opportunity and an escalating legal risk. While solutions like WhatsApp chatbots, generative content tools, and AI-driven analytics are revolutionizing local business operations, their integration often occurs without understanding the legal obligations under Kenya's Data Protection Act, 2019 (DPA). This creates a dangerous compliance gap, further compounded by SMEs' limited resources and the inadequacy of existing tools built for foreign or corporate contexts.

Project AIDA (Artificial Intelligence Data Compliance) offers a tailored, open-source compliance framework designed specifically for Kenyan SMEs adopting AI. This white paper provides a simplified legal primer, a practical toolkit (RoPA, Privacy Policy, DPIA, Risk Checklist), and a relatable fictional case study to guide implementation. By demystifying legal requirements and offering actionable tools, Project AIDA empowers SMEs to innovate responsibly while reducing exposure to enforcement actions by the Office of the Data Protection Commissioner (ODPC).

Chapter One. The Kenyan AI Opportunity

1.1 Introduction: A Technological Tipping Point for SMEs

Kenya's small and medium-sized enterprises (SMEs) which constitute over 90% of the country's private sector and contribute approximately 40% to the GDP are undergoing a rapid digital transformation. This shift is driven not only by mobile penetration and fintech innovation, but increasingly by the emergence of accessible artificial intelligence (AI) tools. Once limited to academia or large corporations, AI is now being deployed by SMEs across sectors like retail, agriculture, education, logistics, fashion, and e-commerce.

Tools such as WhatsApp business chatbots, AI-powered inventory and financial management software, automated customer service bots, and generative content tools like ChatGPT and DALL·E are becoming commonplace. These technologies are affordable, easy to deploy, and often do not require specialized technical skills. For many SMEs, this democratization of AI presents a rare opportunity to leapfrog traditional growth constraints reducing costs, improving customer engagement, streamlining operations, and accessing new markets.

But this opportunity is not without risk.

1.2 What Makes AI Attractive to Kenyan SMEs?

✓ Accessibility

AI tools have become increasingly plug-and-play. WhatsApp chatbots can be deployed via platforms like Twilio or Gupshup without a developer. Inventory forecasting tools powered by machine learning are bundled into apps like QuickBooks or Zoho. Image-generation and content-creation tools can now be used via mobile phones.

✓ Affordability

Unlike legacy enterprise systems, modern AI tools operate on flexible pricing models, sometimes even free for basic use. This has made AI adoption economically feasible for cash-strapped SMEs.

✓ Competitive Necessity

Kenyan consumers are digital-first. Mobile money, social commerce, and real-time communication are the norm. Businesses that don't respond quickly, personalize offerings, or provide 24/7 support risk losing out to more AI-savvy competitors.

✓ Sector-Specific Use Cases

- **Agriculture**: AI is being used to predict weather patterns, monitor crop health, and optimize supply chains.
- **Retail & Fashion**: Recommendation engines and demand forecasting tools help with stock planning and personalization.
- **E-commerce**: AI chatbots are automating order-taking and after-sales service on platforms like WhatsApp and Instagram.

- **Education**: Tutoring bots and adaptive learning tools are supplementing classroom instruction, especially in remote areas.

In short, AI is no longer an emerging trend for Kenyan SMEs it is becoming a core part of doing business.

1.3 The Digital Economy Push: Policy and Infrastructure Support

The Kenyan government has made significant strides in digital infrastructure and policy to support this evolution:

- **Digital Economy Blueprint (2019)**: Kenya's national framework highlights AI as a key driver of productivity and development. It encourages responsible innovation while advocating for safeguards like data protection, digital rights, and inclusive access.
- **Konza Technopolis & Ajira Digital**: National programs are training youth in AI-related skills and promoting tech-driven entrepreneurship.
- **Broadband & Mobile Penetration**: As of 2025, Kenya boasts over 64 million mobile subscriptions and an internet penetration rate exceeding 85%. Most SME owners run operations from smartphones, making AI tools integrated into messaging apps (e.g., WhatsApp bots) highly attractive.

This national digital momentum creates fertile ground for AI adoption, but it also exposes SMEs to regulatory obligations they often don't understand or even know exist.

1.4 The Unseen Compliance Risk

Despite the enthusiasm for AI, there is a glaring blind spot: data protection compliance. Every time an SME installs a chatbot, uses customer data to train a model, or relies on automated decision-making, it is engaging in personal data processing under Kenya's Data Protection Act, 2019 (DPA).

Unfortunately, most SMEs:

- Do **not realize** that tools like chatbots or analytics platforms may fall under regulatory scrutiny.
- Do **not understand** legal concepts like *lawful basis for processing*, *privacy by design*, or *automated profiling*.
- Do **not have** the resources to hire legal counsel or conduct formal Data Protection Impact Assessments (DPIAs).
- May be using AI tools built outside of Kenya (e.g., OpenAI, Meta, Google) without reviewing their privacy implications or compliance risks.

This gap between **AI adoption and regulatory awareness** creates a situation where SMEs are unknowingly exposed to penalties under the DPA despite acting in good faith and using tools to grow their businesses.

1.5 Active Enforcement by the ODPC

Kenya's Office of the Data Protection Commissioner (ODPC) is no longer in its infancy. As of 2025, the ODPC has issued multiple **penalties, enforcement notices, and compliance audits** across sectors, including education, healthcare, retail, and fintech.

Key facts:

- The DPA imposes fines of **up to KES 5 million or 1% of annual turnover**, whichever is higher.
- The ODPC has specifically warned against unauthorized use of personal data, especially in marketing and AI automation contexts.
- SMEs, despite their size, are not exempt from the law. In fact, the ODPC has made it clear that ignorance is not a defense.

This growing enforcement landscape places SME owners at real and immediate risk especially those adopting AI tools with no legal or governance framework in place.

1.6 The Risk of Algorithmic Harm

Beyond legal compliance, AI systems, particularly those using automation and predictive analytics, carry ethical and operational risks that SMEs are often unprepared to handle:

- **Algorithmic Bias**: A chatbot trained on flawed or biased data can deliver discriminatory outcomes (e.g., profiling customers based on name or location).
- **Automated Decision-Making**: An AI deciding who qualifies for a discount or refund without human oversight could lead to unfair outcomes or reputational damage.
- **Data Sovereignty**: Many AI tools store or process customer data in foreign jurisdictions, raising questions about data control, privacy, and legal recourse.

These risks lead to customer backlash, loss of trust, legal action, or even intervention by the ODPC.

1.7 Why a Kenyan SME-Focused AI Governance Framework Is Essential

The rise of AI in Kenyan SMEs is both **inevitable** and **transformative**. However, without tailored support, most businesses are flying blind into a high-risk regulatory environment.

The current compliance options are misaligned:

- **Large enterprise platforms** like OneTrust are expensive and overly complex.
- **Generic GDPR templates** found online do not reflect Kenyan law and ignore AI-specific risks.
- **Top-tier legal advice** is financially out of reach for most SMEs.

