MODEL DATA GOVERNANCE CHARTER

For Startups and Civil Society Organisations (CSOs)

This is a starting template, not a finished policy. It draws on the Office of the Data Protection Commissioner, Kenya (ODPC) Draft Model County Data Protection Guidelines, the data protection principles in the Data Protection Act, 2019 (Kenya), ISO/IEC 38505-1 (the international standard for data governance), and standard data governance charter conventions, simplified and adapted for an organisation without a legal or compliance department.

Replace every [bracketed field] with your own detail, delete what does not apply, and have it approved by whoever leads your organisation.

Before You Begin:

Please Read | Delete this when done with developing your Charter

A charter is different from a policy. A policy sets out day-to-day rules (how long we keep data, who can access what). A charter sits above that: it states why data governance matters to your organisation, who has authority to set and change the rules, and commits leadership to resourcing it. Most organisations need both; this document is the charter, and Section 5 points you to the individual policies and tools that sit underneath it.

This charter is a practical starting point, not legal advice. It does not replace a lawyer, a qualified Data Protection Officer, or formal legal review, and it does not cover every obligation under the Data Protection Act, 2019 (Kenya) or any other law that may apply to your organisation.

It draws on publicly available guidance current as of the drafting date. Data protection law and ODPC guidance are updated periodically; check www.odpc.go.ke for the current version of any guidance note referenced here before relying on it.

If your organisation operates outside Kenya, or handles data from people outside Kenya, you remain responsible for complying with the specific laws of every jurisdiction in which you operate (for example, the GDPR in the EU and/or UK).

Section 1: Purpose and Scope

[Organisation Name] collects and uses personal data to [state your core purpose, e.g. 'deliver our services, pay our staff, and report to our donors and regulators']. This Charter sets out how we do that responsibly: who is accountable, what rules we follow, and what tools we use to protect the people whose data we hold.

This Charter applies to:

- All staff, founders, board members, volunteers, and interns.
- All contractors, consultants, and third-party suppliers who process personal data on our behalf.
- All personal data we hold, whether digital (databases, spreadsheets, cloud storage, apps) or physical (paper files, forms, printed records).
- Every stage of the data lifecycle: collection, storage, use, sharing, and deletion.

'Personal data' means any information that can identify a living person, directly or indirectly, for example a name, phone number, ID number, photo, location, or online identifier. 'Sensitive personal data' is a smaller category needing extra care: health, biometric, genetic, ethnic, religious, or similar information, and any data belonging to a child.

Section 2: Key Terms, Explained Simply

These are the terms used throughout this Charter. They are explained in plain language here so that no one needs a legal background to use this document.

Term	What it means
Data subject	The person the data is about, for example a customer, employee, beneficiary, or donor.
Data controller	The organisation that decides why and how personal data is collected and used. This is usually your organisation itself.
Data processor	A third party that handles personal data on your instructions, for example a payroll provider, cloud host, or email marketing tool.
Consent	A person's clear, freely given 'yes' to a specific use of their data. It must be a real choice, not a condition buried in fine print, and it must be as easy to withdraw as it was to give.
Data Protection Officer (DPO)	The person responsible for advising your organisation on data protection compliance day to day. Not every small organisation is legally required to appoint one, but someone should always hold this responsibility (see Section 4).
Data Protection Impact Assessment (DPIA)	A structured check you carry out before starting a new or high-risk activity involving personal data, to spot and fix privacy risks before they happen.
Data breach	Any incident where personal data is lost, stolen, accessed, or disclosed without authorisation, for example a lost laptop, a hacked account, or an email sent to the wrong person.
Retention	How long you keep a given type of data before deleting or archiving it. Data should not be kept indefinitely 'just in case'.
Anonymisation / Pseudonymisation	Anonymisation permanently removes anything that could identify a person. Pseudonymisation replaces identifying details with a code, keeping the key to reverse it separately and securely. Anonymised data carries far less risk.

Section 3: Our Governance Principles

These principles are drawn from two sources working together: the data protection principles already set out in Section 25 of the Data Protection Act, 2019 (Kenya), which are legally grounded and specific to handling personal data, and ISO/IEC 38505-1, an international standard for data governance more broadly, which adds a few things the Act does not explicitly cover (particularly around everyday habits and checking that our practices actually work). Where a principle exists in both, we have merged them into one plain-language row rather than repeating it twice.

