DATA PROTECTION POLICY

PEOPLE'S PROSPERITY PARTY (PPP)

---

1. Purpose

This Policy sets out how People's Prosperity Party (PPP) ("the Party") collects, uses, stores, shares, and protects personal data in compliance with the Constitution of Kenya, the **Data Protection Act, 2019 (Kenya),** and its related and attendant regulations.

The Party is committed to respecting the privacy and data protection rights of its members, supporters, staff, volunteers, candidates, donors, and the general public that will engage with the Party.

2. Definitions

- **Personal Data:** Any information relating to an identified or identifiable person.
- **Sensitive Personal Data:** Data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family detains including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject.
- **Data Subject:** An individual whose data is processed.

- **Processing:** Any operation or set of operations which is performed on personal data or on sets of personal data whether or not by automated means, such as:
    - Collection, recording, organization, structuring;
    - Storage, adaption or alteration;
    - Retrieving, consultation or use;
    - Disclosure by transmission, dissemination, or otherwise making available; or
    - Alignment or combination, restriction, erasure or destruction.
- **Consent:** Any manifestation of express, unequivocal, free, specific and informed indication of the data subject's wishes by a statement or by a clear affirmation action, signifying agreement to the processing of personal data relating to the data subject.
- **Data Controller:** A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of processing of personal data.
- **Data Processor:** A natural or legal person, public authority, agency or other body which processed personal data on behalf of the data controller.
- **Personal Data Breach:** Breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.
- **Profiling:** Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's race, sex, pregnancy, marital status, health status, ethnic social origin, color, age, disability, religion, conscience, belief, culture, dress, language or birth; personal preferences, interest, behavior, location or movements.
- **Third Party:** Natural or legal person, public authority, agency or other body, other than the data subject, data controller, data processor or person who, under the direct authority of the data controller or data processor, are authorized to process personal data.

3. Legal Framework

This Policy is guided by the following Legal and Regulatory Framework in operation in Kenya:

- Constitution of Kenya, Article 31 (Right to Privacy)
- Data Protection Act, 2019
- Data Protection (General) Regulations, 2021
- Data Protection (Registration of Data Controllers and Processors) Regulations, 2021
- Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021
- Guidance Notes and Guidelines from the Office of the Data Protection Commissioner (ODPC)

4. Scope

This Data Protection Policy applies to all activities of the Party relating the collection, processing, storage, use sharing, and disposal of personal data, in compliance with applicable data protection laws. The policy covers;

- All Party officials, employees, volunteers, interns, contractors and consultants who have access to personal data in the course of carrying out party activities.
- All data subjects whose personal data is collected, stored or processed by the party including but not limited to members, supporters, donors, event participants, voters and volunteers.
- All types of personal data collected including but not limited to sensitive personal data, health data, biometric data and all data collected for purposes of profiling or political engagement.
- All processing activities involving personal data, whether automated or manual, including but not limited to collection, storage, organization, analysis, profiling, sharing with third parties, and disposal of data.
- All party activities within Kenya and any cross-border data transfers involving personal data of individuals located in other jurisdictions.

- All physical and electronic systems and channels used by the party to collect, process, or store personal data, including but not limited to membership databases, fundraising platforms, event registration tools, websites, social media accounts and email communication systems.
- All relationships with third-party service providers, partners and vendors that process personal data on behalf of the party, ensuring compliance with contractual and legal obligations.

5. Principles of Data Protection

The Party shall comply with the following principles of data protection outlines in the Data Protection Act:

a) Respect for the Right of Privacy

Personal data shall be processed in a manner that respects and upholds the constitutional right to privacy. The Party shall avoid unjustified intrusion into individuals' private and family affairs and ensure all data handling is proportionate and lawful.

b) Purpose Limitation

Personal data shall be collected for explicit, specified, and legitimate purposes and shall not be further processed in a manner incompatible with those purposes.

c) Data Minimization

Personal data collected shall be adequate, relevant, and limited to what is necessary for the intended purpose. The Party shall avoid excessive or unnecessary collection of information.

d) Accuracy

Personal data shall be accurate and kept up to date. Reasonable steps shall be taken to correct or erase inaccurate data without delay.

e) **Storage Limitation**

Personal data shall be retained only for as long as necessary for the purpose for which it was collected, after which it shall be securely deleted, destroyed, or anonymized.

f) **Secured against loss, unauthorized access, or misuse**

The Party shall implement appropriate and proportionate technical and organizational measures, including access controls, secure storage, confidentiality obligations, and data breach response procedures, to protect personal data based on its sensitivity and the risks associated with its processing.

g) **Lawfulness, Fairness and Transparency**

Personal data shall be processed lawfully, fairly, and transparently. The Party shall rely on a valid legal basis for processing and provide clear information on how and why personal data is collected and used.

h) **Restriction on Cross-Border Transfers**

Personal data shall not be transferred outside Kenya unless adequate data protection safeguards are in place or the data subject has provided appropriate consent, in accordance with the Act.

i) **Justification for Collection of Family or Private Information**

Where information relating to family or private affairs is required, the Party shall provide a valid explanation and ensure such collection is necessary and proportionate.