What's missing is a **context-specific, affordable, and usable compliance framework** designed for the Kenyan SME reality a framework that:

- Respects their time and resource constraints.
- Translates legal requirements into business-friendly language.
- Focuses specifically on the **intersection of AI use and data protection**.
- Demonstrates **good-faith compliance** in the eyes of the ODPC.

Chapter Two: The Compliance Challenge

2.1 Legal Obligations under Kenya's Data Protection Act (2019)

Kenya's Data Protection Act (No. 24 of 2019) (the *DPA*) sets forth a comprehensive legal framework governing the processing of personal data by data controllers and processors. SMEs adopting AI tools must understand and comply with obligations under this statute. Key legal requirements include:

Obligation	Description
Lawful, fair, transparent processing	Any processing of personal data must be lawful, fair, and transparent to the data subject. The data subject must be informed about who is processing their data, for what purposes, and under what lawful basis. Kenya Law+1
Purpose limitation	Data must be collected for specified, explicit, and legitimate purposes. Further processing must be compatible with those purposes. Kenya Law+1
Data minimisation	Only data which is adequate, relevant, and limited to what is necessary should be collected. Unnecessary or excessive data is not permitted. Kenya Law+1
Accuracy	Reasonable steps must be taken to ensure data is accurate and kept up to date; erroneous data should be corrected or erased without delay. Kenya Law
Storage limitation	Data must be stored no longer than is necessary for the purpose it was collected, unless retention is required by law or other justified purposes. Kenya Law+1
Security / Integrity	Controllers/processors must implement appropriate technical and organizational measures to safeguard data (against loss, unauthorized access, disclosure, etc.). This includes when designing or selecting systems ("data protection by design/default"). Kenya Law+1
Data Protection by Design and by Default	When determining how to process data, organizations must integrate necessary safeguards, consider risks, limit default data collection, pseudonymise or encrypt data, etc. Kenya Law+1
Registration of controllers/processors	Data controllers and processors must register with the ODPC under the "Registration of Data Controllers and Data Processors Regulations, 2021" (Regulations). Failure to register when required is an offense. Kenya Law+2Registered Law Firm in Kenya+2
Transfers outside Kenya	Cross-border transfers are permitted only if adequate safeguards are in place (or explicit consent, etc.), or in cases provided under law. Kenya Law

Rights of data subjects	Data subjects have rights to access, correct, erase, object, receive portability of their data, etc. Kenya Law+1
Breach notification	The Act requires that data controllers (and processors) notify the ODPC and the affected individuals in a timely manner when personal data breaches occur. Kenya Law+1

2.2 Key Areas of Ambiguity and Risk for SMEs

Many SMEs are unaware or uncertain about how the following apply in practice these are high-risk areas that compliance frameworks must address:

1. **Automated Decision-Making & Profiling**
   AI systems often perform automated profiling or make decisions without human oversight (e.g., deciding creditworthiness, eligibility). These practices trigger special scrutiny and may require DPIAs (Data Protection Impact Assessments) under Kenyan law. The SME must assess if their AI tools perform any "high risk" processing. Unfortunately many SMEs do not.

2. **Sensitive Personal Data**
   The Act defines *sensitive personal data* (health, biometrics, religion, etc.). Processing such data requires stronger safeguards, more explicit consent, and has heavier legal consequences for misuse. SMEs may inadvertently collect sensitive data (e.g., via health-related AI tools) without realizing. ICNL+1

3. **Consent: Validity and Scope**
   Consent must be freely given, specific, informed, and an explicit lawful basis. Using vague terms in privacy policies, bundling consent with other terms, or failing to inform data subjects about third-party processors or cross-border transfers can make consent invalid. SMEs often rely on "opt-in" mechanisms without sufficient detail.

4. **Cross-Border Data Transfers**
   Many AI tools are cloud based or hosted abroad. If customer data is stored or processed outside Kenya, the SME must ensure appropriate legal safeguards (contractual, agreements, or consent) are in place. Otherwise, they risk violating the DPA.

5. **Security, Breach Handling & Accountability**
   SMEs may not have internal policies for incident response, auditing, encryption, or regular risk reviews. They often use off-the-shelf AI tools or third-party platforms without verifying security practices. A breach could lead to regulatory action, reputational harm, and financial loss.

6. **Registration with ODPC & Administrative Compliance**
   Some SMEs may not realize they need to formally register as data controllers/processors. Others may not maintain required documentation (e.g., record of processing activities, logs of consent, policies) for audits. Non-registration or incomplete documentation is a common source of ODPC enforcement.

7. **Enforcement Notices and Penalties**
   There is risk not just of fines, but of ODPC issuing enforcement notices, orders to cease processing, image/publication removal, and even regulatory referrals (e.g. urging other regulators to revoke licenses in certain sectors).

2.3 Recent Enforcement and Case Examples

To illustrate that these are not hypothetical risks, below are real cases and enforcement actions by ODPC that show how non-compliance is being penalised:

Case	Nature of Breach	Penalty / Finding
Mulla Pride Ltd (Digital Lender: KeCredit & Faircash)	Used names and contact information obtained from third parties; sent threatening messages / phone calls to individuals who had not consented. Kenya News+2Switch News+2	Lessee penalty: **KES 2,975,000** for violation. Kenya News+1
Private School	Posted images of minors on social media without parental consent (images = personal data; minors require more protections) Clyde & Co.+1	Penalty of KES **4,550,000**. Clyde & Co.+1
Restaurant in Nairobi	Posted image of a data subject on social media without consent. Clyde & Co.	Penalty of ~ **KES 1,850,000**. Clyde & Co.
Whitepath & Regus Kenya	Accessed mobile phone contacts, sent unsolicited / unwarranted messages; failure to respond to enforcement notices. allAfrica.com+1	Fines: up to **KES 5,000,000** each. allAfrica.com+1

These cases show ODPC is enforcing especially around **consent**, **use of contact data**, **use of images / minors**, **unauthorised data access**, and **failure to respond / comply** with notices.

2.4 Penalties, Sanctions, and Legal Consequences

Understanding the scale and types of consequences helps SMEs appreciate risk. Key exposures include:

- **Administrative fines**: Under the DPA, ODPC may impose fines up to **KES 5,000,000** for failure to comply with enforcement notices or other serious breaches. Clyde & Co.+1

- **Criminal liability**: Certain breaches may lead to criminal penalties (including imprisonment) under Part VI of the Act, especially for failure to register, unlawful processing, or false statements. kioi.co.ke+1
- **Reputational damage**: Public penalties or notices diminish customer trust especially when linked to misuse of personal data or exposure of minors, sensitive data.
- **Business continuity risk**: Enforcement notices may force businesses to suspend certain data-driven operations (e.g. AI chatbots that engage in automated processing), or to re-engineer systems at cost. Non-cooperation may attract stricter measures, possibly referrals to other regulatory bodies. E.g. ODPC urging revocation of licenses for errant digital lenders. Tuvuti

2.5 Why SMEs Often Fail to Comply

The following factors explain why many Kenyan SMEs are not fully compliant, even when aware:

