



## OFFICE OF THE DATA PROTECTION COMMISSIONER

# GUIDANCE NOTES FOR ELECTORAL PURPOSES

## DEFINITIONS

**"Act"** means the Data Protection Act, No 24. of 2019.

**"Commission"** means the Independent Electoral and Boundaries Commission as established in Article 88 of the Constitution of Kenya, 2010.

**"Consent"** means any manifestation of express, unequivocal, free, specific and informed indication of the data subject's wishes by a statement or by a clear affirmative action, signifying agreement to the processing of personal data relating to the data subject.

**"Constitution"** means the Constitution of Kenya, 2010.

**"Data Commissioner"** means the person appointed pursuant to section 6 of the Act.

**"Data Controller"** means 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"** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.

**"Data Subject"** means an identified or identifiable natural person who is the subject of personal data.

**"Election"** means the act of selecting a vote of a person or persons from among a number of candidates to fill an office or to a membership of any political party and includes a presidential, parliamentary or county election.

**"Member"** means a registered member of a political party as required under the Political Parties Act No. 11 of 2011.

"**Member register**" means a list of the names, addresses and identification particulars of members of a political party as required under Section 7(2)(f)(i) of the Political Parties Act No. 11 of 2011.

**"Office"** means the Office of the Data Protection Commissioner as established in section 5 of the Act.

"**Office of the Registrar of Political Parties**" means the Office of the Registrar whose bearer is the Registrar of Political Parties as established in Section 33 of the Political Parties Act No. 11 of 2011.

**"Personal Data"** means any information relating to an identified or identifiable natural person.

**"Governance Organisation"** means all stakeholders and entities involved in elections and the collection of voter data including the Office of the Registrar of Political Parties, Political Parties, Civil Society Organisations, volunteers, observers.

**"Political Party"** means an association contemplated in Part 3 of Chapter Seven of the Constitution.

**"Processing"** means any operation or sets of operations which is performed on personal data or on sets of personal data whether or not by automated means, such as:

(a) collection, recording, organisation, structuring;

(b) storage, adaptation or alteration;

(c) retrieval, consultation or use;

(d) disclosure by transmission, dissemination, or otherwise making available; or

(e) alignment or combination, restriction, erasure or destruction.

**"Register of Voters"** means a current register of persons entitled to vote at an election prepared in accordance with section 3 of the Elections Act No 24 of 2011 and includes a register that is compiled electronically (Section 2 Elections Act No 21 of 2011).

**"Registrar"** means the Registrar of political parties appointed under section 33 of the Political Parties Act No. 11 of 2011.

**"Sensitive Personal Data"** means data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject.

**"Voter"** means a person whose name is included in a current register of voters (section 2 Elections Act No 24 of 2011).

## 1. INTRODUCTION

The Office of the Data Protection Commissioner (herein referred to as 'the Office' or 'ODPC') is a State Office in accordance with Article 260 (q) of the Constitution. The Office was established under Section 5(1) of the Data Protection Act No. 24 of 2019 (herein referred to as 'the Act'). The Act was introduced to give effect to Article 31(c) and (d) of the Constitution.

## 2. MANDATE OF THE OFFICE

The mandate of the Office of the Data Protection Commissioner derived from the Act and includes, *inter alia*:

(a) regulate the processing of personal data;
(b) ensure that the processing of personal data of a data subject is guided by the principles set out in section 25 of the Act;
(c) protect the right to privacy of individuals resident in Kenya;
(d) establish the legal and institutional mechanism to protect personal data; and
(e) provide data subjects with rights and remedies to protect their personal data from processing that is not in accordance with the Act.

## 3. VISION

To enhance public trust and be an effective personal data protection regulator.

## 4. MISSION

Safeguarding data protection rights through provision of oversight, public awareness and promotion of self-regulation.

## 5. CORE VALUES

(a) To uphold Values of Public Service as set out in Article 10, and in Chapter Six of our Constitution;
(b) To act lawfully consistent with our Constitution, and within duties and responsibilities set out in the Data Protection Act 2019;
(c) Be consultative in style, transparent and responsive to all stakeholders;
(d) To observe the highest standards of impartiality, integrity and objectivity in leading data processing business while maintaining its independence at all times;
(e) To cause to have in place effective systems of internal controls for effective economical and proper performance of the functions of the Office.

