



Comments on the Data Protection Manual for Non-Profit Organisations in Kenya (First Edition, 2026)

OUR REF:	ACAIGO/SE/4/2026
DATE	10 th October 2026
CONTACT	Email: info@acaigo.africa , website: https://www.acaigo.africa/

Executive summary

The African Centre for AI Governance and Oversight (ACAIGO) reviewed the first edition of the *Data Protection Manual for Non-Profit Organisations in Kenya*, published by Amnesty International Kenya.

ACAIGO recognises the manual as a valuable resource offering accessible, practical compliance guidance tailored to non-profit organisations. Its examples and operational guidance help translate data protection law into everyday practice and support the protection of the communities these organisations serve.

Our review identifies areas of concern relating to legal accuracy, clarity and consistency. The accompanying comments explain these concerns with reference to applicable law, with the aim of strengthening the manual's usefulness and supporting sound data governance in Kenya's non-profit sector.

Detailed comments

Page No.	Statement as currently captured	Issue	Comments/Justification
----------	---------------------------------	-------	------------------------

	Non-Profit work is increasingly data driven. Whether delivering community programmes, conducting research, undertaking advocacy, managing humanitarian responses, providing legal aid, or administering organisational operations, non-profit organisations routinely interact with individuals through the collection, use, and management of personal information. The quality and integrity of that interaction, its fairness, its proportionality, and its accountability is what data protection law and practice seeks to ensure.	N/A	The introductory paragraph under section 2.1 appears to have been inadvertently included in the table of contents. It should be removed from the table of contents and retained in the main body of the manual. The table of contents should list only section headings and their corresponding page numbers.
36	Are we collecting only what we need/require?	Are we collecting only what we need/require?	Delete the to make the statement grammatically sound
38	It enables organizations to identify precisely where personal data exists within their systems and processes, including locations that that were not considered.	It enables organizations to identify precisely where personal data exists within their systems and processes including locations that were not considered.	Delete one that, to avoid repetition
45	It also conditions data transfers outside the	The statement is too broad, as it implies that	Adequacy is only one transfer mechanism.



	EU on third states having adequate (meaning essentially equivalent) data protection standards.	an adequacy decision is required for all transfers outside the EU	The GDPR also permits transfers using appropriate safeguards, such as standard contractual clauses or binding corporate rules, and, in specific circumstances, derogations.
46	Under the GDPR, this burden shifts to non-EU countries. That is, the GDPR contains provisions that apply extraterritorially: non-EU countries processing EU data can be subject to GDPR penalties for failing to protect data according to EU standards. . As a result, to maintain (unpenalized) digital trade and interaction with European Union countries, other countries have a strong incentive under the GDPR to at least approximate European data protection standards.	The statement inaccurately suggests that the GDPR shifts compliance responsibility to non-EU countries	Article 3(2) of the GDPR defines its territorial scope by reference to processing by controllers and processors not established in the EU, where the processing relates to offering goods or services to individuals in the EU or monitoring their behaviour within the EU. The obligations therefore apply to those controllers and processors, rather than to non-EU countries themselves.
58	Clearly explaining to individuals what will be collected, why, and how it will be used, before collecting it so that individuals give informed consent.	The wording appears to link transparency obligation to consent only.	Transparency obligations apply irrespective of the lawful basis relied upon. Section 29 of the Data Protection Act, 2019 requires a data controller or processor, before collecting personal data and insofar as practicable, to inform the data subject of

			the matters specified in that section. Additionally, Section 25(b) requires personal data to be processed lawfully, fairly and transparently in relation to the data subject.
60	An organisation collects participants' contact details for a training event. It cannot then use those contacts to send fundraising communications without going back to participants, informing them of the new purpose.	The statement suggests that informing participants of the new purpose is sufficient to permit further processing.	Notification alone does not establish a lawful basis or resolve purpose compatibility. Under Regulation 6(5) of the Data Protection (General) Regulations, 2021, fresh consent must be sought where the new purpose is incompatible with the original purpose.
60	You must decide and communicate the purpose of data collection before you collect it. You cannot later use the data for a different purpose without informing the data subject.	The statement suggests that informing participants of the new purpose is sufficient to permit further processing.	Notification alone does not establish a lawful basis or resolve purpose compatibility. Under Regulation 6(5) of the Data Protection (General) Regulations, 2021, fresh consent must be sought where the new purpose is incompatible with the original purpose.
65	Legal Reference: General Data Protection Regulations, Article 5 and Regulation 23 of General Regulations Data handlers must be able to demonstrate compliance with	The manual cites the wrong regulation	Regulation 23 concerns data protection policies rather than expressly establishing the accountability principle. While such policies support accountability, the manual