Principle	What it means for us, in practice
Responsibility and Accountability	Every data decision has one named person accountable for it, not 'the team' in general. We can show, not just claim, that we follow our own rules, for example by keeping records of what we decided and why.
Lawfulness, Fairness and Transparency	We only use personal data when we have a genuine, legal reason to (see the lawful basis stated in each of our policies). We are upfront with people about what we are doing with their data, and we treat them fairly, not just technically within the rules.
Purpose Limitation and Strategic Fit	We collect data for a clearly stated reason connected to our mission, and we do not quietly reuse it for something else later without asking again. Our data practices serve our work, not the other way around.
Data Minimisation	We only collect data we can justify needing, and no more. Before adding a new form field or tracking tool, we ask whether we actually need it to do our work.
Accuracy	We keep personal data correct and current, and we fix or delete it when it is wrong, rather than letting errors sit indefinitely.
Storage Limitation	We do not keep personal data indefinitely just in case it might be useful. We set a clear retention period for each type of data and actually delete or archive it once that period ends.
Confidentiality and Vigilance	We protect data with real safeguards, such as access controls and encryption, and we regularly test that those safeguards still work in practice, not just that they are written down somewhere.
Stewardship	Good data practice is built into how people actually work day to day, through training and habit, so it does not depend on someone remembering the rules under pressure.

Section 4: Governance Structure and Roles

Smaller organisations do not need a large committee structure. What matters is that every one of these roles is actually assigned to a real person, even if one person holds more than one role.

Role	Who (fill in)	Responsible for
Board / Founder(s)	*[Name/Title]*	Ultimate accountability for data governance; approves this Charter and resources it (budget, staff time, training).
Data Protection Lead / DPO	*[Name/Title]*	Day-to-day compliance; advises staff; handles data subject requests; leads on DPIAs and breach response. See note below.
Team / Department Leads (Data Owners)	*[Name/Title]*	Know what personal data their team holds and why; ensure their team follows this Charter and its supporting policies.
IT / Systems Admin (Data Custodian)	*[Name/Title]*	Technical safeguards: access controls, backups, encryption, and technical response to security incidents.
All Staff and Volunteers	*Everyone*	Complete data protection training; follow this Charter in day-to-day work; report suspected risks or breaches immediately.
External Partners / Processors	*[Vendor names]*	Follow the data-processing terms in their contract with us; notify us immediately of any breach on their side.
Role	*Who (fill in)*	Responsible for
Board / Founder(s)	*[Name/Title]*	Ultimate accountability for data governance; approves this Charter and resources it (budget, staff time, training).

Appointing a Data Protection Officer is not automatically mandatory for every organisation under the Data Protection Act, 2019, but the responsibility must sit somewhere. Check the ODPC's current Guidance Notes for Data Protection Officers (DPOs)[1] to see whether appointment is required for your organisation's size and type of processing, and consult the ODPC's Guidance Notes on Processing by MSMEs[2] if you are a small or medium enterprise.

[1] https://www.odpc.go.ke/wp-content/uploads/2026/07/ODPC-%E2%80%93-Guidance-Note-for-Data-Protection-Officers-DPOs.pdf
[2] https://www.odpc.go.ke/wp-content/uploads/2025/11/ODPC-%E2%80%93-Guidance-Note-on-Processing-by-MSMEs.pdf

Section 5: The Building Blocks

This Charter sets direction through practical tools that turn it into everyday practice. *[You do not need all of them on day one, but every organisation handling personal data should be working towards having each of them in place.]*

1. Data Inventory (Data Map)
A simple list of what personal data you hold, why you collect it, where it is stored, who can access it, and how long you keep it. Start with a spreadsheet: one row per type of data. This is the foundation everything else builds on.

2. Privacy Notice
A short, plain-language statement telling people what data you are collecting, why, and what you do with it, given before or at the point you collect their data. Avoid legal jargon; write it the way you would explain it to a friend.

3. Data Protection Policy
Your internal rulebook: retention periods, who can access what, security measures, and how you handle data subject requests. The ODPC's Guidance Notes for Data Protection Policies sets out what a compliant policy should cover.

4. Retention Schedule
A simple table: data type, how long you keep it, and what happens after (delete or archive). Without this, data tends to accumulate indefinitely by default, which is itself a risk.

5. Data Protection Impact Assessment (DPIA)
A structured risk check carried out before starting a new or high-risk activity (a new app, a new database, collecting sensitive data, or working with children's data). If your organisation has a separate privacy risk assessment tool, use it here; otherwise, the ODPC's Guidance Note on Data Protection Impact Assessment sets out the expected process.

6. Consent and Rights Log
A record of consents given or withdrawn, and of any data subject requests (to access, correct, or delete their data) and how you responded, including the date and whether you met the response deadline.

7. Incident and Breach Response Plan
A short, rehearsed plan: who to notify internally, when and how to notify the ODPC and affected individuals, and the immediate steps to contain and investigate an incident. Write this before you need it, not during a crisis.

8. Vendor and Third-Party Checklist
Before sharing personal data with any supplier (cloud host, payroll provider, email tool, analytics service), check they have adequate safeguards and sign a data-processing agreement setting out their obligations.

