LEGAL NOTICE NO. 263

THE DATA PROTECTION ACT

(*No*. 24 *of* 2019)

THE DATA PROTECTION (GENERAL) REGULATIONS, 2021

ARRANGEMENT OF REGULATIONS

Regulation

THE DATA PROTECTION ACT, 2019

(No. 24 *of* 2019*)*

IN EXERCISE of the powers conferred by section 71 of the Data Protection Act, 2019, the Cabinet Secretary for Information, Communication, Technology, Innovation and Youth Affairs makes the following Regulations—

THE DATA PROTECTION (GENERAL) REGULATIONS, 2021

PART I—PRELIMINARY

Citation.

1. These Regulations may be cited as the Data Protection (General) Regulations, 2021.

Interpretation.

2. In these Regulations, unless the context otherwise requires—

"Act" means the Data Protection Act, 2019;

"Data Commissioner" means the person appointed as such pursuant to section 6 of the Act; and

No. 24 of 2019.

"Office" has the meaning assigned to it under the Act.

Exemption.
L. N. No.196 of 2020.

3. These Regulations shall not apply to civil registration entities specified under the Data Protection (Civil Registration) Regulations, 2020.

PART II— ENABLING THE RIGHTS OF A DATA SUBJECT

Processing on the basis of consent.

4. (1) Where processing is based on consent in accordance with section 32 of the Act, a data controller or data processor shall, in seeking consent prior to the processing, inform the data subject of'—

(a) the identity of the data controller or data processor;

(b) the purpose of each of the processing operations for which consent is sought;

(c) the type of personal data that is collected and used;

(d) information about the use of the personal data for automated decision-making, where relevant;

(e) the possible risks of data transfers due to absence of an adequacy decision or appropriate safeguards;

(f) whether the personal data processed shall be shared with third parties;

(g) the right to withdraw consent; and

(h) the implications of providing, withholding or withdrawing consent.

(2) The information under sub-regulation (1) may be presented to the data subject through a written notice, oral statement, audio or video message.

(3) In obtaining consent from a data subject, a data controller or a data processor shall ensure that the—

(a) data subject has capacity to give consent;

(b) data subject voluntarily gives consent; and

(c) consent is specific to the purpose of processing.

(4) Pursuant to section 32(4) of the Act, consent shall be considered to have been given freely, unless where —

(a) it is presumed on the basis that the data subject did not object to a proposal to processing of their personal data in a particular manner;

(b) it is presented as a non-negotiable part of the terms and conditions for processing;

(c) the data subject is unable to refuse or withdraw their consent without detriment;

(d) the data controller or data processor merges several purposes for processing without seeking specific consent for each purpose; or

(e) the intention of the data subject is ambiguous.

(5) Where the data subject withdraws consent to any part of the processing, the data controller or data processor shall restrict the part of the processing in respect of which consent is withdrawn, subject to section 34 of the Act.

Lawful basis for processing.

5.(1) A data controller or data processor may process data without consent of a data subject if the processing is necessary for any reason set out in section 30(1) (b) of the Act.

(2) Processing under sub-regulation (1) shall only rely on one legal basis for processing at a time, which shall be established before the processing.

(3) The legal basis relied on under sub-regulation (1) shall be demonstrable at all times and where a data controller uses multiple bases for different processing, the data controller shall—

(a) distinguish between the legal bases being used; and

(b) respond to any data subject rights requests.

Mode of collection of personal data.

6. (1) Pursuant to section 28(2) of the Act, a data controller or data processor may collect personal data indirectly from—

(a) any person other than the data subject;

(b) publications or databases;

(c) surveillance cameras, where an individual is identifiable or reasonably identifiable;

(d) information associated with web browsing; or

(e) biometric technology, including voice or facial recognition.

(2) A data controller or data processor shall, in collecting personal data—

(a) ensure that processing is limited to personal data which the

data subject has permitted the data controller or data processor to collect;

(b) undertake steps to ensure that personal data is accurate, notin excessive and up to date;

(c) undertake processes to secure personal data; and

(d) comply with the lawful processing principles set out under part IV of the Act.

(3) Where a data controller or data processor collects personal data indirectly, the data controller or data processor shall within fourteen days inform the data subject of the collection.

(4) Where a data controller or data processor intends to use personal data for a new purpose, the data controller or data processor shall ensure that the new purpose is compatible with the initial purpose for which the personal data was collected.

(5) Where the new purpose is not compatible with the initial purpose, a data controller or data processor shall seek fresh consent from the data subject in accordance with regulation 4.

Restriction to processing.

7. (1) Pursuant to section 34 of the Act, a data subject may request a data controller or data processor to restrict the processing of their personal data on grounds that—

(a) the data subject contests the accuracy of their personal data;

(b) the personal data has been unlawfully processed and the data subject opposes the erasure and requests restriction instead;

(c) the data subject no longer needs their personal data but the data controller or data processor requires the personal data to be kept in order to establish, exercise or defend a legal claim; or

(d) a data subject has objected to the processing of their personal data under regulation 8 and a data controller or data processor is considering legitimate grounds that override those of the data subject.

(2) A request for restriction to processing of personal data on any of the grounds provided under section 34 of the Act may be made in Form DPG 1 set out in the First Schedule.

(3) A data controller or data processor shall within fourteen days of the request for restriction pursuant to sub-regulation (2), and without charging any fee—

(a) admit and implement the request;

(b) indicate on the data controller or data processors system that the processing of the personal data has been restricted; and

(c) notify any relevant third party of the restriction where personal data, subject to such restriction, may have been shared.

(4) A data controller or a data processor may implement a

restriction to processing request by—

(a) temporarily moving the personal data to another processing system;

(b) making the personal data unavailable to third parties; or

(c) temporarily removing published data specific to the data subject from its website or other public medium in its control.

(5) A data controller or data processor may decline to comply with a request for restriction in processing, where such request is manifestly unfounded or excessive.

(6) Where a data controller or data processor declines a request on any of the grounds provided under section 34(2) of the Act, the data controller or data processor shall within fourteen days of the refusal, notify the data subject of the refusal, in writing, and shall provide the reasons for the decision.

(7) A data controller or data processor shall not process personal data that has been restricted, except to store the personal data, in accordance with section 34(2)(a) of the Act.

Objection to processing.

8. (1) Pursuant to section 36 of the Act, a data subject may request a data controller or data processor not to process all or part of their personal data, for a specified purpose or in a specified manner.

(2) A request to object the processing may be made in Form DPG 1 set out in the First schedule.

(3) A data controller or data processor shall, without charging any fee, comply with a request for objection under sub-regulation (2) within fourteen days of the request.

(4) The right to object to processing applies as an absolute right where the processing is for direct marketing purposes which includes profiling to the extent that it is related to such direct marketing.

(5) Where the data subject objects to processing for direct marketing purposes, the personal data shall not be processed for such purposes.

(6) Where the right to object to processing is not absolute and the request by a data subject has been declined, the data controller or data processor shall inform the data subject of—

(a) the reasons for declining the request for objection; and

(b) the right to lodge a complaint to the Data Commissioner where dissatisfied.

(7) Where a data controller or data processor demonstrates compelling legitimate interest for the processing which overrides the data subject's interests, or for the establishment, exercise or defence of a legal claim, the data controller or data processor shall inform the data subject of—

(a) the reasons for declining the request for objection; and

(b) the right to lodge a complaint to the Data Commissioner where dissatisfied.

Data access request.

9. (1) A data subject has a right to obtain from the data controller or data processor confirmation as to whether or not personal data concerning them is being processed, and, where that is the case, access to the personal data and the information as to—

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, including recipients in other countries or territories;

(d) where possible, the envisaged period for which the personal data may be stored, or, if not possible, the criteria used to determine that period; and

(e) where the personal data is not collected from the data subject, any available information as to the source of collection.

(2) A data subject may request to access their personal data in Form DPG 2set out in the First Schedule.

(3) A data controller or data processor shall—

(a) on request, provide access to a data subject of their personal data in its possession;

(b) put in place mechanisms to enable a data subject to proactively access or examine their personal data; or

(c) provide the data subject with a copy of their personal data.

(4) A data controller or a data processor shall comply with a request by a data subject to access their personal data within seven days of the of the request.

(5) Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

(6) Compliance with a request for access to personal data shall be free of charge.

Rectification of personal data.

10. (1) Pursuant to section 40 of the Act, a data subject may request a data controller or data processor to rectify their personal data, which is untrue, inaccurate, outdated, incomplete or misleading.

(2) A request for rectification may be made in Form DPG 3 set out in the First Schedule.

(3) An application for rectification of personal data may be supported by such documents as may be relevant to the rectification sought.

(4) A data controller or data processor shall within fourteen days

of the request, rectify an entry of personal data in the database where the data controller or data processor is satisfied that a rectification is necessary.

(5) Where a request for rectification is declined, a data controller or data processor shall, in writing, notify a data subject of that refusal within seven days and shall provide reasons for refusal.

(6) A request for rectification shall made free of charge.

Data portability request.

11. (1) Pursuant to section 38 of the Act, a data subject may apply to port or copy their personal data from one data controller or data processor to another.

(2) A request for data portability may be made in Form DPG 4set out in the First Schedule.

(3) A data controller or data processor shall within thirty days of the request and upon payment of the prescribed fees port personal data to the data subject's choice of recipient.

(4) Where fee is charged under sub-regulation (2), the fee shall be reasonable and not exceed the cost incurred to actualize the request.

(5) A data controller or data processor who receives personal data that has been ported shall, with respect to such data, comply with the requirement of the Act and these Regulations.

(6) Where a data controller or data processor declines the portability request, a data controller or data processor shall, within seven days, notify the data subject of the decline and the reasons for such decline in writing.

(7) The exercise of the right to data portability by a data subject shall not negate the rights of a data subject provided under the Act.

Right of erasure.

12. (1) Pursuant to section 40 (1) (b) of the Act, a data subject may, request a data controller or data processor to erase or destroy personal data held by the data controller or data processor where —

(a) the personal data is no longer necessary for the purpose which it was collected;

(b) the data subject withdraws their consent that was the lawful basis for retaining the personal data;

(c) the data subject objects to the processing of their data and there is no overriding legitimate interest to continue the processing;

(d) the processing of personal data is for direct marketing purposes and the individual objects to that processing;

(e) the processing of personal data is unlawful including in breach of the lawfulness requirement; or

(f) the erasure is necessary to comply with a legal obligation.

(2) A data subject may request for erasure of their personal data held by a data controller or data processor in Form DPG5 set out in the

First Schedule.

(3) A data controller or data processor shall respond to a request for erasure under sub-regulation (2) within fourteen days of the request.

(4) A right of erasure does not apply if processing is necessary for one of the following reasons—

(a) to exercise the right of freedom of expression and information;

(b) to comply with a legal obligation;

(c) for the performance of a task carried out in the public interest or in the exercise of official authority;

(d) for archiving purposes in the public interest, scientific research, historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or

(e) for the establishment, exercise or defence of a legal claim.