1. **Lack of legal literacy**
   Terms like "lawful basis," "data subject rights," "processing agreements," or "profiling" are often not understood in business terms. SMEs tend to treat data simply as a resource, not with the obligations it carries under law.
2. **Cost of specialized legal or compliance advice**
   Hiring lawyers familiar with both AI and Kenyan data protection is expensive. DIY templates often miss local specifics and AI risks. SMEs may under-invest in compliance or do minimal compliance superficially.
3. **Lack of documentation & internal processes**
   Many SMEs do not maintain records of processing (RoPA), do not perform DPIAs when required, do not have valid consent records, or do not have clear policies for breach handling. Without documentation, even good-faith efforts may be hard to demonstrate.
4. **Third-party tools and opaque supply chains**
   Many AI tools, chatbots, cloud services are built by third parties. SMEs may not fully understand or control where data is stored, how the tool processes data, or whether the service provider is compliant. Contracts are often overlooked.
5. **Absence of proactive auditing and risk assessment**
   SMEs often only respond when something goes wrong. They frequently lack regular risk assessments, threat modelling, or internal reviews of AI workflows and data practices.
6. **Dynamic changes in AI and regulation**
   AI tools evolve fast. Features like automated decision-making, data sharing, model retraining, etc., may introduce new legal risks over time. SMEs may deploy a tool today under one risk assessment, but later changes may shift its risk profile, without their realizing.

2.6 Consequences of Non-Compliance in the AI Context

When SMEs use AI without aligning with these obligations, the possible harms and exposures multiply:

- **Regulatory risk**: Fines, enforcement, revocations, criminal exposure as noted above.
- **Ethical / reputational harm**: Discriminatory or biased AI outputs damage brand trust; misuse of personal data (images, voice, profile) can lead to public backlash.
- **Operational risk**: If a breach occurs (data leak, unauthorized access), the cost of remedying is high not just in money but in loss of customer loyalty, legal claims, possibly civil suits.
- **Legal exposure via third-party liabilities**: If data is shared via AI tool providers, or via subcontractors, the SME may face liability if those parties' practices violate the Act. Poor contracts or lack of due diligence increases this risk.

2.7 Summary: Where SMEs Need Compliance Focus

To address the compliance challenge, SMEs must prioritize:

1. Understanding which AI use-cases in their operations trigger legal obligations (e.g., profiling, automated decisions, chatbots handling personal/ sensitive data, data transfers abroad).
2. Ensuring consent mechanisms are valid and documented.
3. Registering as a data controller/processor if required by law/regulations.
4. Maintaining internal documentation: Records of Processing Activities (RoPA); privacy policies; data protection impact assessments; breach logs.
5. Instituting technical & organisational safeguards: encryption, pseudonymisation, access controls, regular audits.
6. Designing privacy by design/default into systems: limiting data collection, minimizing storage, building in opt-outs, etc.
7. Preparing for enforcement: creating response protocols, understanding how to respond to ODPC notices, knowing channels for complaints or audit.

The rapid integration of AI technologies presents an unprecedented opportunity to transform Kenyan SMEs, unlocking innovation, efficiency, and competitive advantage. However, this digital leap exposes these businesses to complex and often overlooked regulatory risks under Kenya's Data Protection Act, 2019 risks that, if unmanaged, could result in severe financial penalties and irreversible reputational damage. Given the limited resources and legal expertise typical of SMEs, a tailored, pragmatic, and accessible governance framework is not just beneficial it is essential to enable responsible AI adoption that safeguards both enterprise growth and individual privacy rights. This white paper delivers that framework: a practical, Kenyan-contextualized blueprint empowering SMEs to confidently innovate within the bounds of the law, fostering a resilient, inclusive, and future-ready digital economy.

Chapter Three: A Practical Framework

3.1 Introduction

Kenyan SMEs operate at the confluence of opportunity and risk in adopting AI-driven tools. While AI promises efficiency, customer engagement, and innovation, it also exposes SMEs to complex data protection obligations that can jeopardize their operations if unmet.

This practical framework offers an **SME-focused, open-source compliance toolkit**, designed to be:

- **Legally sound** under Kenya's Data Protection Act (2019) and relevant regulations,
- **Simple and accessible** for non-legal experts,
- **Cost-effective and scalable**, avoiding expensive consultancy or enterprise-grade software,
- **AI-specific**, addressing the novel risks of automated decision-making, algorithmic bias, and cross-border data processing.

3.2 Framework Components

The framework revolves around four essential pillars of compliance tailored to SME realities and AI use cases:

Pillar	Purpose	SME Benefit
1. Records of Processing Activities (RoPA)	Formal documentation of all personal data processing operations within the business.	Demonstrates compliance, aids audits and risk identification.
2. Update Privacy Policy	Transparent communication to customers about data collection, use, rights, and AI-specific disclosures.	Builds trust, ensures lawful, informed consent.
3. Data Protection Impact Assessment (DPIA)	Risk assessment tool for AI applications that process personal data with high risks (e.g., profiling, automated decisions).	Identifies and mitigates AI-related privacy and legal risks early.
4. AI-Specific Risk Checklist	Practical checklist highlighting AI risks such as algorithmic bias, automated decision-making, data accuracy, and cross-border data flows.	Ensures AI risks are comprehensively addressed without technical overload.

3.3 Records of Processing Activities (RoPA)

3.3.1 Purpose and Legal Basis

Under Section 17 of the Kenyan Data Protection Act, all data controllers must maintain a record of their personal data processing activities. The ODPC mandates this as a basic accountability measure.

RoPA serves as a "living document" that captures:

- Types of data processed,
- Processing purposes,
- Data categories and sources,
- Recipients and third parties,
- Data retention periods,
- Security measures implemented,
- Legal basis for processing (e.g., consent, contract).

3.3.2 Key Features for SMEs

- **Simple Template**: Use a spreadsheet or document with clearly defined fields.
- **Regular Updates**: Review at least quarterly or on addition of new AI tools.
- **Integration with AI Tools**: Clearly specify if AI features involve automated profiling or decision-making.
- **Focus on Purpose Limitation**: Ensure all processing has a defined, legitimate purpose.

3.3.3 Benefits

- Demonstrates compliance readiness to ODPC inspectors.
- Helps SMEs identify compliance gaps.
- Facilitates breach response and data subject access requests.

3.4 Privacy Policy Updates

3.4.1 Importance of Transparency

Kenyan law emphasizes transparency; customers must know what data is collected, how it is used, and their rights. With AI, transparency must include:

- Explanation of automated decision-making or profiling.
- Information about data shared with third-party AI service providers.
- Details on international data transfers if AI is cloud-based.

3.4.2 Content Guidelines

The updated privacy policy should clearly include:

- **Data Controller Identity and Contact**: The SME's legal name and contact for data protection queries.
- **Data Collection Purposes**: Clear description of what data is collected and why.
- **Legal Basis for Processing**: e.g., consent, contract necessity.
- **Data Subject Rights**: Access, correction, erasure, objection, portability.
- **Automated Decision-Making Clause**: Explicitly disclose if AI makes decisions impacting customers.
- **Data Sharing and Cross-Border Transfers**: Specify third parties, safeguards (e.g., Standard Contractual Clauses), and transfer countries.
- **Security Measures**: Outline how data is protected.
- **Breach Notification Procedures**: Explain that affected individuals will be informed as per law.
- **Consent Withdrawal**: How customers can withdraw consent.
- **Policy Updates**: How changes will be communicated.