	the data protection principles. Accountability is not a standalone action, but the organisation's overall responsibility to demonstrate, that it is upholding the principles. principles through documentation. This principle ensures organisations don't just intend to comply, but they are able to demonstrate compliance.		should clarify this relationship and avoid presenting the provision as equivalent to Article 5(2) of the GDPR.
69	We do not repurpose personal data for activities beyond its original stated purpose without informing data subjects.	The statement suggests that informing participants of the new purpose is sufficient to permit further processing.	Notification alone does not establish a lawful basis or resolve purpose compatibility. Under Regulation 6(5) of the Data Protection (General) Regulations, 2018, fresh consent must be sought where the new purpose is incompatible with the original purpose.
70	We comply with legal minimum retention periods (e.g. employment records — 3 years; business records — 7 years).	The stated three-year minimum retention period for employment records is inaccurate.	Section 10(6) of the Employment Act, 2007 requires employers to retain the written particulars prescribed in subsection (1) for five years after termination of employment. The manual's stated three-year retention period does not reflect this requirement.

76	Take Note - Sensitive Personal Data The Data Protection Act, 2019 designates certain categories of personal data as sensitive. These include data relating to health, race, ethnic origin, religion or belief, political opinion, financial information, genetic and biometric data, and sexual orientation.	The list does not accurately reflect the definition of sensitive personal data in Section 2 of the Data Protection Act, 2019.	The list includes “political opinion”, which is not expressly listed in Section 2 of the Data Protection Act, 2019. It also omits conscience, marital status, family details including the names of a person’s children, parents, spouse or spouses and sex. Although “includes” indicates a non-exhaustive list, these omissions may leave readers unaware that these categories are expressly protected as sensitive personal data under the Act.
81	Repetition of compliance with legal obligation	The entire segment on compliance with a legal obligation as a lawful basis for processing is repeated.	The segment duplicates content already covered in the manual. Its removal would reduce repetition and improve clarity and flow.
84	Unlike most other lawful bases, this ground does not depend on the consent of the data subject or the performance of a specific legal or contractual obligation. Instead, it requires the organisation to conduct and document a structured three-part	The wording appears to suggest that other lawful bases depend on consent or a specific legal or contractual obligation.	Each lawful basis provides an independent ground for processing, subject to its own applicable conditions. This is consistent with Regulation 5(2) of the Data Protection (General) Regulations, 2021, which requires processing under Regulation 5(1) to rely on

	assessment.		one legal basis at a time, established before processing begins.
100	Critically, when a data subject withdraws consent, the organisation must have systems in place to notify all downstream partners who hold that individual's data. Section 36 of the DPA 2019 and Regulation 18 of the Data Protection (General) Regulations 2021 require that processing by a data processor be governed by a binding contract.	The manual cites the wrong section of the act and regulations	Section 36 of the Act addresses objection to processing and regulation 18 addresses restriction of further direct marketing. Section 42(2)(b) of the Data Protection Act, 2019, read together with Regulation 24 of the Data Protection (General) Regulations, 2021, addresses the contract between a data controller and a data processor.
103	Statutory Reference: Section 36 DPA 2019 & Regulation 18, Data Protection (General) Regulations 2021 Processing by a data processor shall be governed by a binding contract	The manual cites the wrong section of the act and the regulation	Section 36 of the Act addresses objection to processing and regulation 18 addresses restriction of further direct marketing. Section 42(2)(b) of the Data Protection Act, 2019, read together with Regulation 24 of the Data Protection (General) Regulations, 2021, addresses the contract between a data controller and a data processor.
116	Respond within 14 days of receipt. If a brief extension is required (up to 30 days), notify the data subject in writing within the	The section applies a blanket 14-day response period without distinguishing between the statutory timelines applicable	Regulation 9(4) of the Data Protection (General) Regulations, 2021 requires compliance with an access request within