(5) A request for erasure shall be free of charge.

Exercise of rights by others.

13. (1) Subject to section 27 of the Act, where a person duly authorised by a data subject seeks to exercise the rights on their behalf, the data controller or data processor shall act in the best interests of the data subject.

(2) Where the data subject is a child, a data controller or data processor shall ensure that—

(a) a person exercising the right is appropriately identified;

(b) profiling of a child that is related to direct marketing is prohibited; and

(c) the parent or guardian is informed of the inherent risks in processing and the safeguards put in place.

(3) Where a data controller or a data processor is uncertain as to the existence of a relationship between the duly authorised person and the data subject, the data controller or data processor may restrict the request of exercising a right on behalf of the data subject until evidence to the contrary is adduced.

PART III—RESTRICTIONS ON THE COMMERCIAL USE OF PERSONAL DATA

Interpretation of commercial purposes.

14. (1) For the purposes of section 37 (1) of the Act, a data controller or data processor shall be considered to use personal data for commercial purposes where personal data of a data subject is used to advance commercial or economic interests, including inducing another person to buy, rent, lease, join, subscribe to, provide or exchange products, property, information or services, or enabling or effecting, directly or indirectly, a commercial transaction.

(2) A data controller or data processor is considered to use personal data to advance commercial interests where personal data is

used for direct marketing through—

(a) sending a catalogue through any medium addressed to a data subject;

(b) displaying an advertisement on an online media site where a data subject is logged on using their personal data; or

(c) sending an electronic message to a data subject about a sale, or other advertising material relating to a sale, using personal data provided by a data subject.

(3) Marketing is not direct where personal data is not used or disclosed to identify or target particular recipients.

Permitted commercial use of personal data.

15. (1) A data controller or data processor may use personal data, other than sensitive personal data, concerning a data subject for the purpose of direct marketing where—

(a) the data controller or data processor has collected the personal data from the data subject;

(b) a data subject is notified that direct marketing is one of the purposes for which personal data is collected;

(c) the data subject has consented to the use or disclosure of the personal data for the purpose of direct marketing;

(d) the data controller or data processor provides a simplified opt out mechanism for the data subject to request not to receive direct marketing communications; or

(e) the data subject has not made an opt out request.

(2) A data controller or data processor shall not transmit, for the purposes of direct marketing, messages by any means unless the data controller or data processor indicates particulars to which a data subject may send a request to restrict such communications without incurring charges.

(3) A person shall neither transmit, nor instigate the transmission of, a communication for the purposes of direct marketing by means of electronic mail—

(a) where the identity of the person on whose behalf the communication has been sent has been disguised or concealed;

(b) where a valid address to which the recipient of the communication may send a request that such communications cease has not been provided; or

(c) where there is use of automated calling systems without human intervention.

(4) A data controller or data processor who uses personal data for commercial purposes without the consent of the data subject commits an offence and is liable, on conviction, to a fine not exceeding twenty thousand shillings or to a term of imprisonment not exceeding six months, or to both fine and imprisonment.

Features of an opt out message.

16. (1) An opt out mechanism contemplated under regulation 15(1)(d) shall—

(a) have a visible, clear and easily understood explanation of how to opt out;

(b) include a process for opting out that requires minimal time and effort;

(c) provide a direct and accessible communication channel;

(d) be free of charge or where necessary involve a nominal cost to a data subject; and

(e) be accessible to persons with a disability.

(2) Where a data subject has opted out, a data controller or data processor shall not use or disclose their personal data for the purpose of direct marketing, in accordance with the data subject's request.

Mechanisms to comply with opt out requirement.

17. (1) In communicating with a data subject on direct marketing, a data controller or data processor shall include a statement which is prominently displayed, or otherwise draws the attention of the data subject to the fact that the data subject may make an opt out request.

(2) A data controller or data processor may, in complying with an opt out requirement—

(a) clearly indicate, in each direct marketing message, that a data subject may opt out of receiving future messages by replying with a single word instruction in the subject line;

(b) ensure that a link is prominently located in the email, which takes a data subject to a subscription control centre;

(c) clearly indicate that a data subject may opt out of future direct marketing by replying to a direct marketing text message with a single word instruction;

(d) inform the recipient of a direct marketing phone call that they can verbally opt out from any future calls; and

(e) include instructions on how to opt out from future direct marketing, in each message.

(3) A data controller or a data processor may use an opt out mechanism that provides a data subject with the opportunity to indicate their direct marketing communication preferences, including the extent to which they wish to opt out.

(4) Despite sub-regulation (3), a data controller or data processor shall provide a data subject with an option to opt out of all future direct marketing communications as one of outlined preferences.

Request for restriction of further direct marketing.

18. (1) A data subject may request a data controller or data processor to restrict use or disclosure of their personal data, to a third party, for the purpose of facilitating direct marketing.

(2) No fee shall be charged to a data subject for making or giving

effect to a request under this Part.

(3) A data controller or data processor shall restrict use or disclosure of personal data for the purpose of facilitating direct marketing by a third party within seven days of the request.

PART IV—OBLIGATIONS OF DATA CONTROLLERS AND DATA PROCESSORS

Retention of personal data.

19. (1) Pursuant to section 39 of the Act, a data controller or data processor shall retain personal data processed for a lawful purpose, for as long as may be reasonably necessary for the purpose for which the personal data is processed.

(2) A data controller or data processor shall—

(a) establish personal data retention schedule with appropriate time limits for the periodic review of the need for the continued storage of personal data that is no longer necessary or where the retention period is reached; and

(b) erase, delete anonymise or pseudonymise personal data upon the lapse of the purpose for which the personal data was collected.

(3) A personal data retention schedule established under paragraph (2)(a) shall outline the —

(a) purpose for retention;

(b) the retention period;

(c) provision for periodic audit of the personal data retained; and

(d) actions to be taken after the audit of the personal data retained.

(4) An audit of the retained data under paragraph (3)(c), shall seek to—

(a) review records with a view of identifying personal data that no longer requires to be retained and permanently delete the personal data;

(b) ensure the retained data is accurate and up-to-date;

(c) specify the purpose for retention of personal data;

(d) ensure that the personal data security measures are adequate; and

(e) identify the best cause of action where personal data retention period lapses.

(5) A data controller or data processor shall establish appropriate time limits for the periodic review of the need for the continued storage of personal data for any of the law enforcement purposes.

(6) The personal data storage limitation period and data retention schedule outlined under paragraph (2)(a) may be included as part of the policy envisaged in regulation 23.

Requests to deal anonymously or pseudonymously.

20. (1) A data subject may request a data controller or data processor to process their personal data anonymously or pseudonymously where the data subject wishes—

(a) not to be identified;

(b) to avoid subsequent contact such as direct marketing from an entity or third parties;

(c) to enhance their privacy on the whereabouts of a data subject;

(d) to access services such as counselling or health services without it becoming known to others;

(e) to express views in a public arena without being personally identified; or

(f) to minimise the risk of identity fraud.

(3) A data controller or data processor may accede to the request where satisfied that the request is based on any of the reasons specified under sub-regulation (1) and where the request is in the best interests of the data subject.

Sharing of personal data.

21. (1) Subject to section 25 of the Act, a data controller or data processor may share or exchange personal data collected, upon request, by another data controller, data processor, third party or a data subject.

(2) A data controller or data processor shall determine the purpose and means of sharing personal data from one data controller or data processor to another.

(3) Data sharing outlined under this regulation may include—

(a) providing personal data to a third party by whatever means by the data controller or data processor;

(b) receiving personal data from a data controller or data processor as joint participant in a data sharing arrangement;

(c) exchanging or transmission of personal data;

(d) providing third party with access to personal data on the data controller's information systems;

(e) separate or joint initiatives by data controllers or data processors to pool personal data making the data available to each other or a third-party subject to entering into an agreement, as may be applicable; or

(f) routine data sharing between data controllers on a regular or pre-planned basis.

(4) In carrying out any routine data sharing as contemplated under paragraph (3)(f), a data controller shall enter into agreements prior to data sharing.

(5) For the avoidance of doubt, the sharing of data within the organizational structures of a data controller or data processor is not

considered as a data sharing.

(6) A request for sharing personal data under this regulation shall be in writing, and shall specify—

(a) the purpose for which personal data is required;

(b) the duration for which personal data shall be retained; and

(c) proof of the safeguards put in place to secure personal data from unlawful disclosure.

Automated individual decision making.

22. (1) In this regulation—

"an automated individual decision-making" means a decision made by automated means without any human involvement.

(2) Pursuant to section 35 of the Act, a data controller or data processor shall—

(a) inform a data subject when engaging in processing based on automated individual decision making;

(b) provide meaningful information about the logic involved;

(c) ensure—

(i) specific transparency and fairness requirements are in place;

(ii) rights for a data subject to oppose profiling and specifically profiling for marketing are present; and

(iii) where conditions specified under section 31 of the Act arise, a data protection impact assessment is carried out;

(d) explain the significance and envisaged consequences of the processing;

(e) ensure the prevention of errors;

(f) use appropriate mathematical or statistical procedures;

(g) put appropriate technical and organisational measures in place to correct inaccuracies and minimise the risk of errors;

(h) process personal data in a way that eliminates discriminatory effects and bias; and

(i) ensure that a data subject can obtain human intervention and express their point of view.

Data protection policy.

23. (1) A data controller or data processor shall develop, publish and regularly update a policy reflecting their personal data handling practices.

(2) A policy under sub-regulation (1) may include—

(a) the nature of personal data collected and held;

(b) how a data subject may access their personal data and

exercise their rights in respect to that personal data;

(c) complaints handling mechanisms;

(d) lawful purpose for processing personal data;

(e) obligations or requirements where personal data is to be transferred outside the country, to third parties, or other data controllers or data processors located outside Kenya and where possible, specify such recipients;

(f) the retention period and schedule contemplated under regulation 19; and

(g) the collection of personal data from children, and the criteria to be applied.

Contract between data controller and data processor.

24. (1) Subject to section 42(2)(b) of the Act, a data controller shall engage a data processor, through a written contract.

(2) The contract envisaged under sub-regulation (1) shall include the following particulars—

(a) processing details including—

(i) the subject matter of the processing;

(ii) the duration of the processing;

(iii) the nature and purpose of the processing;

(iv) the type of personal data being processed;

(v) the categories of data subjects; and

(vi) the obligations and rights of the data controller;

(b) instructions of the data controller;

(c) duty on the data processors to obtain a commitment of confidentiality from any person or entity that the data processors allows to process the personal data;

(d) security measures subjecting the data processor to appropriate technical and organizational measures in relation to keeping personal data secure;

(e) provision stipulating that all personal data must be permanently deleted or returned on termination or lapse of the agreement, as decided by the data controller; and

(f) auditing and inspection provisions by the data controller.