3.4.3 Language and Accessibility

- Use **plain language**, avoiding legal jargon.
- Provide the policy on websites, apps, and where data is collected.
- Consider translations if targeting non-English speaking customers.

3.5 Data Protection Impact Assessment (DPIA)

3.5.1 When is a DPIA Required?

The DPA and global best practices (aligned with GDPR principles) require DPIAs where data processing is "likely to result in high risk" to individuals' rights and freedoms. AI applications involving:

- Automated decision-making with legal or significant effects,
- Large-scale processing of sensitive personal data,
- Systematic monitoring of public areas or individuals,
- New technologies or novel uses of data.

Examples for SMEs include AI chatbots making decisions on credit, eligibility, or personalized pricing.

3.5.2 DPIA Process Steps

1. **Describe the processing**: What AI systems are used? What data is involved?
2. **Assess necessity and proportionality**: Is AI processing necessary? Can risks be minimized?
3. **Identify risks to individuals**: Potential for bias, discrimination, inaccurate profiling, loss of privacy.
4. **Propose mitigation measures**: Transparency, human oversight, security controls, bias testing.
5. **Document and review**: Formal report reviewed by SME leadership or compliance officer.

3.5.3 SME-Friendly DPIA Template

The framework includes a simplified, guided DPIA form tailored for Kenyan SMEs with AI:

- Step-by-step questions,
- Explanations of technical terms,
- Guidance on risk ratings and mitigation prioritization.

3.6 AI-Specific Risk Checklist

3.6.1 Why an AI-Specific Checklist?

Standard data protection checklists miss AI's unique risks. This checklist covers:

- **Algorithmic bias and fairness**: Are models tested for discrimination?
- **Automated decision-making transparency**: Can decisions be explained to users?
- **Data accuracy**: Is training data up to date and representative?
- **Consent for profiling**: Is explicit consent obtained for profiling activities?
- **Data minimization**: Is only necessary data collected for AI purposes?
- **Security controls**: Are AI tools secure from tampering or data leaks?
- **Third-party AI services**: Are contracts in place ensuring compliance?
- **Cross-border data flows**: Are transfers lawful and safeguarded?
- **Data subject rights enablement**: Can users exercise rights easily?
- **Breach readiness**: Are AI-related breach scenarios covered in incident plans?

3.6.2 Usage Guidelines

- SMEs should complete the checklist **before** deploying new AI tools and **annually** thereafter.
- The checklist doubles as an internal audit tool and preparation for external inspections.
- Helps SMEs prioritize remediations based on risk severity.

3.7 Implementation Roadmap

To operationalize this framework, SMEs should:

Step	Action
1. Awareness & Training	SME owners and managers review the white paper and framework; undertake basic compliance training.
2. Inventory AI Tools & Data	Catalogue AI tools in use, data processed, and functions performed.
3. Develop RoPA	Create or update Records of Processing Activities reflecting AI-driven processing.
4. Update Privacy Policy	Revise the privacy policy incorporating AI disclosures; publish and communicate it.
5. Conduct DPIAs	Perform Data Protection Impact Assessments for high-risk AI tools or processes.

6. Complete AI Risk Checklist	Conduct a thorough risk review addressing AI-specific concerns and mitigation.
7. Implement Remediation	Address identified gaps—technical, organizational, or contractual.
8. Register with ODPC	Confirm registration status and renew as required.
9. Monitor & Review	Establish quarterly reviews and update documentation as systems or regulations evolve.
10. Incident Response Planning	Prepare breach notification procedures, assign responsible persons, and train staff.

Use the pillars templates, attached with this document; the Appendixes

Chapter Four: Case Study: Mavazi Millan

To illustrate how this framework works in practice, consider the case of **Mavazi Millan**, a Kenyan SME operating in the e-commerce space.

Business Profile

Mavazi Millan is a small, Nairobi-based online fashion retailer founded by a young entrepreneur, Wambui Kamau. The business sells affordable, stylish clothing through its website and processes customer orders via a WhatsApp chatbot integrated with Meta's Business API. The chatbot collects names, phone numbers, delivery addresses, and order details, and it offers personalized product suggestions based on previous purchases.

As Wambui scales her operations, she is unknowingly processing large volumes of personal data. Yet, like many SMEs, she has no formal data protection measures in place. When a customer inquires about how their data is used, she realizes she may be exposed to compliance risks under Kenya's **Data Protection Act, 2019** (DPA).

Step-by-Step Use of the Project AIDA Toolkit

Mavazi Millan uses the Project AIDA framework to bring the business into alignment with the DPA without hiring a lawyer or external consultant. Here's how:

Step 1: Understand the Legal Landscape (White Paper)

Wambui reads the white paper provided in the Project AIDA toolkit. It helps her understand three key obligations under the DPA:

- She must have a lawful basis for collecting and using customer data.
- She must implement data protection by design, especially for tools like her AI-powered chatbot.
- She must be able to demonstrate accountability if audited by the Office of the Data Protection Commissioner (ODPC).

The white paper breaks this down in simple language, helping her grasp what's required without the need for legal training.

Step 2: Complete the RoPA (Appendix A)

Wambui uses the Record of Processing Activities (RoPA) to document:

- What data is collected (e.g., name, contact, order history)
- Why it is collected (e.g., order fulfillment, customer engagement)
- Where the data is stored (e.g., WhatsApp Business cloud, backup in Google Drive)
- Who has access (e.g., herself, one part-time staff member)

This simple but structured record helps her meet DPA Article 25 requirements and prepares her for a potential audit by the ODPC.

Step 2: Update the Privacy Policy (Appendix B)

Using the editable AI-Centric Privacy Policy Template, Wambui customizes the document to reflect:

- What data the chatbot collects
- How the data is stored and used (e.g., for fulfilling orders and personalizing suggestions)
- The legal basis for processing (e.g., consent and legitimate interest)
- The rights of customers under the DPA

She posts the new Privacy Policy on her website and links to it from the WhatsApp chatbot's welcome message, ensuring transparency from the first interaction.

Step 3: Conduct a DPIA (Appendix C)

Wambui fills out the Data Protection Impact Assessment (DPIA) form, identifying the risks associated with using AI:

- Customers may not realize their data is being profiled for personalized suggestions.
- There is a small chance of algorithmic bias, such as suggesting products based on assumptions about gender or purchasing habits.

With guidance from the template, she outlines mitigation measures:

- Clear disclosures in the Privacy Policy
- A manual review option for customer complaints
- Regular checks on chatbot performance and suggestions

This demonstrates her proactive approach to minimizing harm and shows accountability in decision-making.

Step 5: Use the AI Risk Checklist (Appendix D)

Finally, Wambui reviews the AI Risk Checklist to ensure ongoing compliance. She confirms:

- The chatbot does not make automated decisions with legal or significant effects (e.g., denying service).
- There is a process to handle data access and deletion requests.
- All AI use is documented and regularly reviewed.