6. Lawful Basis for Processing

The Party shall only process personal data where a lawful basis exists in accordance with the Data Protection Act, 2019. Processing shall not take place unless it is justified under one or more of the following grounds:

a) **Consent of the data subject**

Where the data subject has given clear, informed and voluntary consent for one or more specified purposes.

b) **Performance of a contract**

Where processing is necessary to perform a contract with the data subject, or to take steps at the request of the data subject before entering into a contract such as membership registration or service engagement.

c) **Legal obligation**

Where processing is necessary to comply with a legal or regulatory obligation to which the Party is subject.

d) **Legitimate interests of the Party**

Where processing is necessary for the legitimate interests of the Party or a third party, provided such interests are not overridden by the rights and freedoms of the data subject.

e) **Protection of vital interests**

Where processing is necessary to protect the life or safety of the data subject or another natural person.

f) **Public interest or political activity permitted by law**

Where processing is necessary for the performance of a task carried out in the public interest, in the exercise of official authority or in the exercise of functions of a public nature, including lawful political activities.

7. Categories of Data Collected

In the course of carrying out its political and administrative functions, the Party may collect and process the following categories of personal data:

a) **Member and supporter information**

This may include names, identification details, contact information, membership status, demographic details and communication preferences for purposes of registration, engagement and internal administration.

b) **Voter engagement data**

Information collected through lawful outreach activities, surveys, petitions, canvassing and feedback initiatives used to understand public concerns, policy interests and electoral engagement.

c) **Donor and fundraising records**

Details relating to contributions, including donor identification, contact information, donation amounts, payment records and compliance documentation required under applicable electoral and financial laws.

d) **Staff and volunteer records**

Employment and engagement records, including identification details, contact information, contractual information, role assignments, background documentation where required and performance-related records.

e) **Candidate nomination data**

Personal and compliance information submitted by aspirants or nominees for Party positions or elective office, including identification documents and eligibility verification records as required by law.

f) **Event and campaign participation data**

Registration details, attendance records, photographs, media content and communication records related to Party meetings, rallies, training sessions and campaign activities.

g) **Digital data (website, social media, CCTV)**

Online identifiers, IP addresses, website usage data, social media interactions and CCTV footage collected for communication, security, analytics and operational purposes.

Sensitive data will only be processed where lawful and with appropriate safeguards according to the provisions of the Data Protection Act, 2019.

8. Rights of Data Subjects

In accordance with the Data Protection Act, 209 and specifically Section 25, every individual whose personal data is processed by the Party has the following rights:

a) **Right to be informed**

Individuals shall be informed when their data is collected, including the purpose of collection, the type of data collected, any third parties with whom it may be shared, and the safeguards in place to protect it.

b) **Right to Access**

Individuals may request access to their personal data held by the Party to verify its accuracy and lawfulness of processing.

c) **Right to Correction**

Individuals may request that any inaccurate, incomplete, or misleading personal data be corrected or updated without undue delay.

d) **Right to Object**

Individuals may object to the processing of their personal data, wholly or in part, unless the Party can demonstrate compelling legitimate grounds that override the interests, rights, and freedoms of the individual, or where processing is required for legal claims.

e) **Right to Withdraw Consent**

Where processing is based on consent, individuals may withdraw their consent at any time.

f) **Right to Request Deletion**

Individuals may request the deletion of their personal data that is no longer necessary, inaccurate, or unlawfully processed.

g) **Right to Restrict Processing**

Individuals may request that the Party limits the processing of their personal data under certain circumstances, such as while verifying its accuracy or contesting its lawfulness.

h) **Right to Data Portability**

Individuals may request their personal data in a structured, commonly used, and machine-readable format for transfer to another data controller, where technically feasible.

i) **Right to Lodge a Complaint**

Individuals have the right to lodge a complaint with the Office of the Data Protection Commissioner (ODPC) if they believe their data has been processed in violation of the law or this Policy.