Obligations of a data processor.

25. (1) A data processor shall not engage the services of a third party without the prior authorisation of the data controller.

(2) Where authorisation is given, the data processor shall enter into a contract with the third party.

(3) The contract contemplated under sub-regulation (1) shall include such particulars as provided for under sub-regulation 24(2).

(4) A data processor shall remain liable to the data controller for the compliance of any third party that they engage.

Requirement for specified processing to be done in Kenya.

26. (1) Pursuant to section 50 of the Act, a data controller or data processor who processes personal data for the purposeof strategic interest of the state outlined under sub-regulation (2) shall —

(a) process such personal data through a server and data centre located in Kenya; or

(b) store at least one serving copy of the concerned personal datain a data centre located in Kenya.

(2) The purpose contemplated under sub-regulation (1) includes the processing of personal data for the purpose of—

(a) administering of the civil registration and legal identity management systems;

(b) facilitating the conduct of elections for the representation of the people under the Constitution;

(c) overseeing any system for administering public finances by any state organ;

(d) running any system designated as a protected computer system in terms of section 20 of the Computer Misuse and Cybercrime Act, 2018; No.5 of 2018.

(e) offering any form of early childhood education and basic education under the Basic Education Act, 2013; or No.14 of 2013.

(f) provision of primary or secondary health care for a data subject in the country.

(3) Despite (2), the Cabinet Secretary may require a data controller who processes personal data outside Kenya to comply with sub-regulation (1), where the data controller—

(a) has been notified that personal data outside Kenya has been breached or its services have been used to violate the Act and has not taken measures to stop or handle the violation; and

(b) resists, obstructs or fails to comply with requests of the Data Commissioner or any other relevant authority in—

(i) cooperating to investigate and handle such violations; or

(ii) neutralising and disabling the effect of cyber security protection measures.

PART V—ELEMENTS TO IMPLEMENT DATA PROTECTION BY DESIGN OR BY DEFAULT

Data protection by design or default.

27. A data controller or data processor shall in processing of personal data —

(a) establish the data protection mechanisms set out under the Act and these Regulations are embedded in the processing;

and

(b) design technical and organisational measures to safeguard and implement the data protection principles.

Elements of data protection by design or default.

28. The elements for the protection of personal data by design or by default that are necessary to implement the data protection principles outlined under section 25 of the Act are as set out in this Part.

Elements for principle of lawfulness.

29. The elements necessary to implement the principle of lawfulness include—

(a) appropriate legal basis or legitimate interests clearly connected to the specific purpose of processing;

(b) processing that is necessary for the purpose;

(c) the data subject being granted the highest degree of autonomy possible with respect to control over their personal data;

(d) a data subject knowing what they consented to and a simplified means to withdraw consent; and

(e) restriction of processing where the legal basis or legitimate interests ceases to apply.

Elements for principle of transparency.

30. The elements necessary to implement the principle of transparency include—

(a) the use of clear, simple and plain language to communicate with a data subject to enable a data subject to make decisions on the processing of their personal data;

(b) making the information on the processing easily accessible to the data subject;

(c) providing the information on the processing to the data subject at the relevant time and in the appropriate form;

(d) the use of machine-readable language to facilitate and automate readability and clarity;

(e) providing a fair understanding of the expectation with regards to the processing particularly for children or other vulnerable groups; and

(f) providing details of the use and disclosure of the personal data of a data subject.

Elements for principle of purpose limitation.

31. The elements necessary to implement the principle of purpose limitation include—

(a) specifying the purpose for each processing of personal data;

(b) determining the legitimate purposes for the processing of personal data before designing organisational measures and safeguards;

(c) the purpose for the processing being the determinant for

personal data collected;

(d) ensuring a new purpose is compatible with the original purpose for which the data was collected;

(e) regularly reviewing whether the processing is necessary for the purposes for which the data was collected and test the design against purpose limitation; and

(f) the use of technical measures, including hashing and cryptography, to limit the possibility of repurposing personal data.

Elements for principle of integrity, confidentiality and availability.

32. The elements necessary to implement the principle of integrity, confidentiality and availability include—

(a) having an operative means of managing policies and procedures for information security;

(b) assessing the risks against the security of personal data and putting in place measures to counter identified risks;

(c) processing that is robust to withstand changes, regulatory demands, incidents, and cyber-attacks;

(d) ensuring only authorised personnel have access to the data necessary for their processing tasks;

(e) securing transfers shall be secured against unauthorised access and changes;

(f) securing data storage from use, unauthorised access and alterations;

(g) keeping back-ups and logs to the extent necessary for information security;

(h) using audit trails and event monitoring as a routine security control;

(i) protecting sensitive personal data with adequate measures and, where possible, kept separate from the rest of the personal data;

(j) having in place routines and procedures to detect, handle, report, and learn from data breaches; and

(k) regularly reviewing and testing software to uncover vulnerabilities of the systems supporting the processing.

Elements for principle of data minimization.

33. The elements necessary to implement the principle of data minimization include—

(a) avoiding the processing of personal data altogether when this is possible for the relevant purpose;

(b) limiting the amount of personal data collected to what is necessary for the purpose;

(c) ability to demonstrate the relevance of the data to the processing in question;

(d) pseudonymising personal data as soon as the data is no longer necessary to have directly identifiable personal data, and storing identification keys separately;

(e) anonymizing or deleting personal data where the data is no longer necessary for the purpose;

(f) making data flows efficient to avoid the creation of more copies or entry points for data collection than is necessary; and

(g) the application of available and suitable technologies for data avoidance and minimization.

Elements for principle of accuracy.

34. The elements necessary to implement the principle of accuracy include—

(a) ensuring data sources are reliable in terms of data accuracy;

(b) having personal data particulars being accurate as necessary for the specified purposes;

(c) verification of the correctness of personal data with the data subject before and at different stages of the processing depending on the nature of the personal data, in relation to how often it may change;

(d) erasing or rectifying inaccurate data without delay;

(e) mitigating the effect of an accumulated error in the processing chain;

(f) giving data subjects an overview and easy access to personal data in order to control accuracy and rectify as needed;

(g) having personal data accurate at all stages of the processing and carrying out tests for accuracy at critical steps;

(h) updating personal data as necessary for the purpose; and

(i) the use of technological and organisational design features to decrease inaccuracy.

Elements for principle of storage limitation.

35. The elements necessary to implement the principle of storage limitation include—

(a) having clear internal procedures for deletion and destruction;

(b) determining what data and length of storage of personal data that is necessary for the purpose;

(c) formulating internal retention statements of implementing them;

(d) ensuring that it is not possible to re-identify anonymised data or recover deleted data and testing whether this is possible;

(e) the ability to justify why the period of storage is necessary for the purpose, and disclosing the rationale behind the retention period; and

(f) determining which personal data and length of storage is necessary for back-ups and logs.

Elements for principle of fairness.

36. The elements necessary to implement the principle of fairness include—

(a) granting the data subjects the highest degree of autonomy with respect to control over their personal data;

(b) enabling a data subject to communicate and exercise their rights;

(c) elimination of any discrimination against a data subject;

(d) guarding against the exploitation of the needs or vulnerabilities of a data subject; and

(e) incorporating human intervention to minimize biases that automated decision-making processes may create.

PART VI—NOTIFICATION OF PERSONAL DATA BREACHES

Categories of notifiable data breach.

37. (1) For the purpose of section 43 of the Act, a data breach is taken to result in real risk of harm to a data subject if that data breach relates to —

(a) the data subject's full name or identification number and any of the personal data or classes of personal data relating to the data subject set out in the Second Schedule; or

(b) the following personal data relating to a data subject's account with a data controller or data processor—

(i) the data subject's account identifier, such as an account name or number; and

(ii) any password, security code, access code, response to a security question, biometric data or other data that is used or required to allow access to or use of the individual's account.

(2) A breach of any personal data envisaged under sub-regulation (1) amounts to notifiable data breach under section 43 of the Act.

(3) The personal data or classes of personal data set out in the Second Schedule excludes —

(a) any personal data that is publicly available; or

(b) any personal data that is disclosed to the extent that is required or permitted under any written law.

(4) The personal data referred to in sub-paragraph (3) (a) shall not be publicly available solely because of any data breach.

Notification to Data Commissioner.

38. (1) A notification by data controller to the Data Commissioner of a notifiable data breach under section 43 of the Act shall include—

(a) the date on which and the circumstances in which the data controller or data processor first became aware that the data breach had occurred;

(b) a chronological account of the steps taken by the data

controller or data processor after the data controller or data processor became aware that the data breach had occurred, including the data controller or data processor's assessment that the data breach is a notifiable data breach;

(c) details on how the notifiable data breach occurred, where applicable;

(d) the number of data subjects or other persons affected by the notifiable data breach;

(e) the personal data or classes of personal data affected by the notifiable data breach;

(f) the potential harm to the affected data subjects as a result of the notifiable data breach;

(g) information on any action by the data controller or data processor, whether taken before or to be taken after the data controller or data processor notifies the Data Commissioner of the occurrence of the notifiable data breach to—

(i) eliminate or mitigate any potential harm to any affected data subject or other person as a result of the notifiable data breach; or

(ii) address or remedy any failure or shortcoming that the data controller or data processor believes to have caused, or enabled or facilitated the occurrence of, the notifiable data breach;

(h) the affected individuals or the public that the notifiable data breach has occurred and how an affected data subject may eliminate or mitigate any potential harm as a result of the notifiable data breach; or

(i) contact information of an authorized representative of the data controller or data processor.

(2) Where the data controller intends not to communicate a notifiable data breach to a data subject affected by such breach, under the conditions set out in section 43(1) (b) of the Act, the notification to the Data Commissioner under sub-regulation (1) shall additionally specify the grounds for not notifying the affected data subject.

PART VII—TRANSFER OF PERSONAL DATA OUTSIDE KENYA

Interpretation of the Part VII.

39. In this Part, unless the context otherwise requires —

(a) "data in transit" means personal data transferred through Kenya in the course of onward transportation to a country or territory outside Kenya, without the personal data being accessed or used by, or disclosed to, any entity while in Kenya, except for the purpose of such transportation;

(b) "recipient" means an entity that receives in a country or

territory outside Kenya the personal data transferred to the recipient by or on behalf of the transferring entity, but does not include an entity that receives the personal data solely as a network service provider or carrier;

(c) "transferring entity" means an entity that transfers personal data from Kenya to a country or a territory outside Kenya but does not include an entity dealing with data in transit; and

(d) "relevant international organisation" means an international organisation that carries out functions for any of the law enforcement purposes.

General principles for transfers of personal data out of the country.

40. A data controller or data processor who is a transferring entity shall before transferring personal data out of Kenya ascertain that the transfer is based on—

(a) appropriate data protection safeguards;

(b) an adequacy decision made by the Data Commissioner;

(c) transfer as a necessity; or

(d) consent of the data subject.

