REPUBLIC
OF
KENYA

OFFICE OF
THE DATA PROTECTION
COMMISSIONER

GUIDANCE NOTE ON

CONSENT

GUIDANCE NOTE ON CONSENT

Definitions

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

"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.

"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.

"Office" means the Office of the Data Protection Commissioner as defined in sections 2 and 5 of the Act.

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

"Processing" means any operation or sets of operations which is performed on personal data or on sets of personal data whether 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.

"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.

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 the Constitution.

(b) To act lawfully consistent with the Constitution, and within the 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 eight data protection principles, namely:

(i) Right to privacy - Every data controller or data processor shall ensure that personal data is processed in accordance with the right to privacy of the data subject.

(ii) 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.

(iii) 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.

(iv) 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.

(v) 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 outdated or inaccurate information. Individuals have the right to have inaccurate data about them erased.

(vi) 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.

(vii) 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,

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

Consent is an essential element of Data Protection legislation and principles. Pursuant to the Act, Data Controllers and Data Processors are required to obtain consent for the collection, use and disclosure of personal data, collectively referred to as processing.

The Act provides for consent from a data subject as one of 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. 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 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) 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 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.

7. SCOPE AND PURPOSE OF GUIDELINES

The Act gives a degree of primacy to Consent, and states that processing should subject to a data subject's consents to the processing for one or more specified purposes. Further, the Act makes provision for when consent should be obtained from data subjects. Data Controllers and Data Processors are required to develop consent processes that respect of their statutory obligations as well as the nature of their relationship with the data subjects from whom they collect information. However, in designing such a process, we expect data controllers and data processors to be guided by the provisions of the Act.

The Guidelines were developed to assist data controllers and data processers understand their duties under the Act and understand and appreciate their obligations as relates to obtaining Consent.

These Guidelines take account of:

- The Act; and
- The Privacy and Data Protection Policy; and
- International best practice.

8. CONSENT

Prior to the commencement of any activities that involve processing of personal data, a data controller or data processor must always take consider what would be the appropriate lawful basis for the envisaged processing. As aforementioned, Consent is one of eight lawful bases under the Act.

Consent can only be an appropriate lawful basis if a data subject is offered control and is offered a genuine choice about accepting or declining the terms offered or declining them without detriment. When asking for consent, a data controller or data processor has the duty to assess whether it will meet all the requirements to obtain valid consent. If obtained in full compliance with the Act, consent is a tool that gives data subjects control over whether personal data concerning them will be processed. However, data controllers and data subjects, run the risk of a data subject's consent, being deemed an invalid basis for processing, rendering the processing activity unlawful, if the control becomes illusory.

Inviting a person to accept a data processing operation should be subject to rigorous requirements, since it concerns the fundamental rights of data subjects. Obtaining consent does not negate or in any way diminish the data controller's and data processor's obligations to observe the principles of processing enshrined in the Act and, in particular, Section 25 of the Act with regard to fairness, necessity and proportionality, as well as data quality. Even if the processing of personal data is based on consent of the data subject, this would not legitimise collection of data, which is not necessary in relation to a specified purpose of processing and be fundamentally unfair.
Consent as defined in Section 2, details the minimum criteria; namely that it must be:

1. Any manifestation of express, unequivocal, free, specific.
2. informed indication of the data subject's wishes; and
3. by a statement or by a clear affirmative action, signifying agreement to the processing of personal data relating to the data subject.

The element "free" implies real choice and control for data subjects. It would follow that if the data subject had no real choice, feels compelled to consent or will endure negative consequences if they do not consent, then consent

will not be valid. Further, consent will not be considered to be free if the data subject is unable to refuse or withdraw his or her consent without detriment. Any element of inappropriate pressure or influence upon the data subject which prevents a data subject from exercising their free will, shall render the consent invalid.

The Act provides for consent to be "informed". Therefore, consent by the data subject must be based on an understanding of the processing activities and its implications on the rights of the data subject. Data Controllers or data processors have an obligation to ensure that accurate and full information regarding the nature of the personal data to be processed, purposes of the processing, the recipients of possible transfers, the rights of the data subject, consequences of not consenting to the processing in question and any other relevant information is provided to a data subject to enable the data subject to give "informed" consent.

A data subject must be able to easily understand what they are consenting to. Therefore, data controllers and/or processor must clearly and simply, in a plain language and manner data subjects will understand, explain to data subjects exactly what they are consenting. The request for consent needs to be prominent, concise, separate from other terms and conditions, and in plain language. If the request for consent is vague or difficult to understand, then it will likely fail to meet the minimum criteria required to obtain valid consent and would, therefore, be invalid.

To ensure that data controllers and data processors obtain specific and informed consent, they must, at a minimum provide the following:

i. The data controller and data processor's identity: This means a data controller or data processor must identity itself, and also name any third party who will be relying on the consent.
ii. The purposes of the processing: a consent request must specifically cover all purposes for which the consent is sought.
iii. The processing activities: Granular consent options for each separate type of processing unless those activities are clearly interdependent. Data controllers and/or processors must specifically cover all processing activities, at a minimum.
iv. The right to withdraw consent at any time: details of how a data may exercise their right to withdraw consent should be provided.

Pursuant to the Act, Consent must be "a manifestation of express… by a statement or by clear affirmative action". It is clear from the definition that Consent requires a statement from the data subject or a clear affirmative act, which means that it must always be given through an active motion or declaration. It must be obvious that the data subject has consented to the particular processing. A "clear affirmative act" means that the data subject must have taken a deliberate action to consent to the particular processing. The Act does not go so far as to prescribe or give additional guidance as to how consent may be collected. However, it is commonplace for consent to be collect through a written or (a recorded) oral statement, including by electronic means.