## 6. OVERVIEW

The Data Protection Act, 2019 ("the Act") and Data Protection and Privacy Policy 2019 espouses the seven data protection principles, namely:

(i) Lawfulness, fairness and transparency - All personal data needs to be processed fairly and lawfully, and in a way that is completely transparent. Simply put, an entity is responsible for informing data subjects (natural persons) that they intend to collect data, how the data will be used and whether the data is to be passed on/disclosed to a third party and who the said third party is.

(ii) Purpose limitation - Data collection must be for a reason that is lawful and transparent, it must not be processed in a way that is at odds with the original purpose.

(iii) Data minimisation – Entities which collect data must make sure that the information collected is not excessive, given the purpose of collection. Therefore, the personal data should be adequate, relevant and not excessive.

(iv) Accuracy – Entities collecting data are required to ensure that information held is up-to-date and accurate, which requires a regular review of data held for the purpose of amending any out dated or inaccurate information. Individuals have the right to have inaccurate data about them erased.

(v) Storage Limitation – Data relating to a data subject must be deleted or anonymised once it has served its purpose, subject to the entity having any other grounds for retaining the information.

(vi) Integrity and confidentiality- Entities collecting or processing data have a responsibility to ensure that reasonable steps have been taken to implement security safeguards. This includes ascertaining the integrity of all employees authorised to access an individual's personal information,

(vii) Accountability – Entities collecting and/or processing data must ensure that their practices are compliant with the other principles.

Engagement and communication with voters is crucial for any democratic society. There are a number of legislative frameworks that detail the requirements and importance of registering voters for the , electoral processes, including the maintenance of registers of voters, voter identification, results transmission and maintaining party membership registers. Electoral laws, which include Elections Act, Independent Electoral and Boundaries Commission Act, Political Parties Act and other subsidiary regulations, permit the processing of personal data (including name, address and polling station) and, in the case of the Commission, biometric data (sensitive personal data) which is contained on the Register of Voters or political party member registers for electoral purposes. The various entities permitted to collect personal data in accordance with the aforementioned electoral laws include the Independent Electoral and Boundaries Commission, Office of the Registrar of Political Parties and the various registered Political Parties. Additionally, electoral laws mandate the Commission to make the Register of Voters available to the public for inspection, and use voter identification during elections. Similarly, the Office of the Registrar of parties is required under the Political Parties Act to

The rights afforded by the Data Protection Act are not absolute in nature and are recognised as such in the Act. Therefore, public interest in ensuring the effective operation of a democratic society must be balanced with a data subject's right to data protection. Further, there is a right to recognise that an individual's rights may be limited or restricted by certain legislative provisions or other overarching interests in statute. The Act recognises these exemptions or restrictions, as they apply to processing of personal data.

## 7. SCOPE AND PURPOSE OF THIS GUIDANCE NOTE

The Constitution of Kenya in Article 31 provides that "*Every person has the right to privacy, which includes the right not to have—*

*(c) information relating to their family or private affairs unnecessarily required or revealed; or*

*(d) the privacy of their communications infringed.*"

A number of international instruments such as the International Covenant on Civil and Political Rights also give universal recognition to the importance of safeguarding the right to privacy. The Act provides a legislative framework that promotes the protection of the right to privacy.

It is key, for the integrity of elections and democracy, that all organizations and institutions involved in electoral processes including; voter registration, inspection of the Register of Voters, recruitment of members by political parties and political campaigning, process personal data and/or sensitive personal data, as the case may be, in a manner that is compliance with the Data Protection Act. The Act is the overarching law on the right to privacy and data protection in Kenya and, therefore, applies to all entities and persons processing any personal data of persons resident in Kenya.

Therefore, Data Protection Legislation is applicable to all stakeholders engaged in the election process including, but not limited to the Commission; and Political Parties, the Office of the Registrar of Political Parties, Civil Society organisation, Faith based organisation, observers and volunteer (hereafter collectively referred to as **"governance organisations**"). All governance organisations and the Commission should process personal data lawfully, fairly, only for specified legitimate purposes. The data processing shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair balance between all interests concerned, and the rights and freedoms of data subjects.

This Guidance Note was developed to assist data controllers and data processers dealing with voters personal data, including sensitive personal data, members of political parties personal data to understand their obligations under the Act. This Guidance Note applies solely to the processing of personal data on voters (or potential voters) and the processing of personal data for the purposes of creation and maintenance of member registers. This Guidance Note takes account of:

- The Act; and
- The Data Protection and Privacy Policy; and

- International best practice.