Transfers on the basis of appropriate safeguards.

41. (1) A transfer of personal data to a another country or a relevant international organisation is based on the existence of appropriate safeguards where—

(a) a legal instrument containing appropriate safeguards for the protection of personal data binding the intended recipient that is essentially equivalent to the protection under the Act and these Regulations; or

(b) the data controller, having assessed all the circumstances surrounding transfers of that type of personal data to another country or relevant international organisation, concludes that appropriate safeguards exist to protect the data.

(2) Where a transfer of data takes place in reliance on sub-regulation (1)—

(a) the transfer shall be documented;

(b) the documentation shall be provided to the Commissioner on request; and

(c) the documentation shall include—

(i) the date and time of the transfer;

(ii) the name of the recipient;

(iii) the justification for the transfer; and

(iv) a description of the personal data transferred.

Deeming of appropriate safeguards.

42. For the purpose of confirming the existence of appropriate data protection safeguards anticipated under section 49 (1) of the Act and these Regulations, any country or a territory is taken to have such

safeguards if that country or territory has—

(a) ratified the African Union Convention on Cyber Security and Personal Data Protection;

(b) a reciprocal data protection agreement with Kenya; or

(c) a contractual binding corporate rules among a concerned group of undertakings or enterprises.

Binding corporate rules.

43. (1) The contractual binding corporate rules contemplated under regulation 41 shall be valid if they—

(a) are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;

(b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and

(c) fulfil the requirements laid down in sub-regulation (2).

(2) The binding corporate rules referred to in sub-regulation (1) shall specify—

(a) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;

(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of another country or countries in question;

(c) their legally binding nature, both internally and externally;

(d) the application of the general data protection principles;

(e) the rights of data subjects in regard to processing and the means to exercise those rights;

(f) the complaint procedures; and

(g) the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules.

Transfers on the basis of an adequacy decision.

44. (1) A transfer of personal data to another country or a relevant international organization is based on an adequacy decision where the Data Commissioner makes a decision that—

(a) the other country or a territory or one or more specified sectors within that other country, or

(b) the international organization, ensures an adequate level of protection of personal data.

(2) The Data Commissioner may publish on its website a list of the countries, territories and specified sectors within that other country

and relevant international organisation for which the Data Commissioner has made a decision that an adequate level of protection is ensured.

Transfers on the basis of necessity.

45. (1) Personal data may be transferred to another country or territory on the basis of necessity is such a transfer is necessary for any of the purpose outlined under section 48 (c) of the Act.

(2) Prior to making a transfer under sub-regulation (1), a transferring entity shall ascertain that—

(a) that the transfer is strictly necessary in a specific case outlined under section 48(c) of the Act;

(b) there are no fundamental rights and freedoms of the data subject concerned that override the public interest necessitating the transfer.

(3) This section does not affect the operation of any international agreement in force between Kenya and other countries in the field of judicial co-operation in criminal matters and police co-operation.

Transfer on basis of consent.

46. (1) In accordance with section 25 (g) of the Act, in the absence of an adequacy decision, appropriate safeguards or prerequisites for transfer as a necessity, a transfer or a set of transfers of personal data to another country shall take place only on the condition that the data subject—

(a) has explicitly consented to the proposed transfer; and

(b) has been informed of the possible risks of such transfers.

(2) Without limiting the generality of sub-regulation (1), a data controller or processor must seek consent from a data subject for the transfer of sensitive personal data, in accordance with section 49 of the Act.

Subsequent transfers.

47. (1) Where personal data is transferred in accordance with this Part, the entity effecting the transfer shall make it a condition of the transfer, that the data is not to be further transferred to another country or territory without the authorisation of the transferring entity or another competent authority.

(2) A competent authority may give an authorisation under sub-regulation (1) only where the further transfer is necessary for a law enforcement purpose.

Provisions for the agreement to cross boarder transfer.

48. A transferring entity may enter into a written agreement with the recipient of personal data, which shall contain provisions relating to—

(a) unlimited access by the transferring entity to ascertain the existence of a robust information system of the recipient for storing the personal data; and

(b) the countries and territories to which the personal data may be transferred under the contract.

PART VIII—DATA PROTECTION IMPACT ASSESSMENT

Processing activities requiring data protection impact assessment.

49. (1) For the purpose of section 31 (1) of the Act, processing operations considered to result in high risks to the rights and freedoms of a data subject include —

(a) automated decision making with legal or similar significant effect that includes the use of profiling or algorithmic means or use of sensitive personal data as an element to determine access to services or that results in legal or similarly significant effects;

(b) use of personal data on a large-scale for a purpose other than that for which the data was initially collected;

(c) processing biometric or genetic data;

(d) where there is a change in any aspect of the processing that may result in higher risk to data subjects;

(e) processing sensitive personal data or data relating to children or vulnerable groups;

(f) combining, linking or cross-referencing separate datasets where the data sets are combined from different sources and where processing is carried out for different purposes;

(g) large scale processing of personal data;

(h) a systematic monitoring of a publicly accessible area on a large scale;

(i) innovative use or application of new technological or organizational solutions; or

(j) where the processing prevents a data subject from exercising a right.

(2) A data processor or data controller shall, prior to processing data under sub-regulation (1) conduct a data protection impact assessment.

Conduct of data protection impact assessment.

50. (1) Where a data protection impact assessment is required, a data controller or data processor may conduct the assessment through a template set out in the Third Schedule.

(2) Despite sub-regulation (1), a format of the data protection impact assessment may be varied by the Data Commissioner through guidance notes as may be issued from time to time.

Prior consultation.

51. (1) In accordance with section 31 (3) of the Act, where a data controller or a data processor is required to consult the Data Commissioner on the data protection impact assessment prior to processing, such consultations shall be done within sixty days from the date of the receipt of the impact statement report.

(2) In making a request under sub-regulation (1), the data controller or data processor shall provide—

(a) the data protection impact assessment prepared under section 31(1) of the Act; and

(b) where applicable, the respective responsibilities of the data controller or data processors involved in the processing.

(3) Where the Data Commissioner considers that the intended processing is likely to infringe on the Act or these Regulations, the Data Commissioner may issue such advice to the data controller or the data processor, in writing.

Consideration of the data protection impact assessment report.

52. (1) In conducting a data protection impact assessment, a data controller or a data processor may consult the Office for advice on whether risks identified and mitigation measures suggested are viable in the outlined circumstances.

(2) In reviewing the data protection impact assessment report, the Data Commissioner may make any recommendations to be incorporated prior to commencing the processing operations.

(3) Where a data controller or data processor, upon submitting the data protection impact assessment report to the Data Commissioner, does not receive any communication within sixty days of submission, may commence processing operations and the assessment report shall be taken to have been approved.

(4) A data controller or data processor may publish on its website the data protection impact assessment Report.

Audit of compliance with Assessment Report.

53. Pursuant to section 23 of the Act, the Data Commissioner may carry out periodic audits to monitor compliance with the Assessment Report and any recommendations that may have been provided by the Data Commissioner.

PART IX— PROVISIONS ON EXEMPTIONS UNDER THE ACT

Exemption for national security.

54. (1) For the purposes of section 51(2) (b) of the Act, the processing of personal data by a national security organ referred to in Article 239 (1) of the Constitution in furtherance of their mandate constitutes a processing for national security.

(2) Despite sub-regulation (1), a data controller or data processor who processes personal data for national security and wishes to be exempt on that ground shall apply to the Cabinet Secretary for an exemption.

(3) The Cabinet Secretary shall, upon being satisfied that the grounds supporting the application are sufficient, issue a certificate of exemption.

(4) The Cabinet Secretary may revoke a certificate of exemption issued, at any time, where the grounds on which the certificate was issued no longer apply.

Exemptions for public interest.

55. For the purposes of section 51(2) (b) of the Act, the processing of personal data is exempted from the Act on the grounds of public interest where such processing exists as a—

(a) permitted general situation; or

(b) permitted health situation.

Permitted general situation.

56. A permitted general situation referred to under regulation 55 (a)relates to the collection, use or disclosure by a data controller or data processor of personal data about data subject including for—

(a) lessening or preventing a serious threat to the life, health or safety of any data subject, or to public health or safety;

(b) taking appropriate action in relation to suspected unlawful activity or serious misconduct;

(c) locating a person reported as missing;

(d) asserting a legal or equitable claim;

(e) conducting an alternative dispute resolution process; or

(f) performing diplomatic or consular duties.

Permitted health situation.

57. (1) A permitted health situation referred to under regulation 55 (b) relates to the collection, use or disclosure by a data controller or data processor of personal data about a data subject, including for—

(a) the collection of health information to provide a health service;

(b) the collection, use, or disclosure of health data is for health research and related purposes;

(c) the use or disclosure of genetic information where necessary and obtained in course of providing a health service;

(d) the disclosure of health information for a secondary purpose to a responsible person for a data subject.

(2) A permitted health situation under sub-regulation (1) applies where a data controller or data processor discloses health data about a data subject, and—

(a) they provide a health service to the data subject;

(b) the recipient of the personal data is a responsible person for the data subject;

(c) a data subject is either physically or legally incapable of giving consent to the disclosure, or physically cannot communicate consent to the disclosure;

(d) the disclosure is necessary to provide appropriate care or treatment of a data subject, or the disclosure is made for compassionate reasons;

(e) the disclosure is not contrary to any wish expressed by the data subject before the data subject became unable to give or communicate consent of which the carer is aware or of which the carer could reasonably be expected to be aware; and

(f) the disclosure is limited to the extent reasonable and necessary to provide appropriate care or treatment of the individual or to fulfil the purpose of making a disclosure for compassionate reasons.

PART X —GENERAL PROVISIONS

Complaints against data controller and data processor.

58. A person aggrieved by a decision of a data controller or a data processor under this Regulation or non-compliance with any provision may lodge a complaint with the Data Commissioner in accordance with the Act and regulations on complaints handling made thereunder.

FIRST SCHEDULE

FORM DPG 1 (r. 7 (2) & (r.8 (2))

REQUEST FOR RESTRICTION OR OBJECTION
TO THE PROCESSING OF PERSONAL DATA

Note

(i) A documentary evidence in support of the objection may be required.

(ii) Where the space provided for in this Form is inadequate, submit information as an Annexure

A. NATURE OF REQUEST

Mark the appropriate box with an "x". Request for:

RESTRICTION ☐ OBJECTION ☐

B. DETAILS OF THE DATA SUBJECT

Name: .....
Identity Number: .....
Phone number:.....
E-mail address: .....

(Your details below where initiating the request for a minor or a person who has no capacity)

Name .....
Relationship with the Data Subject
Contact Information:

C. REASONS FOR THE REQUEST

(*Please provide detailed reasons for the restriction or objection)*

D. DECLARATION

I certify that the information given in this application is true

Signature _____ Date _____

DPG 2 (r. 9(2))

REQUEST FOR ACCESS TO PERSONAL DATA

Note:

(i) Documentary evidence in support of this request may be required.