	standard 14-day period and explain the reasons.	to different data subject rights. Additionally, the wording appears to suggest that a 30-day extension applies to all data subject rights requests.	seven days, while Regulation 11(3) provides thirty days for compliance with a data portability request. Section 38(7) of the act allows extension only for complex portability request
117	Date and time the request was received (starts the 14-day clock)	The section applies a blanket 14-day response period without distinguishing between the statutory timelines applicable to different data subject rights.	Regulation 9(4) of the Data Protection (General) Regulations, 2021 requires compliance with an access request within seven days, while Regulation 11(3) provides thirty days for compliance with a data portability request
118	What Happens When a DSR Involves Third-Party Data? • The non-profit (data controller) remains responsible for responding to the data subject within 14 days. • The non-profit must immediately notify the third-party processor of the DSR and request their cooperation. • The third-party processor must assist the non-profit in fulfilling the request (this should be contractually required in the Data Processing	The heading “What Happens When a DSR Involves Third-Party Data?” does not accurately reflect the section’s content. Additionally, the section applies a blanket 14-day response period without distinguishing between the statutory timelines applicable to different data subject rights.	Third-party data refers to personal data relating to individuals other than the person exercising the right. The section instead addresses cooperation between a data controller and a third-party processor in responding to a data subject request. Regulation 9(4) of the Data Protection (General) Regulations, 2021 requires compliance with an access request within seven days, while Regulation 11(3) provides

	Agreement). • If a third-party refuses to cooperate with a rectification or erasure instruction, the non-profit must document this, inform the data subject, and report the non-compliance to the regulatory body where applicable.		thirty days for compliance with a data portability request.
123	Must enter into a written data processing agreement with each processor (Section 41(2), DPA 2019).	The manual cites the wrong section of the act	Section 41(2) of the Data Protection Act, 2019 addresses data protection by design and default, whereas section 42(2)(b) requires a written contract between a data controller and a data processor.
123	Must notify the controller of a breach within 48 hours of becoming aware (Regulation 38, General Regulations 2021).	The manual cites the wrong regulation	Regulation 38 of the Data protection General regulation addresses notification by data controller to the Data Commissioner.
124	Organizations are required to designate a Data Protection Officer (DPO) where they process personal data, their core activities require regular and systematic monitoring of data subjects on a large scale, or their core activities involve large-scale processing of sensitive personal data.	The manual introduces a “large-scale” criterion that is not included in Section 24(1)(b) or (c) of the Data Protection Act, 2019.	Section 24(1)(b) and (c) of the Data Protection Act, 2019 does not impose a “large-scale” criterion. Introducing this threshold may dissuade controllers from appointing a DPO because they consider their processing operations not large scale, even where their core activities require regular and systematic monitoring of data

			subjects or involve processing sensitive categories of personal data. This concern remains relevant notwithstanding the discretionary nature of DPO appointment under Section 24.
126	within 48 hours of becoming aware of the breach (Regulation 38, General Regulations 2021). This gives the controller time to assess and meet the 72-hour deadline.	The manual cites the wrong the regulation	Regulation 38 of the Data protection General regulation addresses notification by data controller to the Data Commissioner.
127	General Criminal Penalty S.72, DPA 2019 Fine not exceeding KES 3,000,000 OR imprisonment not exceeding 10 years, or both.	The manual cites the wrong section of the Act	While section 72 of the Act addresses offences involving unlawful disclosure of personal data, Section 73(1) provides the general penalty.
127	Administrative Fine S.58(4) & S.62, DPA 2019 Fine not exceeding KES 5,000,000 or 1% of annual turnover of the preceding financial year, whichever is lower.	The manual cites the wrong section of the Act	Section 58(4) of the Data Protection Act, 2019 does not exist. The applicable administrative fines are addressed in Section 58(3).
127	Compounded Offences S.58(8) & S.74, DPA 2019; General Regulations 2021 The Data Commissioner may compound offences for payment of up to two-thirds of the	The manual cites the wrong section of the Act	Section 58(8) of the Data Protection Act, 2019 does not exist. Section 74 addresses codes, guidelines and certification that may