Consent should include an indication of a data subject's wishes signifying their agreement. The notion of "indication" implies a need for action. In taking a contextual and ordinary meaning view of the definition, the other elements required for consent such that it be "unequivocal" support this interpretation.

A. CONDITIONS FOR CONSENT

The Act in section 32 sets out Conditions for consent which are:

"(1) A data controller or data processor shall bear the burden of proof for establishing a data subject's consent to the processing of their personal data for a specified purpose.

(2) Unless otherwise provided under this Act, a data subject shall have the right to withdraw consent at any time.

(3) The withdrawal of consent under sub-section (2) shall not affect the lawfulness of processing based on prior consent before its withdrawal.

(4) In determining whether consent was freely given, account shall be taken of whether, among others, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."

The Act does not stipulate how and what methods should be put in place to ensure compliance with the provisions relating to Consent. Therefore, data controllers and data processors may develop methods to comply that are appropriate and align with their daily operations.

However, the duty to demonstrate that a data subject's consent has been

obtained valid consent from a data subject falls upon the data controller and/or data processor. A data controller and/or data processor should easily be able to show that there is a link between the consent and the processing. Therefore, such a duty should not, of itself, lead to excessive amounts of additional data processing.

The Act places an onus on data controllers and/or data processors to prove that valid consent was obtained from the data subject. The Act is silent on how this is to be done. However, data controllers and data processors must be able to prove that a data subject in a given case has consented. For as long as the data controller and or data processor continues to process the personal data, including holding the personal data, the obligation to demonstrate consent exists endures. Thereafter, following the completion on the processing activity, data controllers and processors are advised to retain such proof of consent for only as long as it is strictly necessary for compliance with a legal obligation or for the establishment, exercise, or defence of legal claims, in accordance with the Act. An example is the keeping of records of consent statements by a data controller or processor, to demonstrate when consent was obtained and what information was provided to the data subject at the time of obtaining consent.

The obligation to demonstrate that valid consent was obtained is based on the data protection principle of accountability. Therefore, data controllers and data controllers must be accountable with regard to obtaining valid consent from data subjects and the consent mechanisms they have put in place.

Data Subjects have a right to withdraw consent, subject to legal or contractual restrictions which are outlines in Section 32(3). Withdrawal of consent by a data subject should be followed by a stop to any further processing activity that relates to that data subject's personal data by the data controller and/or data processor. Retention of any personal data following the withdrawal of consent shall only be for as long as it is strictly necessary for compliance with a legal obligation or for the establishment, exercise, or defence of legal claims, in accordance with the Act.

B. AT WHAT POINT SHOULD CONSENT BE SOUGHT?

Whilst the Act does not explicitly state that consent should be obtained prior to the commencement of processing activities a common sense

interpretation of the Act, the phrase "a data controller or data processor shall not process personal data, unless-" in Section 30 of the Act suggests that a valid lawful basis must be present before starting a data processing. Therefore, consent should be given prior to the processing activity.

It may be sufficient to ask for a data subject's consent once. However, data controllers and/or data processors must obtain a new and specific consent if purposes for data processing change after consent was obtained or if an additional purpose is envisaged. Consent must also be requested when the purpose of the processing changes. In this case the information to be provided will have to focus on what is needed in the specific context, in relation to the purpose. Consent, which was validly obtained, prior to the commencement of the Act and is compliant with the provisions of the Act will continue to be valid.

Data controllers and data processors must keep consents under review and refresh them if their purposes or activities evolve beyond what was originally specified when seeking a data subject's consent. Consent will cease to be specific if details of the processing activity change. In other words, there is no such thing as 'evolving' consent. This applies even if the new purpose is considered 'compatible' with the data controller's and/or data processor's original purpose. Therefore, should the processing activity change, and a data controller or data processor is relying on consent, it will need to either obtain new/fresh specific consent, or else identify a new lawful basis for the new purpose.

C. INTERACTION BETWEEN CONSENT AND OTHER LAWFUL BASIS

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. The application of one of these eight bases must be established prior to the processing activity and in relation to a specific purpose.

It is key to note that where a data controller chooses to rely on consent for any part of the processing, they must be prepared to respect that choice and stop that part of the processing if an individual withdraws consent. A data controller and/or data processor must be consistent in its application of one lawful basis over another. Therefore, a data controller or data processor should not retrospectively utilise another favourable lawful basis to justify processing, where there is an issue relating to the validity of consent. The Act imposes a duty to notify under section 29. Therefore, the data controller

must have decided in advance of processing what the applicable lawful basis is the data controller or data processor is relying upon at the time of processing of personal data.

The lawful basis of consent is likely to overlap with other lawful bases. For example, a data controller and or data processor may have a statutory obligation to process certain personal data. However, the data controller and/or data processor wishes to process more personal data than is required under the statute for a specified purpose. In this case, there is a need to adopt a hybrid models, where consent is sought for any processing that may be deemed to be beyond statutory requirement and the data subject advised of the statutory requirement and its limitations with respect to the processing activity.

D. CONSENT IS NOT A SILVER BULLET

Data controllers and data processors are advised that consent does not waive or negate their obligations under the Act. If a data subject consented to have their personal data being processed contrary to legal requirements, the data subject would still be considered in contravention of those requirements.

The Office of the Data Protection Commissioner.
P.O. Box P.O. Box 30920 - 00100 NAIROBI, CA Centre
Email. info@odpc.go.ke
Telephone: +254 000 00 00 00