Outcome

In just under two weeks, Mavazi Millan has transformed from a high-risk SME to a compliance-aware, privacy-conscious business. If ever audited, Wambui can now show:

- A written policy
- Documented risk assessments
- Clear records of data processing
- Good-faith effort to protect her customers

This significantly reduces her exposure to fines and builds customer trust a competitive edge in the digital economy.

Conclusion & A Call for Collaboration

Kenya stands at a pivotal moment in its digital transformation journey. The rapid adoption of AI tools by small and medium enterprises signals immense opportunity but also significant regulatory risk. Without accessible, practical guidance, many SMEs will unknowingly fall afoul of data protection laws, exposing themselves to penalties that could derail innovation, livelihoods, and trust.

Project AIDA exists to prevent that outcome.

This framework is built on a single, powerful belief: ***responsible innovation is not only possible it is necessary***. SMEs should not be forced to choose between growth and compliance. With the right tools, they can do both. By translating complex legal requirements into practical, localized, and freely available resources, Project AIDA offers a way forward that is grounded, affordable, and effective.

The white paper and attached toolkit have been developed specifically for the Kenyan SME context. They are:

- **Open-source**
- **Adaptable**
- **Published under a Creative Commons Attribution 4.0 International License**

This means any individual, organization, or institution is free to **use, modify, share, and build upon** these materials as long as proper credit is given.

We Invite You to Collaborate

This is Version 1.0 of Project AIDA. It is a starting point not the final word.

We are actively seeking feedback from:

- **SME owners** who want to share their experiences with AI tools
- **Legal and data protection professionals** who can offer peer review
- **Policy institutions and academic researchers** focused on digital rights and tech governance
- **Technologists and designers** who can help improve usability and accessibility
- **Translators and local champions** who can help localize this work for different regions, sectors, or languages

Together, we can improve this framework, keep it current, and extend its impact across industries and borders. We are especially interested in partnerships that help tailor the toolkit for underserved communities including rural businesses, informal traders, and youth-led startups.

Let's Build a Safer AI Future, Together

If you believe that innovation should not come at the cost of privacy, and that good governance should be within reach for every entrepreneur then we invite you to engage.

Use the tools. Improve them. Share them. Tell us what's missing.

Together, we can build a digital economy where growth is responsible, rights are respected, and no business is left behind.

Contact:

Email: sme.compliance.ke@zohomail.com

Github link(press the link)

Section Two

(Recommended use the attached documents)

Appendix A: **Records of Processing Activities (RoPA) Template for Kenyan SMEs**

1. Purpose

The RoPA document serves as a centralized, comprehensive record that details all personal data processing activities within an SME. It enables accountability, facilitates compliance audits, and forms the basis for risk assessments and incident response under Kenya's Data Protection Act, 2019.

2. Usage Guidance

- **Who should maintain it?**
  The SME owner or designated Data Protection Officer (DPO), if appointed, is responsible for maintaining and regularly updating the RoPA.
- **How often should it be updated?**
  At minimum, quarterly reviews are required or immediately when new processing activities (including AI tools) are introduced or materially changed.
- **Format:**
  Use an electronic format (Excel spreadsheet or Google Sheets) to enable easy updates, filtering, and sharing with ODPC if requested.
- **Language:**
  Use clear, non-technical language where possible; include explanatory notes for legal terms.
- **Confidentiality:**
  While RoPA contains internal information, ensure it is securely stored and access is limited to authorized personnel.

3. Template Structure

Field	Description	Example
Processing Activity Name	A clear, concise title describing the processing activity.	"Customer Order Management via WhatsApp Chatbot"
Purpose of Processing	The specific business purpose(s) for collecting and processing personal data.	"To manage and fulfill customer orders and provide customer support"
Categories of Personal Data	Types of personal data processed (e.g., name, phone number, payment info).	"Name, phone number, delivery address, payment details"

Data Subject Categories	The groups or individuals whose data is processed (e.g., customers, employees).	"Customers placing orders via chatbot"
Legal Basis for Processing	The lawful basis for processing under the DPA (e.g., consent, contract, legitimate interest).	"Contractual necessity (order fulfillment)"
Data Source(s)	Where the data originates from (e.g., directly from data subjects, third parties).	"Provided directly by customers via WhatsApp chatbot"
Recipients / Third Parties	Any external parties receiving data (e.g., payment processors, cloud providers).	"M-Pesa payment gateway, AWS cloud hosting services"
International Data Transfers	Indicate if data is transferred outside Kenya and specify countries and safeguards (e.g., Standard Contractual Clauses).	"Yes; data stored in AWS servers in South Africa under Standard Contractual Clauses"
Retention Period	How long the personal data is retained before secure deletion or anonymization.	"Data retained for 2 years post transaction, then securely deleted"
Technical and Organizational Security Measures	Brief description of security measures applied (e.g., encryption, access controls).	"End-to-end encryption on WhatsApp; role-based access to backend systems; regular security audits"
Automated Decision-Making / AI Involvement	Specify if AI is used and if any automated decisions impacting data subjects are made.	"Yes; AI chatbot automates order processing but human review available for flagged orders"
Data Protection Impact Assessment (DPIA) Completed?	Indicate if a DPIA has been performed for this activity and date.	"Yes; DPIA completed on 01-Sep-2025"
Data Breach History	Note if any breaches related to this processing have occurred, with date and mitigation measures taken.	"No breaches to date"

4. Detailed Explanations of Each Field

4.1 Processing Activity Name

- Use descriptive names that easily identify the activity.
- Examples: “Employee Payroll Management,” “Customer Support via AI Chatbot,” “Email Marketing Campaign.”

4.2 Purpose of Processing

- Be explicit about why data is processed.
- Avoid vague terms like “business purposes.”
- The purpose should align with lawful processing bases under DPA.

4.3 Categories of Personal Data

- List all personal data types processed, including sensitive data (e.g., health information, biometric data).
- Be specific: Instead of “contact info,” state “phone number, email address.”

4.4 Data Subject Categories

- Identify who the data subjects are (customers, employees, suppliers, website visitors).
- This helps clarify the scope of processing.

4.5 Legal Basis for Processing

- Kenyan DPA Section 6 outlines lawful bases: consent, contract, legal obligation, vital interests, public interest, legitimate interest.
- Choose the correct basis and be ready to justify it.
- For SMEs, common bases include contractual necessity and consent.

4.6 Data Source(s)

- Indicate if data is collected directly from the individual or through third parties.
- Helps clarify transparency and accountability.

4.7 Recipients / Third Parties

- List all external entities receiving or processing data.
- This must include cloud providers, payment processors, marketing agencies, AI vendors.
- Contracts with these parties must include data protection clauses.

4.8 International Data Transfers

- Kenya’s DPA restricts transfers outside Kenya unless adequate safeguards exist.

- If data is hosted or processed abroad (e.g., cloud servers), specify locations and safeguards.
- Typical safeguards include Standard Contractual Clauses or adequacy decisions.

4.9 Retention Period

- Define how long data is kept and rationale (e.g., tax requirements, customer service).
- After retention, data should be deleted or anonymized securely.