## 8. LAWFUL BASIS

The Act provides for eight lawful bases for processing personal data. Section 30 of the Act requires that personal data shall only be processed if at least one of eight legal grounds listed in that Section apply. In particular, personal data shall only be processed (a) based on the data subject consents to the processing for one or more specified purposes; or if the processing is necessary —

(b) for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject before entering into a contract;
(c) for compliance with any legal obligation to which the controller is subject;
(d) in order to protect the vital interests of the data subject or another natural person;
(e) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(f) the performance of any task carried out by a public authority;
(g) for the exercise, by any person in the public interest, of any other functions of a public nature;
(h) for the legitimate interests pursued by the data controller or data processor by a third party to whom the data is disclosed, except if the processing is unwarranted in any particular case having regard to the harm and prejudice to the rights and freedoms or legitimate interests of the data subject; or
(i) for the purpose of historical, statistical, journalistic, literature and art or scientific research.

Broadly, the collection of data for fulfilment of mandates and obligations enumerated in the electoral laws that relate to voter's and member personal data include:

1. **Legal obligation**:

   This lawful basis would arise where a data controller or data processor is obliged to process personal data so as to comply with an existing law, including any obligation under common law.

   Governance organisations and the Commission should be able to identify the obligation in question, either by reference to the specific legal provision or else by pointing to an appropriate source of advice or guidance that sets it out clearly. A Governance organisation or the Commission will then have the onus to ensure that the overall purpose of the processing must be to comply with a legal obligation which has a sufficiently clear basis in either common law or statute.

2. **Public task**:

   This lawful basis covers mandates of public institutions that are set out in legislations, including subsidiary legislation, in Kenya. This lawful basis also covers the performance of specific functions and powers as provided for and set out in Kenyan legislation. For

example: Section 4 of the Elections Act No. 24 of 2011 sets out a requirement for the Independent Electoral and Boundaries Commission ("Commission") to compile and maintain the Register of Voters , which is to contain "*such information as the Commission shall prescribe*".

The processing of personal data by the Commission is likely to fall under the 'lawful basis' that it is 'necessary for the performance of a task carried out in the public interest or in the exercise of the official authority vested in the controller' pursuant to the electoral laws. The Commission has an overall statutory duty to maintain the Register of Voters and to administer elections in accordance with the Elections and its mandate under the Constitution and the Independent Electoral and Boundaries Commission Act, No. 9 of 2011(the "IEBC Act"). It is important to note that section 25 of the IEBC Act was amended with the passage of the Data Protection Act to provide that '*the principles of personal data protection set out in the Data Protection Act shall apply to the processing of personal data of voters*.'

The Commission and Governance organisations will need to consider the appropriate lawful basis for the processing of personal data not covered by electoral laws, and be able to demonstrate to the Office, that relevant the Commission or governance organisation has the requisite lawful basis.

3. **Legitimate interests**:

The processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks).

4. **Consent**:

Consent can only be an appropriate lawful basis if a data subject is offered control and is offered a genuine choice with regard to accepting or declining the terms offered or declining them without detriment. Consent as defined in Section 2, details the minimum criteria; namely that it must be:

a. Any manifestation of express, unequivocal, free, specific;
b. informed indication of the data subject's wishes; and
c. by a statement or by a clear affirmative action, signifying agreement

The Act further provides that a data controller or processor bears the burden of proof for establishing a data subject's consent to the processing of their personal data for a specified purpose and, unless otherwise provided under this Act, a data subject shall have the right to withdraw consent at any time.

*For further information see the Office's Guidance Note on Consent (available on www.odpc.go.ke ).*

**5. Sensitive personal data:**

Section 44 and 45 of the Act provide for instances in which it is acceptable to process sensitive information. The Act prescribes as follows:

Section 44: "*No category of sensitive personal data shall be processed unless section 25 applies to that processing.*

Section 45: "*Without prejudice to section 44, sensitive personal data of a data subject may be processed where —*

*(a) the processing is carried out in the course of legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that —*

*(i) the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes; and*

*(ii) the personal data is not disclosed outside that body without the consent of the data subject.*

*(b) the processing relates to personal data which is manifestly made public by the data subject; or*

*(c) processing is necessary for—*

*(i) the establishment, exercise or defence of a legal claim;*

*(ii) the purpose of carrying out the obligations and exercising specific rights of the controller or of the data subject; or*

(iii) *) protecting the vital interests of the data subject or another person where the data subject is physically or legally incapable of giving consent.*"

The conditions set out in Section 44 and 45 do not replace or override the usual rules on having a lawful basis for processing. Instead, they operate as an additional layer of conditions for processing sensitive personal data.