(ii) Where the space provided for in this Form is inadequate, submit information as an annexure

*(iii) All fields marked as * are mandatory*

A. DETAILS OF THE DATA SUBJECT

(*This section is to provide the details of the Data Subject*).

Name*: _____

Identity Number*:

Phone number*:

e-mail address:

(Provide the following details where making a request on behalf of a minor or a person who has no capacity)
Name*

Relationship with the Data Subject*

Contact Information*

B. DETAILS OF THE PERSONAL DATA REQUESTED

(Describe the personal data requested)

MODE OF ACCESS

I would like to: *(check all that apply)*

[ ] Inspect the record

[ ] Listen to the record

[ ] Have a copy of the record made available to me in the following format:

[ ] photocopy *(Please note that copying costs will apply)*

number of copies required: .....

[ ] electronic

[ ] transcript *(Please note that transcription charges may apply)*

[ ] Other *(specify)* .....

C. Delivery Method

[ ] collection in person

[ ] by mail (provide address where different / in addition to details provided above)

Town/City: .....

[ ] by e-mail (provide email address where different / in addition to details provided above): .....

DECLARATION

Note any attempt to access personal data through misrepresentation may result in prosecution.

☐ I certify that the information given in this application is true.

Signature

Da

FORM DPG 3 (r.10 (2))

REQUEST FOR RECTIFICATION

Fill as appropriate

Note:

(i) Documentary evidence in support of this request may be required.

(ii) Where the space provided for in this Form is inadequate, submit information as an annexure

*(iii) All fields marked as * are mandatory*

A. DETAILS OF THE DATA SUBJECT

(*This section is to provide the details of the Data Subject*).

Name*:

Identity Number*:

Phone number*:

e-mail address:

(Provide the following details where making a request on behalf of a minor or a person who has no capacity)

Name*

Relationship with the Data Subject*

Contact Information*

Signature Date

PROPOSED CHANGE (S)

	Personal data to be corrected e.g. name, residential status, and mobile number, email address.	*Proposed change*	*Reason for the proposed change*
1.			
2.			
3.			
4.			
5.			

B. DECLARATION

Note any attempt to rectify personal data through misrepresentation may result in prosecution.

☐ I confirm that I have read and understood the terms of this request form and certify that the information given in this application is true.

Signature _____ Date _____

FORM DPG 4 (r. 11 (2))

REQUEST FOR DATA PORTABILITY

Note:

(iv) Documentary evidence in support of this request may be required.

(v) Where the space provided for in this Form is inadequate, submit information as an annexure

*(vi) All fields marked as * are mandatory*

A. DETAILS OF THE DATA SUBJECT

(*This section is to provide the details of the Data Subject*).

Name*:

Identity Number*:

Phone number*:

e-mail address:

(Provide the following details where making a request on behalf of a minor or a person who has no capacity)

Name*

Relationship with the Data Subject*

Contact Information*

B. DETAILS OF THE REQUEST

Please transfer a copy of my personal data to *

By either:

- Emailing a copy to them at
- Mailing to:
- Others (*Please specify)*

DECLARATION

Note, any attempt to port personal data through misrepresentation may result in prosecution.

☐ I certify that the information given in this application is accurate to the best of my knowledge

Signature _____ Date _____

FORM DPG 5 (r.12(2))

REQUEST FOR ERASURE OF PERSONAL DATA

Fill as appropriate

Note:

(i) Documentary evidence in support of this request may be required.

(ii) Where the space provided for in this Form is inadequate, submit information as an annexure

*(iii) All fields marked as * are mandatory*

i. DETAILS OF THE DATA SUBJECT

(*This section is to provide the details of the Data Subject*).

Name*: .....

Identity Number*: .....

Phone number*: .....

e-mail address: .....

(Provide the following details where making a request on behalf of a minor or a person who has no capacity)

Name* .....

Relationship with the Data Subject* .....

Contact Information* .....

ii. REASON FOR ERASURE REQUEST

(Tick the appropriate box)

(a) Your personal data is no longer necessary for the purpose for which it was originally collected;	☐
(b) You have withdrawn consent that was the lawful basis for retaining the personal data;	☐
(c) You object to the processing of your personal data and there is no overriding legitimate interest to continue the processing;	☐
(d) the processing of your personal data has been unlawful	☐
(e) Required to comply with a legal obligation.	☐

PERSONAL DATA TO BE ERASED

Describe the personal data you wish to have erased.

iii. Declaration

Note any attempt to erase personal data through misrepresentation may result in prosecution.

☐ I confirm that I have read and understood the terms of this request form and certify that the information given in this application is true.

Signature Date

SECOND SCHEDULE (r.37 (1)& (3))

The following personal data or circumstances amount to a notifiable data breach—

1. The amount of any wages, salary, fee, commission, bonus, gratuity, allowance or other remuneration paid or payable to the data subject by any person, whether under a contract of service or a contract for services.

2. The income of the data subject from the sale of any goods or property.

3. The number of any credit card, charge card or debit card issued to or in the name of the data subject.

4. The number assigned to any account the data subject has with any entity that is a bank or finance company.

5. Any information that identifies, or is likely to lead to the identification of, the data subject who is a child in conflict with the law or in need of care and protection.

6. Any private key of or relating to a data subject that is used or may be used —

(a) to create a secure electronic record or secure electronic signature;

(b) to verify the integrity of a secure electronic record; or

(c) to verify the authenticity or integrity of a secure electronic signature as provided under the Kenya Information and Communications (Electronic Certification and Domain Name Administration) Regulations, 2010 or any other related law.

7. The net worth or creditworthiness of a data subject.

8. The deposit or withdraw of monies by a data subject with any entity.

9. The withdrawal by the individual of moneys deposited with any entity or a payment system.

10. The granting by a person of advances, loans and other facilities by which the data subject, being a customer of the entity, has access to funds or financial guarantees.

11. The existence, and amount due or outstanding, of any debt —

(a) owed by the data subject to an entity; or

(b) owed by an entity to the data subject.

12. The incurring by the entity of any liabilities on behalf of the data subject.

13. The payment of any moneys, or transfer of any property, by any person to the individual, including the amount of the moneys paid or the value of the property transferred, as the case may be.

14. The data subject's investment in any capital markets products.

15. Any term and condition, premium or benefits payable, or any detail relating to the condition of health, from an accident, health, or life policy of which the data subject is the policy owner or a beneficiary.

16. The assessment, diagnosis, treatment, prevention or alleviation by a health professional of any of the following affecting the data subject—

(a) any sexually-transmitted diseases;

(b) Human Immunodeficiency Virus Infection;

(c) mental disorder;

(d) substance abuse and addiction.

17. The provision of treatment to the individual for or in respect of —

(a) the donation or receipt of a human egg or human sperm; or

(b) any contraceptive operation or procedure or abortion;

18. Any of the following—

(a) the donation and removal of any organ from the body of the deceased individual for the purpose of its transplantation into the body of another individual;

(b) the donation and removal of any specified organ from the individual, being a living organ donor, for the purpose of its transplantation into the body of another individual;

(c) the transplantation of any organ mentioned in paragraph (a) or (b) into the body of the individual.

19. The suicide or attempted suicide of the individual.

20. Domestic abuse, child abuse or sexual abuse involving or alleged to involve the data subject.

21. Any of the following—

(a) information that the individual is or had been adopted pursuant to an adoption order made under the Children Act No 8 of 2001, or is or had been the subject of an application for an adoption order;

(b) the identity of the natural father or mother of the data subject;

(c) the identity of the adoptive father or mother of the subject;

(d) the identity of any applicant for an adoption order;

(e) the identity of any person whose consent is necessary under that Act for an adoption order to be made, whether or not the court has dispensed with the consent of that person in accordance with that Act.

THIRD SCHEDULE (r.50 (1))

DATA PROTECTION IMPACT ASSESSMENT TEMPLATE

Part 1: Description of the processing operations

Name of Data Controller/ Data Processors: .....
Postal Address: .....
Email Address: .....
Telephone Number: .....
1. Project Name
2. Assess the need for Data Impact Assessment
(Assess whether there is need for DPIA by determining if project involves personal data that is likely to result in high risk, specify risk where appropriate)
3. Project Outline:
(Explain broadly what the project aims to achieve and what type of processing it involves)
4. Personal data
(*e.g type of personal data data being processed.)*
5. Describe the Information Flow.
Describe the collection, use and deletion of personal data here, including; where you are getting the data from; how is the data being collected; where the data will be stored; how long will the data be stored; where data could be transferred to; and, how many individuals are likely to be affected by the project.
6. Describe how the data processing flow complies with the data protection principles-

Part 2: An assessment of the necessity and proportionality of the processing operations in relation to the purpose.

Require the assessment and provide the parameters of the assessment.

Describe compliance and proportionality, measures, in particular:	
The lawful basis for processing	
Methods of obtaining of consent.	
Whether processing personal data is key to achieving your purpose?	
Is there another way to achieve the same outcome without processing personal data?	
Data quality and data minimization	
Notification of the data subjects on the processing activity	
Exercising of the rights of the data subjects	
The parties are involved in the processing and their specific roles	
Measures to ensure compliance by the parties involved, if any	
Processing safeguard of the personal data	
Safeguard prior to and Cross border transfers, if any	

Part 3: The measures envisaged for addressing the risks and the safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Data Protection Act

Risk Assessment - Identifying Privacy Risks and Evaluating Privacy Solutions							
Risk Identity and Description	*Consequence*	*Risk Owner*	*Current internal CONTROLS (provide details of how you will manage the risk)*	*Assessment of Risk*			*Describe what further ACTIONS you will take to reduce the Impact/Likelihood and mitigate the risk. State who is the risk owner for each action*
				Impact (1,2,3,4,5)	Likelihood (1,2,3,4,5)	=Score(impact + likelihood)	

Part 5: Sign Off and Record Outcomes

ITEM DESCRIPTION	NOTES/INSTRUCTIONS
Consultation with Office of the Data Protection Commissioner (where applicable)	
This DPIA will be kept under review by:	

Made on the 7th December, 2021.

JOE MUCHERU,
Cabinet Secretary, Ministry of Information, Communication, Technology, Innovation and Youth Affairs.

LEGAL NOTICE NO. 264

THE DATA PROTECTION ACT

(No. 24 *of* 2019*)*

THE DATA PROTECTION (COMPLAINTS HANDLING AND ENFORCEMENT PROCEDURES) REGULATIONS, 2021

ARRANGEMENT OF REGULATIONS

Regulation

THE DATA PROTECTION ACT, 2019

(No. 24 of 2019)

IN EXERCISE of the powers conferred by section 71 of Data Protection Act, 2019, the Cabinet Secretary for Information, Communications, Technology, Innovation and Youth Affairs makes the following Regulations—

THE DATA PROTECTION (COMPLAINTS HANDLING PROCEDURE AND ENFORCEMENT) REGULATIONS, 2021

PART I—PRELIMINARY

Citation.