4.10 Security Measures

- Briefly describe measures such as encryption, access restrictions, authentication, staff training.
- Must demonstrate “appropriate” technical and organizational security per DPA Section 28.

4.11 Automated Decision-Making / AI Involvement

- Specify if AI or automated systems make decisions affecting individuals.
- Explain if human intervention is available.
- Transparency about profiling is critical.

4.12 Data Protection Impact Assessment (DPIA) Completed?

- Confirm if DPIA was done to assess risks for high-risk processing.
- Provide dates for records and audit trails.

4.13 Data Breach History

- Document any security incidents related to this processing.
- Include actions taken and outcomes.

5. Example Completed Entry

Field	Entry
Processing Activity Name	Customer Order Management via WhatsApp Chatbot
Purpose of Processing	To manage and fulfill customer orders and provide customer support
Categories of Personal Data	Name, phone number, delivery address, payment details
Data Subject Categories	Customers placing orders via chatbot
Legal Basis for Processing	Contractual necessity
Data Source(s)	Provided directly by customers via WhatsApp chatbot
Recipients / Third Parties	M-Pesa payment gateway, AWS cloud hosting services
International Data Transfers	Yes; AWS servers in South Africa under Standard Contractual Clauses
Retention Period	Data retained for 2 years post transaction, then securely deleted
Security Measures	End-to-end encryption on WhatsApp; role-based access; regular security audits
Automated Decision-Making / AI Involvement	Yes; AI chatbot automates order processing with human review for exceptions
DPIA Completed?	Yes; DPIA completed on 01-Sep-2025
Data Breach History	No breaches to date

6. Final Recommendations

- **Keep it concise but comprehensive**: Include all relevant details but avoid overcomplication.
- **Integrate with other compliance documents**: Link RoPA entries with DPIA results and Privacy Policy clauses.
- **Train staff**: Ensure team members understand how RoPA supports data protection.
- **Prepare for ODPC audits**: Have RoPA ready for inspection and be prepared to explain entries.
- **Leverage this as a living document**: Update promptly with new AI tools, data flows, or regulation changes.

Appendix B: **Privacy Policy Updates Template for Kenyan SMEs with AI-Specific Disclosures**

[Company Name] Privacy Policy

Effective Date: [Insert Date]
Last Reviewed: [Insert Date]
Contact: [Data Protection Officer's Name/Email/Phone]

1. Introduction

At [Company Name], your privacy is a top priority. This Privacy Policy explains how we collect, use, disclose, and protect your personal data when you interact with our business, including through AI-powered tools such as chatbots and automated customer service systems.

We are committed to complying with the **Kenya Data Protection Act, 2019 (DPA)** and ensuring that your personal information is handled transparently, securely, and lawfully.

2. Scope

This policy applies to all personal data collected and processed by [Company Name], whether online, offline, or through AI-enabled technologies. It covers customers, employees, suppliers, and website visitors.

3. Personal Data We Collect

We collect the following types of personal data:

- **Identity Data:** Name, date of birth, gender
- **Contact Data:** Phone number, email address, postal address
- **Transaction Data:** Payment information, purchase history
- **Technical Data:** IP address, device identifiers, browser type
- **Interaction Data:** Chat logs, customer support inquiries, AI chatbot interactions
- **Other Data:** Any additional information voluntarily provided during our interactions

4. Sources of Personal Data

We collect data directly from you when you:

- Register on our website or mobile app
- Use our AI-powered chatbots or automated customer support tools
- Make a purchase or request a service
- Communicate with us via WhatsApp, email, or telephone
- Provide feedback or participate in surveys

We may also collect data from third-party service providers such as payment processors and cloud service providers.

5. How We Use Your Personal Data

Your personal data is used for the following purposes:

- To process and fulfill orders and payments
- To provide customer support, including through AI-powered chatbots
- To improve our services and personalize your experience
- To comply with legal and regulatory obligations
- To send promotional communications where you have consented
- To detect and prevent fraud and other unauthorized activities

6. Legal Bases for Processing

Under the Kenya Data Protection Act, 2019, we process your data based on the following lawful grounds:

- **Contractual Necessity:** Processing is required to perform our contract with you (e.g., to fulfill orders).
- **Consent:** Where you have provided explicit consent (e.g., marketing communications).
- **Legal Obligation:** To comply with legal duties (e.g., tax or audit requirements).
- **Legitimate Interests:** For purposes such as improving service quality and fraud prevention, balanced against your rights and interests.

7. AI and Automated Decision-Making

We use Artificial Intelligence technologies, including chatbots and automated systems, to:

- Respond to customer inquiries promptly
- Automate routine transactions (e.g., order placement)
- Analyze data to improve service delivery

Important disclosures:

- **Automated Decisions:** Some decisions, such as order confirmations and responses, are made automatically. However, human oversight is maintained to review flagged cases or complex issues.

- **Transparency:** Our AI systems operate based on defined rules and data inputs; we do not use profiling that would significantly affect your rights or freedoms without explicit consent.
- **Fairness and Bias Mitigation:** We actively monitor our AI tools to minimize bias and ensure fair treatment for all customers.

8. Sharing and Disclosure of Personal Data

We may share your personal data with trusted third parties under strict confidentiality agreements, including:

- Payment processors (e.g., M-Pesa)
- Cloud service providers (e.g., AWS)
- Customer support platforms
- Legal and regulatory authorities, where required

We ensure all third parties comply with the Kenya Data Protection Act and implement appropriate security measures.

9. International Data Transfers

Where your data is processed or stored outside Kenya, such as on cloud servers in South Africa or other jurisdictions, we ensure adequate protections are in place. This includes:

- Use of **Standard Contractual Clauses (SCCs)** approved by Kenyan regulators
- Verification of recipient countries' data protection standards

10. Data Retention

We retain your personal data only as long as necessary to fulfill the purposes outlined in this policy or as required by law. Typical retention periods include:

- Transaction records: 2 years post-transaction
- Customer support interactions: 1 year
- Marketing consents and preferences: Until withdrawal

After the retention period, your data is securely deleted or anonymized.

11. Data Security

We implement appropriate technical and organizational measures to protect your personal data from unauthorized access, alteration, disclosure, or destruction, including:

- End-to-end encryption of communication channels (e.g., WhatsApp)
- Role-based access controls

- Regular security audits and vulnerability assessments
- Staff training on data protection principles

12. Your Rights

Under the Kenya Data Protection Act, you have the following rights regarding your personal data:

- **Right to Access:** Request a copy of the personal data we hold about you
- **Right to Rectification:** Request corrections to inaccurate or incomplete data
- **Right to Erasure:** Request deletion of personal data, subject to legal retention requirements
- **Right to Object:** Object to processing based on legitimate interests or direct marketing
- **Right to Withdraw Consent:** Where processing is based on consent
- **Right to Data Portability:** Request your data in a portable format for transfer
- **Right to Lodge a Complaint:** With the Office of the Data Protection Commissioner (ODPC)

To exercise these rights, contact our Data Protection Officer at [Insert Contact].

13. Cookies and Tracking Technologies

Our website and AI platforms use cookies and similar tracking technologies to enhance user experience. These technologies collect information about your usage patterns to:

- Personalize content
- Analyze performance
- Provide targeted advertising (with consent)

You can manage cookie preferences through your browser settings.