9. Data Security Measures

The Party, being committed to ensuring confidentiality, integrity and availability of personal data. To achieve this, the Party shall implement a combination of technical and organizational measures as follows:

a. Technical Measures

i. **Password protection and access controls:** All systems containing personal data shall be protected by strong passwords and access permissions based on roles to prevent unauthorized access.
ii. **Encryption of sensitive records:** Personal data, especially sensitive or high-risk information, shall be encrypted during storage and transmission to prevent unauthorized disclosure.
iii. **Secure databases and backups:** Databases shall be secured against tampering, and regular backups shall be maintained to ensure data can be restored in case of loss or corruption.
iv. **Anti-malware and firewall protection**: Party IT systems shall be protected against malware, viruses, and external attacks using up-to-date anti-malware software and firewalls.

b. Organizational Measures

i. **Confidentiality agreements:** All staff, volunteers, and third-party service providers with access to personal data shall sign confidentiality agreements to formalize their responsibility to protect the data and to further ensure accountability.
ii. **Role-based access:** Access to personal data shall be granted strictly according to job roles and responsibilities, ensuring that individuals only access data necessary for their duties.
iii. **Staff training on data protection:** All personnel shall receive regular training on data protection principles, responsibilities, and best practices to reduce the risk of accidental or unlawful processing.
iv. **Secure physical filing systems**: Paper records shall be stored in locked cabinets or restricted areas, and physical access shall be controlled to prevent unauthorized viewing or theft.

10. Data Sharing and Transfers

The Party recognizes the need to protect personal data whenever it is shares with third parties or transferred across borders.

- **Sharing personal data with third-parties:** Personal data shall only be shared with authorized third parties, including service providers, partners, or contractors, under formal written agreements that clearly define the purpose of processing, obligations, and security requirements. The Party shall ensure that third parties process data in compliance with the Data Protection Act, 2019 and this Policy.
- **Cross-border transfers**: Personal data shall not be transferred outside Kenya unless there are adequate safeguards in place, or explicit consent has been obtained from the data subject. All cross-border transfers shall comply with the requirements of the Act and, where applicable, approvals or guidance from the Office of the Data Protection Commissioner (ODPC).

Additionally, the Party shall document all data sharing and transfer activities and regularly review them to ensure compliance and protection of data subjects' rights.

11. Data Retention

The Party shall retain personal data only for as long as necessary to achieve the purposes for which it was collected, including membership management, campaign activities, fundraising, compliance with legal obligations, or other legitimate Party functions.

- Once personal data is no longer required, it shall be securely deleted, destroyed, or anonymized to prevent unauthorized access or misuse.
- The Party shall implement a data retention schedule specifying retention periods for different categories of data, taking into account legal, regulatory, and operational requirements.
- Retention practices shall be regularly reviewed to ensure compliance with the Data Protection Act, 2019 and this Policy.

12. Breach Management

The Party is committed to promptly identifying, reporting, and managing personal data breaches to minimize harm to data subjects and ensure compliance with the Data Protection Act, 2019.

- **Reporting:** Any suspected or actual personal data breach must be reported immediately to the Party's Data Protection Officer (DPO) or designated authority.
- **Investigation and Containment:** The DPO shall investigate the breach, contain its impact, and take remedial action to prevent recurrence.
- **Notification:** Where required by law, the Party shall notify the Office of the Data Protection Commissioner (ODPC) and affected data subjects within the legally prescribed timelines.
- **Documentation:** All breaches, including minor incidents, shall be documented, detailing the cause, impact, remedial measures, and lessons learned.
- **Review and Prevention:** The Party shall review breaches regularly to strengthen technical and organizational safeguards and improve its breach response procedures.

These measures ensure that the Party maintains accountability, protects the rights of data subjects and minimizes the risk of data loss or misuse.

13. Data Protection Officer (DPO)

The Party may appoint a **Data Protection Officer** in line with the criteria set out in the Data Protection Act for the following purposes:

a) **Compliance Oversight**

Ensure that all personal data processing by the Party complies with applicable data protection laws and this Policy.

b) **Data Subject Requests**

Serve as the primary point of contact for handling requests from data subjects, including access, correction, deletion, and objections.

c) **Advisory Role**

Provide guidance on data protection requirements, including conducting or advising on Data Protection Impact Assessments (DPIAs).

d) **Liaison with ODPC**

Cooperate with the Office of the Data Protection Commissioner (ODPC) and other relevant authorities on matters relating to data protection.

e) **Capacity Building**

Train and support staff and volunteers involved in data processing to ensure they understand and comply with data protection requirements.

14. Complaints and Enforcement

Any individual who believes that their personal data has been processed in violation of this Policy or the Data Protection Act, 2019 may:

- **Lodge a Complaint with the Party:** Contact the Party's Data Protection Officer (DPO) to report concerns or seek resolution.
- **Lodge a Complaint with the ODPC:** Approach the Office of the Data Protection Commissioner for investigation or enforcement action.

The Party shall investigate complaints promptly, take corrective action where necessary, and ensure that data subjects are informed of outcomes in a timely manner

15. Review

This Policy shall be reviewed:

- **Annually**: to ensure continued relevance and compliance with best practices and legal obligations.
- **When there are changes** in data protection laws, regulations, or the Party's operations that affect the processing of personal data.

All revisions shall be approved by the Party leadership and communicated to staff, volunteers, and other relevant stakeholders.

Approved by:

Moses Odero Siguda
Secretary General
PEOPLE'S PROSPERITY PARTY (PPP)