9. Training and Awareness Plan
A short onboarding session for new staff, plus periodic refreshers, so everyone knows the basics: what personal data is, how to spot a risk, and who to tell if something goes wrong.

10. Registration with the ODPC
Confirm whether your organisation is required to register as a data controller or data processor with the ODPC, and keep that registration current. The ODPC's Guidance Note on Registration of Data Controllers and Data Processors explains the thresholds and process.

---

[3] *https://www.odpc.go.ke/wp-content/uploads/2024/02/ODPC-Guidance-Note-on-Data-Protection-Impact-Assessment-1.pdf*

Section 6: Adoption, Review, and Version Control

This Charter is a living document. It should be reviewed at least once a year, and sooner if any of the following happen: your organisation starts collecting a significant new type of data, a new law or ODPC guidance note is issued, or a data breach or near-miss reveals a gap in this Charter or the tools beneath it.

Version	Date	Approved by	Summary of changes

Approved by (name and title)	
Signature	
Date	
Next scheduled review date	

Appendix: First 90 Days Checklist

If you are starting from nothing, work through this list roughly in order over your first three months.

- [ ] Assign a Data Protection Lead, even if they hold the role part-time alongside other duties.
- [ ] Build your first data inventory: list every type of personal data you hold.
- [ ] Write a plain-language privacy notice for your website, app, or intake forms.
- [ ] Set retention periods for your main data types and document them.
- [ ] Check whether you need to register with the ODPC, and do so if required.
- [ ] List your key vendors/processors and confirm each has adequate safeguards; sign data-processing agreements where missing.
- [ ] Draft a one-page breach response plan: who to call, in what order, within what timeframe.
- [ ] Run a short training session for all current staff and volunteers.
- [ ] Identify any high-risk or new project (e.g. involving children's data, biometrics, or health data) and complete a DPIA before it launches.
- [ ] Schedule your first annual review of this Charter.

References

Data Protection Act, No. 24 of 2019 (Kenya).
Data Protection (General) Regulations, 2021 (Kenya).

International Organization for Standardization. (2017). ISO/IEC 38505-1:2017 — Information technology — Governance of IT — Governance of data — Part 1: Application of ISO/IEC 38500 to the governance of data. https://www.iso.org/standard/56639.html

Office of the Data Protection Commissioner, Kenya. (n.d.-a). Data sharing code. https://www.odpc.go.ke/wp-content/uploads/2025/03/FINAL-DATA-SHARING-CODE.pdf

Office of the Data Protection Commissioner, Kenya. (n.d.-b). Guidance note on consent. https://www.odpc.go.ke/wp-content/uploads/2025/09/Guidance-note-on-Consent.pdf

Office of the Data Protection Commissioner, Kenya. (n.d.-c). Guidance note on data protection impact assessment. https://www.odpc.go.ke/wp-content/uploads/2024/02/ODPC-Guidance-Note-on-Data-Protection-Impact-Assessment-1.pdf

Office of the Data Protection Commissioner, Kenya. (n.d.-d). Guidance note on registration of data controllers and data processors. https://www.odpc.go.ke/wp-content/uploads/2024/02/ODPC-Guidance-Note-on-Registration-of-Data-Controllers-and-Data-Processors.pdf

Office of the Data Protection Commissioner, Kenya. (n.d.-e). Guidance notes for data protection officers (DPOs). https://www.odpc.go.ke/wp-content/uploads/2026/07/ODPC-–-Guidance-Note-for-Data-Protection-Officers-DPOs.pdf

Office of the Data Protection Commissioner, Kenya. (n.d.-f). Guidance notes for data protection policies. https://www.odpc.go.ke/wp-content/uploads/2026/07/ODPC-–-Guidance-Note-for-Data-Protection-Policies.pdf

Office of the Data Protection Commissioner, Kenya. (n.d.-g). Guidance notes for processing children's data. https://www.odpc.go.ke/wp-content/uploads/2025/11/ODPC-–-Guidance-Note-for-Processing-Childrens-Data.pdf

Office of the Data Protection Commissioner, Kenya. (n.d.-h). Guidance notes on biometric data. https://www.odpc.go.ke/wp-content/uploads/2025/11/ODPC-–-Guidance-Note-on-Biometric-Data.pdf

Office of the Data Protection Commissioner, Kenya. (n.d.-i). Guidance notes on processing by MSMEs. https://www.odpc.go.ke/wp-content/uploads/2025/11/ODPC-–-Guidance-Note-on-Processing-by-MSMEs.pdf

Office of the Data Protection Commissioner, Kenya. (n.d.-j). Guidelines. https://www.odpc.go.ke/guidelines-2/

Office of the Data Protection Commissioner, Kenya. (n.d.-k). ODPC complaints management manual. https://www.odpc.go.ke/wp-content/uploads/2024/02/ODPC-Complaints-Management-Manual-1.pdf