Where the Commission or a governance organisation is processing sensitive personal data, they will still be required to identify a lawful basis for the processing in exactly the same way as for any other personal data. Further, the commission or the governance organisation will need to be able to demonstrate that the processing has been done in accordance to the principles set out in Section 25 of the Act.

In addition to the above, processing of sensitive personal data is considered to be high risk or "*likely to have a high risk to the rights and freedoms of a data* subject". Therefore, the Commission and any governance organisation permitted under law to collect biometric data must conduct Data Protection Impact Assessments (discussed below). Further, Commission and any governance organisations that collects sensitive personal data will need to put in place more robust safeguards to mitigate any impact or risks to the data subject.

**The Register of Voters**

The Elections Act and the IEBC Act require that the Commission maintain a Register of Voters. Further, the Commission is mandated to make the Register of Voters accessible to the public

and published in accordance with the provisions of the Elections (Registration of Voters) Regulations, 2012.

The Elections Act and the Independent Electoral and Boundaries Commission Act do not provide for statutory opt-out mechanisms for voters registered on the Register of Voters. Therefore, processing personal data for inclusion on the Register of Voters, other than the collection of same, is done on the lawful basis that it is necessary to perform a public task.

The Elections Act does not give a statutory right for the collection of voter's personal data or sensitive personal data without obtaining of consent from the data subject. The data protection conditions for consent will be required for the collection of personal and sensitive personal data, as registration of as a voter is not a mandatory obligation. However, statutory obligations will govern other aspects of the processing and use of the personal data (and sensitive personal data) contained in the Register of Voters and maintained in accordance with the Elections Act.

**The Register of Members**

The Political Parties Act under section 7(2)(f)(i) requires that political parties submit to the Registrar a list of the names, addresses and identification particulars of all its members. Additionally, the same Act requires that the Registrar of Political Parties to "*verify and make publicly available the list of all members of political parties*".

The Political Parties Act does not give a statutory right for the collection of member's personal data without obtaining of consent from the data subject. However, the aforementioned Act does give political parties the duty to transfer such personal data to the Registrar and provides that the Registrar has a statutory duty to verify and publish the member register.

Therefore, in obtaining member data, Political Parties must also rely on consent prior to collecting member's personal data for the purpose of inclusion in, and maintaining, a member register and transferring same to the Registrar of Political Parties.

## 9. DUTY TO NOTIFY

One of the key principles of data protection is transparency. The personal data processed by the Commission and governance organisations or other electoral stakeholders shall be processed fairly and in a transparent manner. At the time of collection, the Commissioner, representatives of governance organisations and electoral stakeholders must comply with the obligations under Section 29 of the Act which states that data controllers and data processers have a duty to notify data subjects of the following prior to the collection of personal data, in so far as is practicable:

(a) the rights of data subject specified under section 26;
(b) the fact that personal data is being collected;
(c) the purpose for which the personal data is being collected;
(d) the third parties whose personal data has been or will be transferred to, including details of safeguards adopted;
(e) the contacts of the data controller or data processor and on whether any other entity may receive the collected personal data;

(f) a description of the technical and organizational security measures taken to ensure the integrity and confidentiality of the data;
(g) the data being collected pursuant to any law and whether such collection is voluntary or mandatory; and
(h) the consequences if any, where the data subject fails to provide all or any part of the requested data.

The above information should be provided to data subjects to enable them to understand how their personal data is used, this can be achieved by a **privacy notice**. It is advised that the information in a privacy notice must be provided in clear plain language and be provided free of charge. The privacy notice must be kept up to date to meet any changes in your approach to processing data.

## 10. RIGHTS OF A DATA SUBJECT

The Data Protection Act affords a number of rights to a data subject. These are:

(a) to be informed of the use to which their personal data is to be put (*section 26*);
(b) to access their personal data in custody of data controller or data processor; to object to the processing of all or part of their personal data (*section 26*);
(c) to object to processing of all or part of their personal data (*section 26*);
(d) to correction of false or misleading data (*section 26*);
(e) to deletion of false or misleading data about them (*section 26*);
(f) the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning or significantly affects the data subject (*section 35*);
(g) to data portability (*section 38*);
(h) to request rectification of their personal data or erasure (right to be forgotten) (*section 40*).