1. These Regulations may be cited as the Data Protection (Complaints Handling Procedure and Enforcement) Regulations, 2021.

Interpretation.

2. In these Regulations, unless the context otherwise requires —

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

"complainant" means a data subject or a person who has lodged a complaint pursuant to regulation 4;

"Data Commissioner" means the person appointed under section 6 of the Act;

"Office" means the office of the Data Protection Commissioner;

"enforcement notice" means a notice issued by the Data Commissioner under regulation 16;

"penalty" means a penalty imposed by a penalty notice;

"penalty notice" means a notice issued by the Data Commissioner under regulation 20;

"respondent" means a person against whom a complaint is lodged; and

"summons" means an order of the Data Commissioner, in writing, directing a person to appear before the Office.

Object and purpose of the Regulations.

3. The object and purpose of these Regulations is to—

(a) facilitate a fair, impartial, just, expeditious, proportionate and affordable determination of complaints lodged with the Data Commissioner in accordance with the Act and these Regulations, without undue regard to technicalities of procedure;

(b) provide for issuance of enforcement notices as contemplated under section 58 of the Act;

(c) provide for issuance of issuance of penalty notices as contemplated under section 62 of the Act;

(d) provide for the procedure for hearing and determining of complaints; and

(e) provide for the resolution of complaints lodged with the Data Commissioner by means of alternative dispute resolution mechanisms as specified under section 9(1) (c) of the Act.

PART II—PROCEDURE FOR LODGING, ADMISSION AND RESPONSE TO COMPLAINTS

Lodging of a complaint.

4. (1) Pursuant to section 56 of the Act, a data subject or any person aggrieved on any matter under the Act may lodge a complaint with the Data Commissioner.

(2) A complaint lodged under sub-regulation (1) may be lodged in Form DPC 1 set out in the Schedule—

(a) orally, subject to section 56(3) of the Act;

(b) through electronic means, including email, web posting, complaint management information system; or

(c) by any other appropriate means.

(3) A complaint under sub-regulation (1) may be lodged—

(a) by the complainant in person;

(b) by a person acting on behalf of the complainant;

(c) by any other person authorized by law to act on behalf of a data subject; or

(d) anonymously.

(4) The Data Commissioner shall acknowledge receipt of the complaint within seven days of receipt of the complaint under sub-regulation (1).

(5) The complaint under sub-regulation (1) shall be lodged free of charge.

Register of complaints.

5. (1) The Data Commissioner shall keep and maintain an up to date Register of Complaints.

(2) An entry into the register of complaints shall state the particulars of the complainant and the complaint filed with the Data Commissioner.

(3) The Data Commissioner shall protect the identity of the complainant where the request to protect the identity is sought by the complainant.

Admission of complaint.

6. (1) The Data Commissioner shall undertake a preliminary review of a complaint, upon receipt of the complaint by the Office.

(2) The Data Commissioner may, upon undertaking a preliminary review of the complaint—

(a) admit the complaint;

(b) where applicable, advise the complainant in writing that the matter is not within the mandate of the Data Commissioner; or

(c) advise the complainant that the matter lies for determination by another body or institution and refer the complainant to that body or institution.

(3) Despite sub-regulation (2), the Data Commissioner may

decline to admit a complaint where the complaint does not raise any issue under the Act.

(4) Upon admission of a complaint, the Data Commissioner may—

(a) conduct an inquiry into the complaint;

(b) conduct investigations;

(c) facilitate mediation, conciliation or negotiation in accordance with the Act and these Regulations; or

(d) use any other mechanisms to resolve the complaint.

(5) Where a complaint is declined for admission under sub-regulation (3), the complaint may be re-admitted within six months from the date of decline, where the complaint raises new issues for determination under the Act.

(6) A complaint under sub-regulation (5) shall be lodged in accordance with regulation 4.

Discontinuation of a complaint.

7. (1) The Data Commissioner may discontinue an existing complaint in Form DPC 2 set out in the Schedule, where—

(a) a complaint does not merit further consideration; or

(b) a complainant refuses, fails or neglects to communicate without justifiable cause.

(2) The Data Commissioner shall provide the reasons for discontinuation on any of the grounds specified under sub-regulation (1) (a) or (b) and shall, in writing, notify the complainant and respondent within fourteen days from the date the decision to discontinue a complaint is made.

(3) A complainant may, where a complaint has been discontinued pursuant to these Regulations, re-institute a complaint upon providing grounds for the restitution to the Data Commissioner.

Withdrawal of a complaint.

8. (1) A complaint may be withdrawn at any stage during its consideration but before a determination is made.

(2) A complainant may, at any time during the consideration of a complaint lodged pursuant to regulation 4 and before its determination, withdraw the complaint.

(3) An application for a withdrawal under sub-regulation (1) shall be in Form DPC 2 set out in the Schedule.

(4) A withdrawn complaint under sub-regulation (1) may be re-lodged, within six months from the date of withdrawal of such complaint.

(5) A complaint re-lodged under this regulation shall be processed in accordance with the provisions of this Part.

Joint consideration of complaints.

9. (1) Where two or more complaints are lodged in which similar issues are raised against a respondent, the Data Commissioner may with the consent of the complainants—

(a) consolidate the complaints and make a determination; or

(b) treat one complaint as a test complaint and stay further action on the other complaints pending resolution of the test complaint.

(2)The Data Commissioner shall, with necessary modifications, apply the decision of a test complaint to all the complaints stayed under sub-regulation (1)(b).

(3) The Data Commissioner shall, in writing, communicate to the complainants and all the parties the decision made under this regulation.

(4) Where complaints are consolidated in accordance with this regulation, the complaint shall be treated as a single complaint and shall be determined in accordance with the provisions of these Regulations.

Language.

10. (1) Proceedings before the Office shall be conducted in Kiswahili, English or Kenyan Sign Language.

(2) The Office may ensure that a party who cannot speak, hear or understand the language of proceedings receives the services of an interpreter provided for by the Office.

Notification of a complaint to the respondent.

11. (1) Upon admission of a complaint, the Data Commissioner shall notify the respondent of the complaint lodged against him, in Form DPC 3 set out in the Schedule and shall require the respondent to within twenty-one days —

(a) make representations and provide any relevant material or evidence in support of its representations;

(b) review the complaint with a view of summarily resolving the complaint to the satisfaction of the complainant; or

(c) provide a response with the required information.

(2) Where a respondent does not take any action as contemplated under sub-regulation (1), the Data Commissioner shall proceed to determine the complaint in accordance with the Act and these Regulations.

(3) The notice referred to under sub-regulation (1) shall specify options available to resolve a complaint including determining the complaint through alternative dispute resolution mechanisms specified in the Act and these Regulations.

Joinder of parties.

12. (1) Where it appears to the Data Commissioner, or by an application by either the complainant or the respondent, that it is necessary that a person becomes a party to a complaint, the Data Commissioner may order that person to be enjoined as a party.

(2) A person who has sufficient interest in the outcome of a complaint may apply to the Office for leave to be enjoined in the proceedings prior to the hearing of the complaint.

(3) An application under sub-regulation (1) shall include —

(a) the names of the parties to which that application relates;

(b) the name and address for service of the person wishing to be enjoined;

(c) the grounds the applicant relies on to be enjoined;

(d) a copy of any relevant document in support of the application; and

(e) the relief sought.

Investigations of a complaint.

13. (1) In investigating a complaint, the Data Commissioner may, subject to section 57 of the Act—

(a) issue summons in Form DPC 4 set out in the Schedule requiring the attendance of any person at a specified date, time and place for examination;

(b) examine any person in relation to a complaint;

(c) administer an oath or affirmation on any person during the proceedings;

(d) require any person to produce any document or information from a person or institution; and

(e) on obtaining warrants from the court, enter into any establishment or premises and conduct a search and may seize any material relevant to the investigation.

(2) Upon completion of the investigation, the Data Commissioner shall prepare an investigation report.

(3) In conducting investigations under this regulation, the Data Commissioner shall be guided by the provisions of the Fair Administrative Action Act, 2015.

No. 4 of 2015.

Outcome of investigation.

14. (1) The Data Commissioner shall, upon the conclusion of the investigations, make a determination based on the findings of the investigations.

(2) A determination under sub-regulation (1) shall be in writing and shall state—

(a) the nature of the complaint;

(b) a summary of the relevant facts and evidence adduced;

(c) the decision and the reasons for the decision;

(d) the remedy to which the complainant is entitled; and

(e) any other relevant matter.

(3) The remedies contemplated under sub-regulation (2) (d) may include—

(a) issuance of an enforcement notice to the respondent in accordance with the Act and these Regulations;

(b) issuance of a penalty notice imposing an administrative fine

where a respondent fails to comply with the enforcement notice;

(c) dismissal of the complaint where it lacks merit;

(d) recommendation for prosecution; or

(e) an order for compensation to the data subject by the respondent.

(4) The Data Commissioner shall within seven days from the date of such determination, communicate the decision under sub-regulation (3) to the parties, in writing.

(5) The decision of the Data Commissioner made under these Regulations shall be—

(a) binding on the parties; and

(b) shall be enforced as an order of the Court.

Negotiation, mediation or conciliation.

15. (1) Where the complaint is to be determined through negotiations, mediation or conciliation, the provisions of these Regulations shall apply.

(2)Where parties to a complaint agree to negotiation, mediation or conciliation, the Data Commissioner may in consultation with the parties facilitate the process.

(3) During the negotiations, mediation or conciliation, the Data Commissioner may apply such procedures as may, in the interest of the parties, deem appropriate in the circumstances.

(4) At the conclusion of the negotiations, mediation or conciliation process, the parties shall sign a negotiation, mediation or conciliation agreement in the manner specified in Form DPC 5 set out in the Schedule.

(5) A negotiation, mediation or conciliation agreement entered into under this regulation shall be deemed to be a determination of the Data Commissioner, and shall be enforceable as such.

(6) Despite this regulation, a party to dispute who is subject to a negotiation, mediation or conciliation may withdraw from the proceedings at any stage and shall notify the Data Commissioner and other parties of such withdrawal within seven days from the date of making such a decision.

(7) Parties to a dispute shall take all reasonable measures to amicably determine a dispute and act in good faith.

(8) Where the complaint is not determined through negotiation, mediation or conciliation, the Data Commissioner shall proceed to determine the complaint as provided for in the Act and these Regulations.

PART III—ENFORCEMENT PROVISIONS

Issuance of enforcement notice.

16. (1) The Data Commissioner may pursuant these Regulations or section 58 of the Act issue an enforcement notice.