	maximum applicable fine.		be issued by the Data Commissioner.
132	Article 46 of the DPA 2019 and Regulation 26 of the General Regulations provide conditions under which personal data may be transferred outside Kenya	The manual cites the wrong provisions the wrong section of the Act and the Regulation	Section 46 of the Data Protection Act, 2019 addresses health data, while Regulation 26 of the Data Protection (General) Regulations, 2021 concerns processing for purposes of strategic interest of the State. Transfers of personal data outside Kenya are addressed in Sections 48–50 of the Act and Part VII (Regulations 39–48) of the General Regulations.
162	Section 28 of the Data Protection Act, 2019 requires organisations to designate a Data Protection Officer where they process personal data and their core activities require regular and systematic monitoring of data subjects on a large scale or involve large-scale processing of sensitive personal data.	The manual cites the wrong section of the Data Protection Act	Section 28 of the Data Protection Act, 2019 addresses the collection of personal data, whereas section 24 governs the designation or appointment of data protection officers. Additionally, Section 24(1)(b) and (c) of the Data Protection Act, 2019 does not impose a “large-scale” criterion. These provisions refer to core activities requiring regular and systematic monitoring of data subjects or consisting of processing sensitive categories of personal data.

163	Regulation 41–45 of the Data Protection (General) Regulations, 2021 govern DPIAs. A DPIA must be conducted, at minimum, before commencing:	The manual cites the wrong regulation	Regulations 41–45 of the Data Protection (General) Regulations, 2021 address international data transfers, whereas Part VIII addresses data protection impact assessments (DPIAs).
164	List any processing activity currently planned or underway that could count as high risk under Section 31 and Regulation 41.	The manual cites the wrong regulation	Regulation 41 of the Data Protection (General) Regulations, 2021 addresses transfers on the basis of appropriate safeguards, whereas Regulation 49(1) identifies processing activities considered to pose a high risk to data subjects' rights and freedoms.
167	Under Section 41(2) of the Data Protection Act, 2019, a written data processing agreement is required wherever a processor is engaged	The manual cites the wrong section of the Data Protection Act	Section 41(2) of the Data Protection Act, 2019 addresses data protection by design and default, whereas section 42(2)(b) requires a written contract between a data controller and a data processor.
174	Under Section 31 and Regulations 41–45 of the Data Protection (General) Regulations, 2021, when is a DPIA required, and what	The manual cites the wrong regulation	Regulations 41–45 of the Data Protection (General) Regulations, 2021 address international data transfers, whereas Part

	are its key stages?		VIII addresses data protection impact assessments (DPIAs).
174	Explain the independence requirement for a Data Protection Officer under Section 28 of the Act and describe a scenario in which that independence could be compromised in a small nonprofit organisation	The manual cites the wrong section of the Data Protection Act, 2019	Section 28 of the Data Protection Act, 2019 addresses the collection of personal data, whereas section 24 governs the designation or appointment of data protection officers.
182	Data subject request compliance Number of requests received and percentage responded to within the statutory timelines.	This content appears out of place in this section	The “Data subject request compliance” row appears misplaced in the complaint-process table. Its content describes a performance indicator for handling data subject requests, rather than a stage in the ODPC complaints procedure.
182	The ODPC may facilitate: • mediation; • conciliation; • negotiation; or • other forms of alternative dispute resolution. This authority is recognized under Regulation 12.	The manual cites the wrong regulation in support of this requirement	Regulation 12 of the Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021 addresses joinder of parties, whereas Regulation 15 provides for negotiation, mediation and



			conciliation.
--	--	--	---------------

For ACAIGO

Jane Awuor Ombiro
Co-Founder & Principal Advisor
Privacy and AI

AFRICAN CENTRE FOR AI GOVERNANCE AND OVERSIGHT
<https://www.acaigo.africa/> | info@acaigo.africa | Nairobi, Kenya