### A. Right to be informed

Voters and members are entitled to be informed how their personal information was obtained, and from what source. This is in addition to the duty to notify under Section 29 of the Data Protection Act.

### B. Right to access their personal data

Voters and members should be able to obtain on request and without excessive delay, confirmation of the processing of personal data relating to him or her, and access to their personal data in an intelligible form.

### C. Right to object to processing, correct false or misleading data, deletion of false or misleading data

Voters and members should be able to object to the processing of data on him or her by an electoral organisation, and to request rectification or erasure/ deletion, as the case may be, if the data is inaccurate, obsolete, incomplete, false or misleading.

The Act provides for the "right to object" in section 26. This means that the data subject can object to the processing of their personal data. This right **does** apply when processing is required for the performance of a public task (such as maintaining the voter register or publishing of a member register).

The right to object to processing cannot however be applied to information where the collection of or the nature of the processing is specified in electoral laws. For example in relation to the Register of Voters, the data subject can object to the processing of their email or telephone contact details but not to the use of their name, identification, address or such other personal data as the Commission deems necessary, within reason, for the purpose of maintaining and publishing the Register of Voters, if the data subject is a registered voter. The same would apply for the publication of a member register by the Office of the Registrar of Political Parties.

**D. Right not to be subject to automated decision making**

Voters or members have the right not to be subject to decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration or without human intervention, if such decision is likely to have produce legal effects or other affects that could significantly affect the voter or member. **Where voters receive or subjected to automated delivery of digital political advertising, the voters have the right to know why they are receiving such advertising material or receiving the "ads".**

**E. Right to rectification of personal data or erasure**

Voters and members are entitled to know about the reasoning underlying the processing of their personal data by political campaigns. This may be particularly important where a voter is contacted by a political party with whom they have not had a prior relationship.

Voters and Members who object to data processing for political marketing purposes are entitled to the unconditional erasure or removal of the personal data covered by that objection.

The Act gives data subjects the right of erasure. This right is commonly referred to as the "right to be forgotten". This provision means that a data subject can request that their personal data be erased or deleted without undue delay. The right to be forgotten **does not** apply when processing is required for the performance of a public task (such as the maintaining of Register of Voters by the Commission or public member register by the Registrar) or where it is necessary for archival in the public interest. However, it can apply to the deletion of certain aspects of personal data such as email or other contact information that is not required for the maintenance of a Register of Voters or Member Register.

The right to be forgotten **does** apply for processing of member data carried out by Political Parties. The Political Party then has a duty to inform the Registrar of Political Parties to delete any personal data held by the Registrar including that which is contained in the public member register.

## 11. PRIVACY BY DEFAULT OR DESIGN

The Act, in section 41, provides that "*every data controller or data processor shall implement appropriate technical and organisational measures which are designed —*
*(a)to implement the data protection principles in an effective manner; and*
*(b) to integrate necessary safeguards for that purpose into the processing."*

Further the Act states:

> "*(3) A data controller or data processor shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which is necessary for each specific purpose is processed, taking into consideration*
>
> *(a) the amount of personal data collected;*
>
> *(b) the extent of its processing;*
>
> *(c) the period of its storage;*
>
> *(d) its accessibility; and*
>
> *(e) the cost of processing data and the technologies and tools used.*
>
> *(4) To give effect to this section, the data controller or data processor shall consider measures such as —*
>
> *(a) to identify reasonably foreseeable internal and external risks to personal data under the person's possession or control;*
>
> *(b) to establish and maintain appropriate safeguards against the identified risks;*
>
> *(c) to the pseudonymisation and encryption of personal data;*
>
> *(d) to the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;*
>
> *(e) to verify that the safeguards are effectively implemented; and*
>
> *(f) to ensure that the safeguards are continually updated in response to new risks or deficiencies."*

Data protection by design is an approach that ensures data controllers and data processers consider privacy and data protection issues at the design phase of any system, service, product or process and then throughout the lifecycle. Data protection by default requires data controllers and processors ensure that only data that is necessary to achieve your specific purpose is processed. Data protection by default means data controllers and processors need to specify this data before the processing starts, appropriately inform individuals and only process the data needed for the specific purpose.