(2) An enforcement notice shall specify the consequences of failure to comply with the notice including issuance of a penalty notice as provided under section 62 (1) of the Act.

Service of an enforcement notice.

17. (1) An enforcement notice shall be deemed to have been duly served on the concerned person where—

(a) an electronic copy of enforcement notice is sent to the concerned person's last used email address; or

(b) the enforcement notice is posted or physically delivered to the registered offices of the concerned person, in the absence of an electronic address.

(2) The enforcement notice shall take effect from the date of service specified under sub-regulation (1).

Review of enforcement notice.

18. (1) A person to whom an enforcement notice is given may apply in Form DPC 6 set out in the Schedule to the Data Commissioner for a review of the enforcement notice.

(2) An application under sub-regulation (1) may be made —

(a) before the end of the period specified in the enforcement notice; and

(b) on the ground that—

(i) a change of circumstances or new facts have arisen; or

(ii) one or more of the provisions of that notice need not be complied with in order to remedy the failure identified in the notice.

Appeals against enforcement notice.

19. Subject to sections 58 (2) (d) and 64 of the Act, a person may before the lapse of thirty days from the date of service of the enforcement notice, appeal to the High Court against a decision arising out of the enforcement of the notice.

Issuance of penalty notice.

20. (1) The Data Commissioner shall, where any of the circumstances specified under section 62 of the Act and these Regulations arises, issue a penalty notice for each breach identified in the enforcement notice.

(2) A penalty notice shall contain—

(a) the name and address of the concerned person, to whom it is addressed;

(b) the reasons why the Data Commissioner proposes to impose the penalty and the amount thereof;

(c) an administrative fine imposed as contemplated under section 63 of the Act;

(d) details of how the penalty is to be paid; and

(e) details of the rights of appeal under section 64 of the Act.

(3) The administrative fine levied under sub-regulation (2)(c) shall consider each individual case and have due regard to factors or reasons outlined under section 62 (2) of the Act.

(4) A penalty notice may impose a daily fine of not more than ten thousand shillings for each breach identified until the breach is rectified.

(5) The daily fine imposed under sub regulation (4) shall be managed in accordance with section 67 of the Act and the Public Finance Management Act, 2012.

Enforcement of penalty notice.

21. The Data Commissioner shall enforce or take action to recover a penalty—

(a) upon the lapse of the period specified in the penalty notice for payment of the penalty;

(b) on the final determination of any appeal against the penalty notice; or

(c) on the lapse of the period given to appeal against the penalty.

SCHEDULE

FORM DPC 1 (r. 4 (2)(a))

COMPLAINT SUBMISSION FORM

A. PARTICULARS OF THE COMPLAINANT/ REPRESENTATIVE	
Full Names	
National Identification Card Number/ Passport Number	
Contact information (Phone number/ email address)	
B. PARTICULARS OF THE COMPLAINT	
Describe your complaint;	
Indicate to whom the complaint is against;	
When did you become aware of the alleged breach	
C. REMEDY SOUGHT	
Explain the remedy you are seeking for the alleged breach;	
D. Which other steps have you already taken in relation to the Complaint, if any	
State any other institution contacted over the complaint, if any.	

Signature Date

Note

** If the space provided for in this Form is inadequate, submit information as an annex.*

** If you have supporting documents to substantiate your claim, please annex copies to this Form.*

** The information submitted will be treated with the upmost confidentiality.*

FORM DPC 2 (r. 7(1) & r.8(3))

REQUEST TO DISCONTINUE OR WITHDRAW A COMPLIANT

A. NATURE OF REQUEST	
Mark the appropriate the box with an "x". Request for: DISCONTINUATION ☐ WITHDRAWAL ☐	
B. PARTICULARS OF THE COMPLAINANT/ REPRESENTATIVE	
Full names	
National Identification Card Number/ Passport Number	
Contact Information (Phone Number/ Email Address)	
C. NATURE OF THE COMPLAINT	
Complaint Number/Reference Number	
D. STATE REASON FOR WITHDRAWAL/DISCONTINUATION OF COMPLAINT	

Signature Date

Note:

**If the space provided for in this Form is inadequate, submit information as an Annexure to this form*

**If you have supporting documents to substantiate your claim, please annex copies to this Form.*

**The information submitted will be treated with the upmost confidentiality.*

FORM DPC (r.11 (1))

Notification of a complaint to the Respondent

Details of the Respondent	
Full names	
Complaints Register entry number	
Email address	
Details of the Complainant	
Full Names	
National Identification Card Number/ Passport Number	
Contact information	
Particulars of the Complaint	
Representations to be made to the Data Commissioner by:	

Signature Date

FORM DPC 4 (r.13 (1) (a))

Summons to Enter Appearance

OFFICE OF THE DATA PROTECTION COMMISSIONER

COMPLAINT NO…….. OF ……

_____ } Complainant

AGAINST

_____ } Respondent

TO: _____

_____ *Person required to attend*

_____

WHEREAS the above-named Complainant has instituted a Complaint against you, the Respondent particulars of which are set out in the copy of Complaint annexed herewith.

YOU ARE HEREBY REQUIRED to attend to the Office of the Data Commissioner on _____(Date), _____ _____(*Venue)* At _____ _____(*Time)* (am/pm)

Should you fail to attend to the above mentioned summons, you may be liable to an offence under section 57 of the Data Protection Act, 2019.

Dated…… day of ……. 20…..

……

Data Commissioner

Form DPC 5 (r. 15 (4))

ALTERNATIVE DISPUTE RESOLUTION SETTLEMENT AGREEMENT

The undersigned parties, on this _____ day of _____,_ , have agreed to the following settlement of their dispute concerning _____
_____
_____,and hereby memorialize such agreement according to the following terms:

_____
_____
_____,_____

The Settlement Agreement is binding on the parties and is admissible in court for enforcement purposes.

In order to facilitate the above-specified terms of settlement, the parties further agree that on or before the _____day of _____, 20_, they will Complainant:_____
_____
_____
_____
_____

Respondent:
_____
_____

Complainant:

Signature Date

_____ _____

Respondent:

Signature Date

_____ _____

Form DPC 6 (r. 18 (1))

REVIEW OF ENFORCEMENT NOTICE

A. PARTICULARS OF THE PERSON ISSUED WITH THE ENFORCEMENT NOTICE	
Full Names	
Registration Number/ Identification Number	
Contact information (Phone number/ email address)	
B. REFERENCE NUMBER OF THE ENFORCEMENT NOTICE	
C. GROUNDS FOR REVIEW OF THE ENFORCEMENT NOTICE (*tick as appropriate)*	
(i) Change of circumstances or new facts have arisen; or	☐
(ii) One or more of the provisions of that notice need not be complied with in order to remedy the failure identified in the notice.	☐

Note:

**If the space provided for in this Form is inadequate, submit information as an Annex to this Form*

**If you have supporting documents to substantiate your claim, please annex copies to this Form.*

**The information submitted will be treated with the upmost confidentiality.*

Made on the 7th December, 2021.

JOE MUCHERU,
Cabinet Secretary, Ministry of Information, Communications, Technology, Innovation and Youth Affairs.

LEGAL NOTICE NO. 265

THE DATA PROTECTION ACT

(*No*. 24 *of* 2019)

THE DATA PROTECTION (REGISTRATION OF DATA CONTROLLERS AND DATA PROCESSORS) REGULATIONS, 2021

ARRANGEMENT OF REGULATIONS

Regulation

THE DATA PROTECTION ACT

(No. 24 *of* 2019*)*

IN EXERCISE of the powers conferred by section 71 of the Data Protection Act, 2019, the Cabinet Secretary for Information, Communication, Technology, Innovation and Youth Affairs, makes the following Regulations—

THE DATA PROTECTION (REGISTRATION OF DATA CONTROLLERS AND DATA PROCESSORS) REGULATIONS, 2021

Citation and commencement.

1. (1) These Regulations may be cited as the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021.

(2) The provisions of these Regulations shall come into effect six months from the date of publication.

Interpretation No. 24 of 2019.

2. In these Regulations, unless the context otherwise requires—

"Act" means the Data Protection Act, 2019;

"Data Commissioner" means the person appointed under section 6 of the Act;

"data controller" has the meaning assigned to it under the Act;

"data processor" has the meaning assigned to it under the Act;

"register" has the meaning assigned to it under the Act;

"Office" has the meaning assigned to it under the Act;

"establishment documents" include—

(a) a Statute, Charter or statutory instrument in which a body is established;

(b) registration certificate;

(c) trust deeds in which a trust has been established; and

(d) other instruments by which a body is established including its governing and administrative structure.

Scope of Regulations.

3. (1) These Regulations provide for the procedure for registration of data controllers and data processors as provided under section 18 of the Act.

(2) These Regulations shall not apply to civil registration entities specified under the Data Protection (Civil Registration) Regulations, 2020.

L.N. No. 100 of 2020.

Requirements for registration.

4. (1) Subject to regulation 13 (1), every data controller and data processor shall be required to register in accordance with the provisions of the Act and these Regulations.

(2) For purposes of registration, a person shall register as a—

(a) data controller, where the person determines the purpose and means for processing personal data; or

(b) data processor, where the person processes personal data on behalf of the data controller but excludes employees of the data controller and has—

(i) a contractual relationship with the data controller; and

(ii) no decision making power on the purpose and means of processing personal data.

(3) Despite sub-regulation (2) (a), a data controller may apply for registration as both a data controller and a data processor with regards to any processing operations and shall be required to pay the requisite fees applicable for both a data controller and a data processor thereto.

(4) Despite sub-regulation (2) (b), where a data processor processes personal data other than as instructed by the data controller, thedata processor shall be considered to be a data controller in respect of that processing activity, for purposes of assessing liability.

Application for registration.

5. (1) An application for registration of a data controller or data processor shall—

(a) be in Form DPR1 set out in the First Schedule; and

(b) be accompanied by the registration fees specified in the Second Schedule.

(2) An application for registration under sub-regulation (1) shall be accompanied by—

(a) a copy of the establishment documents;

(b) particulars of the data controllers or data processors including name and contact details;

(c) a description of the purpose for which personal data is processed; and

(d) a description of categories of personal data being processed.

Payment of registration fees by specified public bodies.

6. (1) A state department or county department shall register and pay the fees on behalf of their respective entities.

(2) The entities referred to under sub-regulation (1) shall be the public entities at national or county government which—

(a) operates within a state department or county department;

(b) is wholly funded from the Consolidated Fund; and

(c) provides a public service.

(3) The fees paid by the state department or county department under sub-regulation (1) shall cater for the specified entities registered under the concerned state department or county department.

(4) Despite this regulation, a State Corporation or a County Corporation shall be required to register as a data controller or a data processor in respect of their processing activity, in the manner specified under these Regulations.

Processing ofan application for registration.

7. The Data Commissioner shall undertake a verification process of the details provided in the application for registration.