14. Changes to This Privacy Policy

We may update this Privacy Policy to reflect changes in our practices or legal requirements. We will notify you of significant changes via our website or direct communication.

15. Contact Information

For questions, concerns, or requests related to this Privacy Policy or your personal data, please contact:

Data Protection Officer
[Name]
Email: [DPO Email]
Phone: [DPO Phone]
Address: [Company Address]

16. Acknowledgment and Consent

By using our services, including AI-powered tools, you acknowledge that you have read and understood this Privacy Policy and consent to the collection and use of your personal data as described.

Appendix C: **Data Protection Impact Assessment (DPIA) Template**

[Company Name]

Data Protection Impact Assessment (DPIA) Form

Effective Date: [Insert Date]
Version: 1.0
DPIA Lead: [Name, Position]
Contact: [Email, Phone]

1. Project/Processing Activity Details

Field	Description / Input
Project / Processing Activity Name	Describe the specific data processing or AI project under assessment.
Date DPIA Conducted	[DD-MM-YYYY]
Description of Processing	Detailed description of what personal data is collected, how, and why.
Purpose(s) of Processing	Business reasons and objectives for data processing.
Data Categories	Specify types of personal data involved (e.g., name, biometric data).
Data Subjects	Identify individuals whose data is processed (customers, employees, suppliers).
Legal Basis for Processing	Specify lawful basis per Kenya DPA (e.g., consent, contractual necessity).
Data Flow Diagram Attached?	Yes / No (Attach diagram showing data movement and systems used).

2. Necessity and Proportionality

Question	Response
Is the processing necessary to achieve the stated purpose?	[Yes/No] – Explain why no less intrusive alternative exists.
Have you considered alternatives that minimize data use?	[Yes/No] – Describe any options evaluated.
Does the processing respect data minimization principles?	[Yes/No] – Detail measures to limit data collected and processed.

3. Risk Assessment

Potential Risk	Likelihood (Low/Med/High)	Impact (Low/Med/High)	Risk Level (L/M/H)	Mitigation Measures
Unauthorized access to personal data				Access controls, encryption, staff training
Data breach involving AI processing system				Regular audits, patch management, incident response plan
Inaccurate data leading to wrong automated decisions				Human oversight, data validation procedures
Algorithmic bias impacting data subjects				Bias testing, diverse training data, regular reviews
Non-compliance with Kenya DPA and AI regulations				Regular compliance checks, staff awareness sessions

Inadequate data retention and deletion practices				Defined retention policies, automated deletion protocols

4. Consultation Process

Stakeholders Consulted	Method	Summary of Feedback
Internal Teams (IT, Legal, Compliance)	Meetings, emails	[Brief summary of key points and concerns]
Data Subjects (Customers/Users)	Surveys, focus groups	[Summary of privacy concerns and preferences]
External Experts / Consultants	Workshops, advisory reports	[Input on risk and mitigation strategies]

5. Measures to Address Risks and Ensure Compliance

Risk / Issue	Mitigation Measure	Responsible Person	Deadline	Status
Unauthorized access	Implement role-based access control and encryption	IT Manager	[Date]	[Open/Closed]
Data breach	Develop and test incident response plan	Compliance Officer	[Date]	[Open/Closed]
Inaccurate automated decisions	Establish human review mechanism for AI decisions	AI Project Lead	[Date]	[Open/Closed]
Algorithmic bias	Conduct regular fairness audits and bias mitigation	Data Scientist	[Date]	[Open/Closed]

Non-compliance with DPA	Schedule quarterly compliance reviews	DPO	[Date]	[Open/Closed]
Data retention	Automate secure deletion after retention period	IT Administrator	[Date]	[Open/Closed]

6. Residual Risks

Risk	Residual Risk Level (Low/Med/High)	Justification
[E.g., Minor risk of data breach]	[Low/Medium/High]	[Explanation of residual risk after mitigation]

7. Approval and Sign-Off

Name	Role	Signature	Date
DPIA Lead			
Data Protection Officer			
Senior Management			

8. Review and Update Schedule

Next Review Date [Insert Date]

DPIA must be reviewed annually or whenever significant changes to processing occur.

Guidance Notes

- **When to conduct a DPIA:**
  Required before commencing any new high-risk processing involving personal data, especially when deploying AI systems that process sensitive data or perform automated decision-making.
- **Data Flow Diagram:**
  Attach or create a simple flowchart illustrating data collection points, storage, transfer, processing (including AI components), and deletion.
- **Consultation:**
  Document how you engaged stakeholders, including data subjects if possible, to identify privacy concerns.

- **Risk Assessment:**
  Be objective and thorough. Include technical, organizational, legal, and reputational risks.
- **Mitigations:**
  Specify concrete actions, responsible persons, deadlines, and status to track progress.
- **Documentation:**
  Keep the DPIA and related records securely and be prepared to present to the ODPC upon request.

Step-by-Step Guide to Completing the DPIA Form

Step 1: Project/Processing Activity Details

Purpose: Define the scope and context of the data processing activity clearly.

- **Project / Processing Activity Name:**
  Provide a concise but descriptive name for the AI or data processing project (e.g., "WhatsApp Chatbot Customer Support AI"). This helps identify the DPIA in future audits.
- **Date DPIA Conducted:**
  Enter the date when you are completing the DPIA (format: DD-MM-YYYY).
- **Description of Processing:**
  Explain in detail what personal data you will collect and process, how you collect it (e.g., via chatbot, online forms), and what technology or platforms are used (e.g., WhatsApp API, cloud storage).
- **Purpose(s) of Processing:**
  Clearly state why the data is collected and processed (e.g., "To automate customer service responses and improve order processing efficiency").
- **Data Categories:**
  List all types of personal data involved (e.g., names, phone numbers, payment details, IP addresses).
- **Data Subjects:**
  Identify whose data you are processing customers, employees, suppliers, website visitors, etc.
- **Legal Basis for Processing:**
  Specify the lawful grounds under the Kenya Data Protection Act for this processing, such as:
    - Consent
    - Contractual necessity
    - Legal obligation
    - Legitimate interests (balance this carefully)
- **Data Flow Diagram Attached:**
  Attach a clear, simple data flow diagram showing how data moves through your systems from collection to storage, processing (including AI components), sharing, and deletion.

Step 2: Necessity and Proportionality Assessment

Purpose: Ensure the processing is justified and limited to what is necessary.

- **Is the processing necessary?**
  Confirm that the processing is essential for your stated business purpose. If alternatives exist that involve less personal data or no personal data, explain why they were not chosen.
- **Consider alternatives:**
  Describe any alternatives that reduce data use or impact on privacy (e.g., anonymization, pseudonymization, manual processes).
- **Data minimization:**
  Explain how you ensure you only collect and process the minimum personal data needed for your purposes.

Step 3: Risk Assessment

Purpose: Identify and analyze privacy risks related to your data processing.