The Commission and governance organisations are usually involved in processing voters' data on a large-scale. Applying appropriate security measures to voter and member data, and its processing environments both at rest and in transit, is vital to ensure voters' and members'

data are protected to the highest standards. Security measures should take into account the current state of the art data-security methods and techniques in the field of data processing. Their cost should be commensurate with the seriousness and probability of the potential risks.

The Commission and governance organisations often engage in the sharing of data on voters and members with large numbers of campaign volunteers, contractors and employees. The Commission and governance organisations should take appropriate security measures to ensure against accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data. These measures include: training in privacy and security; access controls; confidentiality agreements; and physical controls.

Where data is processed by third party service providers, the Commission and governance organisations must remain aware of their ongoing responsibilities as data controllers. Controllers must demonstrate due diligence to establish the third party's ability to protect personal data confidentiality.

Risk assessment prior to processing must assess whether data is protected against unauthorised access, modification and removal/destruction. Risk assessment should seek to achieve outcomes that embed high standards of security throughout the processing. Such an assessment must be informed by considerations of necessity and proportionality, and the fundamental data protection principles across the range of risks including physical accessibility, networked access to devices and data, and the backup and archiving of data.

The Commission and governance organisations should train all workers, including employees and temporary volunteers, on the importance of privacy and security measures. Each employee or volunteer should sign confidentiality agreements.

## 12. DATA PROTECTION IMPACT ASSESSMENT

The carrying out of a DPIA is only mandatory where processing is "*likely to result in a high risk to the rights and freedoms of data subjects*". In cases where it is not clear whether a DPIA is required, it is recommended that a DPIA is carried out nonetheless as a DPIA is a useful tool to help data controllers and/or data processors comply with data protection law. In addition to the aforesaid, the Act requires that all data controller and processers implement appropriate technical and organisational measures and integrate appropriate safeguards to ensure the adequate protection of personal data of data subjects.

*The Office has published a Guidance Note on Data Protection Impact Assessments on www.odpc.go.ke. The Guidance Note includes the form which a Data Protection Impact Assessment should be submitted and guidance on when it should be submitted.*

## Appendix 1 – Summary checklist of actions

This checklist summarises the actions highlighted throughout this Guidance Note for your reference.

| # | Action | Y/N | Comment |
|---|---|---|---|
| **1.** | Contact the Office to support you in meeting your obligations and utilise the available material on www.odpc.go.ke | | |
| **2.** | Review your processing activities. How can you **demonstrate** you are processing data in accordance with section 25? | | |
| **3.** | Determine the lawful basis on which you are collecting/processing **all** personal data (in accordance with sections 25 and 30. If collecting sensitive personal data in line with sections 25, 30, 44 and 45 of the Act. | | |
| **4.** | When seeking consent ensure that you do so in line with the Act (see www.odpc.go.ke for Guidance Note on Consent) | | |
| **5.** | If you are processing data for the performance of a public task, determine and record what the basis for that public task is. | | |
| **6.** | If you are processing data for compliance with a legal obligation, determine, record and be able to demonstrate what the basis of the legal obligation is. | | |
| **7.** | Review your own forms and letters to check they contain appropriate data protection notices | | |
| **8.** | Ensure you are not using personal data for unrelated purposes | | |
| **9.** | Review your existing privacy notices to ensure they remain compliant with your organisation's Duty to Notify and detail the lawful basis you are relying on for processing | | |
| **10.** | Undertake a Data Protection Impact Assessment (DPIA) as a matter of best practice when you undertake a new process (see Guidance Note on DPIAs on www.odpc.go.ke ) | | |
| **11.** | Review existing DPIA | | |

| # | Action | Y/N | Comment |
|---|---|---|---|
| **12.** | Ensure that all staff training (core team, canvassers, polling station staff) reflects current data protection requirements | | |
| **13.** | Understand that a data subject is entitled to see personal information that is held about them | | |
| **14.** | Ensure that there are provisions and mechanisms put in place to allow data subjects to exercise their rights under the Act | | |
| **15.** | Ensure that you have put appropriate data protection/ privacy by design and default safeguards as prescribed in section 41 of the Act | | |
| **16.** | Understand the penalties for failure to comply with data protection legislation | | |
| **17.** | Ensure your plans and risk registers highlight the safeguards you have to avoid a data breach | | |
| **18.** | Ensure you have procedures to detect, report and investigate a data breach | | |


**OFFICE OF THE DATA PROTECTION COMMISSIONER**

P.O. BOX 30920-00100

NAIROBI

info@odpc.go.ke | www.odpc.go.ke