Approval and issuance of certificate of registration.

8. Where the Data Commissioner is satisfied that the applicant fulfills the requirements for registration under these Regulations, the Data Commissioner shall, within fourteen days—

(a) issue the applicant with a certificate of registration for the duration specified under regulation 9; and

(b) enter the particulars of the successful applicant in the register.

Duration of certificate of registration.

9. A certificate of registration issued under regulation 8 (a) shall be valid for a period of twenty-four months from the date of issuance.

Refusal of registration.

10. (1) Where the Data Commissioner declines to approve an application for registration, the Data Commissioner shall within twenty-one days from the date of such decision—

(a) notify, in writing, the applicant of the refusal; and

(b) provide reasons for such refusal.

(2) The Data Commissioner may decline to grant an application for registration, where the—

(a) particulars provided for inclusion in an entry in the register are insufficient;

(b) appropriate safeguards for the protection of the privacy of the data subject have not been provided by the data controller or a data processor; or

(c) the data controller or data processor is in violation of any provisions of the Act and these Regulations.

(3) A data controller or data processor whose application for registration has been declined under these Regulations may make a fresh application upon complying with the requirements specified in the refusal notice.

(4) An application under sub-regulation (3) shall be processed as any other application and in the manner specified under these Regulations.

Renewal of registration.

11. (1) Pursuant to section 20 of the Act, a registered data controller or data processor shall apply for a renewal of registration as a data controller or data processor, after the expiry of the certificate of registration.

(2) An application for renewal of a certificate of registration shall be—

(a) made in Form PR 2 set out in the First Schedule; and

(b) accompanied by the appropriate renewal fee specified in the Second Schedule.

(3) The Data Commissioner shall, upon receipt of the application,

and where satisfied that the applicant complies with the requirements for registration, renew the certificate of registration.

(4) Despite sub-regulation (2), where renewal is for a distinct purpose or categories of data other than that for which the data controller or data processor had been registered for, the Data Commissioner shall undertake a verification process in the manner provided under regulation 7.

Refusal of renewal.

12. (1) Where the Data Commissioner declines to renew an application for registration, the Data Commissioner shall within twenty-one days from the date of such decision—

(a) notify, in writing, the applicant of the refusal; and

(b) provide reasons for such refusal.

(2) The provisions of regulation 10 shall, with necessary modifications, apply where refusal to renew notice is to be or has been issued.

Exemption from mandatory registration.

13. (1) For purposes of this regulation—

"revenue" means the total income of profit-making data controllers or data processors for the year immediately preceding the year of registration;

"turnover" means the utilized annual budget of non-profit making data controllers or data processors for the year immediately preceding the year of registration;

"non-profit making data controller or data processors" means an entity whose core mandate excludes the generation of profit and includes non-governmental organizations, charitable and religious institutions, multi-lateral agencies or civil society organizations.

(2) A data controller or data processor is exempt from mandatory registration under these Regulations where the data controller or data processor—

(a) has an annual turnover of below five million shillings or annual revenue of below five million shillings; and

(b) has less than ten employees.

(3) Despite the provisions of sub-regulation (2), the data controller and data processor exempt under sub-regulation (2) shall be required to comply with the provisions of the Part IV and Part VI of the Act.

(4) The exemption provided under sub-regulation (1) shall not apply to a data controller or data processor whose annual turnover is below five million shillings and processes personal data for the purposes specified under the Third Schedule.

(5) The data controllers and data processors contemplated under sub-regulation (2), shall be required to undertake mandatory registration in accordance with Part III of the Act and these Regulations.

Register.

14. (1) Subject to section 21 of the Act, the Data Commissioner shall keep and maintain an up to date register which shall contain—

(a) the names and particulars of registered data controllers and data processors;

(b) categories of personal data being processed by the data controllers and data processors;

(c) the address of the principal places of business of the data controllers and data processors;

(d) where applicable, details of data protection officers; and

(e) any other relevant particular.

(2) The Office shall, once every thirty days, publish on the official website a list of registered data controllers or data processors.

Change of particulars.

15. (1) Subject to section 19(2) of the Act, a data controller or data processor shall, within fourteen days of the occurrence of any changes in the particulars of a data controller or a data processor, notify the Data Commissioner in writing.

(2) The Data Commissioner shall, on receiving the notification make the necessary changes on the register, where necessary.

(3) The Data Commissioner may prior to making any change on the register, request for any necessary documents or proof thereof.

(4) A data controller or data processor who contravenes this regulation commits an offence and shall, on conviction, be liable to the penalty specified under section 73 of the Act.

Cancellation or variation of registration.

16. (1) Subject to section 22 of the Act, the Data Commissioner may cancel a certificate of registration or vary the conditions for registration, where –

(a) the data controller or data processor applies for cancellation or variation;

(b) the Data Commissioner establishes that the data controller or data processor provided false or misleading information in relation to any registration particulars; or

(c) the data controller or data processor willfully or negligently, fails to comply with provisions of the Act and any Regulations made thereunder.

(2) The Data Commissioner shall, before cancelling or varying the conditions of registration, be guided by the provisions of the Fair Administrative Actions Act, 2015. No. 4 of 2015.

Electronic registration.

17. An application made under these Regulations shall be submitted through electronic means provided for on the Office website.

Offences.

18. A data controller or a data processor who—

(a) processes personal data without registering in accordance with these Regulations;

(b) provides false or misleading information for the purpose of registration; or

(c) fails to renew a certificate of registration and continues to process personal data after the expiry of the certificate,

commits an offence and shall, upon conviction, be liable to penalty specified under section 73 of the Act.

FIRST SCHEDULE

FORM DPR 1 (r. 5(1(a))

REGISTRATION FORM FOR DATA CONTROLLERS AND DATA PROCESSORS

SECTION 1 – BASIC DETAILS	
Indicate if you are registering as a Data Controller ☐ Data Processor ☐	
Name:	
Postal Address:	
Telephone Number:	
Email Address:	
County:	
Countr:	
Sector:	
Legal establishment:	
For public body: (Specify the state department or county department)	

SECTION 2 – PERSONAL DATA		
Provided the details of the various subsets of personal data being processed and the purpose of processing.		
CATEGORY OF DATA SUBJECTS (E.g. employee, client, students, supplier, shareholder, etc.)	DESCRIPTION OF PERSONAL DATA TO BE PROCESSED (E.g. name, address, Identification number etc.)	PURPOSE OF PROCESSING (E.g. for payroll, invoicing, Know Your Customer (KYC), registration, etc.)

SECTION 3 – SENSITIVE PERSONAL DATA

Applicable ( ) Not Applicable ( )

If applicable, please fill in the below details, otherwise please proceed to section 4

Please select the type(s) of sensitive categories of personal data you process	Specify purpose(s) for processing sensitive personal data:
Racial or ethnic origin	
Political opinion or adherence	
Religious or philosophical beliefs	
Marital status and family details	
Physical or mental health or condition	
Sexual orientation, practices or preferences	
biometric data	

SECTION 4 – TRANSFER OF DATA OUTSIDE KENYA

Applicable ( ) Not Applicable ( )

If applicable, please fill in the below details, otherwise please proceed to section 5.

List the country/(ies):

SECTION 5 – MEASURES FOR PROTECTION OF PERSONAL DATA

No.	Identify risks to personal data (E.g. unauthorized access/disclosure, theft, etc.)	Safeguards, security measures and mechanisms implemented to protect personal data (E.g. Access control, visitors' logbook, privacy policy, information security policy, etc.)
1		
2		
3		
4		
5		

SECTION 6: NUMBER OF EMPLOYEES (INDICATE BY TICKING)

Organization with 1-9 employees	
Organization with 10-49 employees	
Organization with 50-99 employees	
Organization with more than 99 employees	

SECTION 7: PREVIOUS YEAR ANNUAL TURNOVER (INDICATE BY TICKING)

Organization has less than KES 2,000,000 annual turnover	
Organization has KES 2,000,000-5,000,000 annual turnover	
Organization has KES 5,000,000-10,000,000 annual turnover	
Organization has KES 10,000,000-50,000,000 annual turnover	
Organization with more than KES 50,000,000 annual turnover	

I certify that the particulars provided are correct and complete and hereby apply to be registered as Data Controller or a data Processor.

Signature: _____

Date: _____

Name: _____

FORMDPR 2 (r. 11 (2)(a))

RENEWAL FORM FOR DATA CONTROLLERS AND DATA PROCESSORS

Indicate if you are registering as a—

Data Controller ☐ Data Processor ☐

SECTION 1 – BASIC DETAILS	
Name:	
Postal Address:	
Telephone Number:	
Email Address:	
Country:	
Sector:	
Legal Establishment	
For public body: (Specify the state department or county department)	
SECTION 2: DISTINCT PURPOSE	
Specify whether renewal is for a distinct purpose or categories of data other than that for which the data controller or data processor had been registered for, respectively-	

SECOND SCHEDULE

Fees charged by office(r. 5(2)(b)

Category	*Description*	*Registration fee in Kshs. per Data Controller/Processor) (payable Once)*	*Renewal fee in Kshs. per Data Controller/Processor) (after every 2 years)*
Micro and Small Data Controllers /Processors	A data controller/ processor with between 1 and 50 employees and an annual turnover/revenue of a maximum of Kshs 5Million	4,000	2,000
Medium Data Controllers /Processors	A data controller/ processor with between 51 and 99 employees and an annual turnover/revenue of between Kshs 5,000,001 and maximum of Kshs 50,000,000	16,000	9,000
Large Data Controllers /Processors	Data controller/processor with more than 99 employees and an annual turnover/revenue of more than Kshs 50Million	40,000	25,000

Public entities	Data controller/processor offering government functions (Regardless of number of employees or revenue/turnover)	4,000	2,000
Charities and Religious entities	Data controller or Data processor offering charity or religious functions (Regardless or revenue/turnover)	4,000	2,000

THIRD SCHEDULE

THRESHOLDS FOR MANDATORY REGISTRATION *(r. 13(3))*

A data controller or data processor processing personal data for the following purposes shall register as a data controller or a data processor as provided for under these Regulations—

1. Canvassing political support among the electorate.
2. Crime prevention and prosecution of offenders (including operating security CCTV systems).
3. Gambling.
4. Operating an educational institution.
5. Health administration and provision of patient care.
6. Hospitality industry firms but excludes tour guides.
7. Property management including the selling of land.
8. Provision of financial services.
9. Telecommunications network or service providers.
10. Businesses that are wholly or mainly in direct marketing.
11. Transport services firms (including online passenger hailing applications)
12. Businesses that process genetic data.

Made on the 7th December, 2021.

JOE MUCHERU,
Cabinet Secretary, Ministry of Information,
Communication, Technology, Innovation and Youth Affairs.

PRINTED AND PUBLISHED BY THE GOVERNMENT PRINTER, NAIROBI