- **List potential risks:**
  Brainstorm all possible risks security breaches, unauthorized access, inaccurate data, AI bias, non-compliance penalties, reputational damage.
- **Assess likelihood:**
  For each risk, estimate how likely it is to occur (Low / Medium / High) based on your environment and controls.
- **Assess impact:**
  Estimate the potential damage if the risk occurs (Low / Medium / High). Consider harm to individuals' rights, financial penalties, and business impact.
- **Determine risk level:**
  Combine likelihood and impact to classify each risk's overall level (Low / Medium / High).
- **Document mitigation measures:**
  For each risk, detail the controls and safeguards in place or planned, such as encryption, access controls, training, incident response plans, bias testing.

Step 4: Consultation Process

Purpose: Demonstrate you have sought input from relevant stakeholders.

- **Identify stakeholders:**
  Include internal teams (IT, legal, compliance), data subjects (customers, employees), and external experts (consultants, legal advisors).
- **Method of consultation:**
  Note how you consulted stakeholders meetings, emails, surveys, workshops.

- **Summary of feedback:**
  Capture key concerns raised, suggestions made, and how you plan to address them.

Step 5: Measures to Address Risks and Ensure Compliance

Purpose: Show how you are managing and reducing risks.

- **For each identified risk, specify:**
  - The concrete mitigation action (e.g., “Implement multi-factor authentication”).
  - The responsible person or team for implementing it.
  - Deadlines for completion.
  - Status updates to track progress.
- **Ensure all high and medium risks have documented mitigations.**

Step 6: Residual Risks

Purpose: Recognize any remaining risks after mitigation.

- **List any residual risks:**
  Identify risks that remain after applying mitigation measures.
- **Rate their residual level:**
  Again, Low / Medium / High.
- **Justify residual risk acceptance:**
  Explain why these risks are acceptable or what future plans exist to reduce them further.

Step 7: Approval and Sign-Off

Purpose: Obtain formal approval and accountability.

- **DPIA Lead:**
  The person who completed the DPIA signs and dates here.
- **Data Protection Officer (DPO):**
  The DPO reviews and approves to confirm compliance with data protection laws.
- **Senior Management:**
  Senior management’s sign-off ensures organizational commitment and resource allocation.

Step 8: Review and Update Schedule

Purpose: Ensure the DPIA remains current and relevant.

- **Set a date for next DPIA review:**
  Typically within 12 months or sooner if significant changes occur.
- **Update DPIA if:**
  New risks arise, processing activities change, or after incidents.

Additional Tips for Completing the DPIA

- **Be thorough but clear:** Avoid jargon. Write clearly to ensure all readers understand risks and mitigations.
- **Use evidence:** Attach supporting documents like risk assessment reports, data flow diagrams, training records.
- **Collaborate:** Engage IT, legal, compliance, and business teams early to gather accurate information.
- **Record version control:** Keep versions dated and archived for accountability.
- **Train staff:** Ensure those responsible understand the DPIA's importance and use it to inform decision-making.

Appendix D: **AI Risk Checklist Template**

Project AIDA: AI Risk Checklist for Kenyan SMEs

Purpose:
To systematically identify and manage risks arising from AI-powered data processing, ensuring compliance with the Kenya Data Protection Act, 2019 and the Office of the Data Protection Commissioner's (ODPC) enforcement expectations.

Instructions:

- Review each risk category and sub-item carefully.
- For each item, mark the risk level (Low / Medium / High).
- Indicate existing controls or mitigation measures.
- Identify gaps and plan corrective actions.
- Update regularly, especially when AI systems or processes change.

Section	Risk Factor	Risk Level	Existing Controls / Mitigations	Action Required / Comments
1. Data Collection & Processing				
1.1 Data Minimization	Does the AI system collect only necessary personal data?	Low/Med/High		
1.2 Lawful Basis	Is there a documented lawful basis under DPA for all data processing activities?	Low/Med/High		
1.3 Consent Management	Is explicit, informed consent obtained and recorded when required?	Low/Med/High		
1.4 Transparency & Notice	Are data subjects adequately informed about AI data use (e.g., updated Privacy Policy)?	Low/Med/High		
2. Data Quality & Accuracy				

2.1 Accuracy Checks	Are there mechanisms to ensure personal data used by AI is accurate and up-to-date?	Low/Med/High		
2.2 Data Correction Procedures	Can data subjects easily correct inaccurate data processed by AI?	Low/Med/High		
3. Algorithmic Risks				
3.1 Bias and Discrimination	Has the AI been tested for bias or unfair discrimination against protected groups?	Low/Med/High		
3.2 Explainability & Transparency	Can the AI's decision-making logic be explained in understandable terms to data subjects?	Low/Med/High		
3.3 Automated Decision-Making	Are high-risk decisions automated? If so, is human oversight in place?	Low/Med/High		
4. Data Security & Integrity				
4.1 Access Controls	Are strict access controls in place for AI data and systems?	Low/Med/High		
4.2 Encryption	Is data encrypted at rest and in transit?	Low/Med/High		
4.3 Incident Response	Is there an established protocol for responding to data breaches involving AI systems?	Low/Med/High		
5. Third-Party & Vendor Risks				
5.1 Vendor Due Diligence	Have all AI technology vendors been vetted for compliance with Kenya's data protection laws?	Low/Med/High		
5.2 Data Processing Agreements	Are contracts in place ensuring third-party compliance with DPA and data security standards?	Low/Med/High		
6. Data Subject Rights				
6.1 Right to Access	Can data subjects request and obtain their personal data processed by AI?	Low/Med/High		

6.2 Right to Rectification	Are processes in place for data subjects to request corrections?	Low/Med/High		
6.3 Right to Object	Can data subjects object to AI processing where applicable?	Low/Med/High		
6.4 Right to Erasure	Are data subjects able to request deletion of their data when appropriate?	Low/Med/High		
7. Compliance & Governance				
7.1 DPIA Conducted	Has a Data Protection Impact Assessment (DPIA) been completed for the AI system?	Low/Med/High		
7.2 Staff Training & Awareness	Are staff trained on AI-related data protection obligations and risks?	Low/Med/High		
7.3 Continuous Monitoring	Are AI systems and compliance controls regularly audited and updated?	Low/Med/High		
7.4 Incident Reporting	Is there a clear process for reporting data breaches and regulatory notifications?	Low/Med/High		

Summary & Risk Management

- **Overall Risk Level:** (fill)
- **Key High Risks Identified:** (fill)
- **Immediate Actions Planned:** (fill)
- **Responsible Person(s):** (fill)
- **Next Review Date:** (fill)

Definitions

- **Low Risk:** Risk is minimal and adequately controlled.
- **Medium Risk:** Risk exists and requires ongoing monitoring and mitigation.
- **High Risk:** Significant risk requiring immediate attention and robust controls.

Notes for SMEs

- Complete this checklist **before launching or updating AI systems** that process personal data.
- Use it as part of your **DPIA documentation** and compliance records.
- Engage legal and technical advisors if unsure about any risk factor.
- Regular updates are essential, especially when AI capabilities or data usage change.

Use the attached documents

This AI Risk Checklist template is offered under a Creative Commons license to empower Kenyan SMEs to safely harness AI innovation while protecting data rights and reducing regulatory risk.