11 May 2021,

Taskforce on the Development of the Data Protection Regulations,
The Ministry of ICT, Innovation and Youth Affairs,
Nairobi.

Dear Sirs,

RE: Memorandum on the Data Protection Regulations

The Kenya ICT Action Network (KICTAnet is a multistakeholder think tank whose overall objective is to act as a catalyst for reform in the ICT sector through public policy advocacy, research, and multi stakeholder engagement at both national, regional and global processes. KICTAnet has established strong partnerships within the region with representatives of government, private sector, civil society, academia, philanthropic organizations and the technical community within Africa. The Network conducts research and country-level studies and has produced reports, policy briefs and toolkits on various ICT policy issues which are available online. The KICTANet mailing list serves as an online platform for information, debate and discussion on key local and global ICT policy issues.

Currently, KICTANet supports ICT reforms through advocacy, research, capacity building, and technology for public interest. KICTANet infuses a multi-stakeholder approach to promote cooperation and collaboration among its diverse membership.

The Kenya ICT Action Network (KICTAnet) presents this memorandum in response to the call by the Ministry of ICT, Innovation and Youth Affairs through a Taskforce on the development of the Data Protection Regulations for public participation on the Data Protection (General) Regulations, 2021, the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021, and the Data Protection (Compliance and Enforcement) Regulations, 2021.

I can be reached on 0722701495 or on ggithaiga@kictanet.or.ke

Kind regards,

Grace Githaiga

Grace Githaiga,
Convenor

Memorandum on the:

1. **Data Protection (General) Regulations, 2021;**
2. **The Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021; and,**
3. **Data Protection (Compliance and Enforcement) Regulations, 2021**

Submitted to:

The Ministry of ICT, Innovation and Youth Affairs Taskforce on the development of the Data Protection Regulations

Contact:

The Kenya ICT Action Network

PO Box 14866 - 00800,

Nairobi.

Email: ggithaiga@kictanet.or.ke / info@kictanet.or.ke

www.kictanet.or.ke

11 May 2021

Table of Contents

GENERAL COMMENTS

No.	Proposal	Concerns and Justification
1	Review all the three regulations to ensure that they are data subject centric and less bureaucratic.	The purpose of having a Data Protection Law in Kenya is to ensure that Kenyans data is protected. However, these regulations appear to create more bureaucratic hurdles for data subjects to exercise their rights. This is seen throughout the Regulations e.g. various forms to exercise one's rights, the complex process of registration of data controllers and data processors etc. The data subject should be at the core of the objectives of the Regulations to enable them exercise their rights without procedural hurdles. Currently, the ODPC risks being reduced to a registration office and not one whose purpose is to provide oversight of data protection to ensure data subjects rights are protected. ODPC can develop an online portal such as the NTSA/eCitizen to facilitate a data subject centric approach to regulation.
2	The role of making regulations is with the Cabinet Secretary as is in the Data Protection Act.	The only Regulations in compliance with the DPA is The Data Protection (General) Regulations, 2021 which is drafted by the CS of ICT through the powers conferred to them under Section 71 of the DPA. The Data Protection (Compliance And Enforcement) Regulations, 2021 have been drafted by the ODPC yet this should not be the case. Given that two of the regulations are issued by the ODPC, this contravenes section 71 of the DPA 2019 which provides that only the CS, Ministry of ICT, has the power to develop the regulations. Section 74 of the DPA limits the ODPC to issue guidelines or codes of practice for the Data Controllers, Data Processors and Data Protection Officers. Further, sections 18, 31, 54, 61 of the DPA do not grant the ODPC power to make regulations.
3	Review the bureaucratic effect of various forms in the regulations on achieving compliance. A needs and risk based approach to achieving compliance should be adopted. This will ensure the resources of the ODPC are directed where there is the highest	Currently, the regulations provide forms to enable compliance e.g registration. In our view, these are too many requirements and forms, which may create a bureaucracy and result in avoidance or non-compliance. In turn this will affect the realisation of the objectives of the DPA. The requirements under each of the regulations may prove to be a challenge to implement especially by Small and Medium Sized Companies. Kenya can borrow a leaf from the GDPR which advocates on selective implementation of certain sections of

	risk, and they have a procedure where after every year or two they review and find out the risks.	the GDPR. The GDPR takes the approach of how much data a company processes and if the data collection is at the core of the business. This approach is particularly geared to SMEs in order to avoid burdening them with the cost of implementation of the GDPR. When it comes to the registration of data processors and controllers, Kenya can peg it on level or risk, based on the nature of the activities, the type of organization or type of processing. Activities that present high risks for the individuals' rights and freedoms, whether they are carried out by an SME or by a large corporation, should trigger a stringent compliance with the regulations.
4	The compliance levels required in the regulations should be viewed against the capacity of, and the resources available to the ODPC to enforce, and of the data processors and collectors to implement the regulations.	The ODPC should analyse whether they have the capacity to provide oversight, and at the same time, register all the data controllers and processors and conduct investigations on data breaches and enforce the DPA. Even though the ODPC can outsource assistance, this should not be tied to requirements where data subjects privacy and protection would be compromised. In addition, the ODPC should also be cognizant of Principle 42 of the Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019 that calls for an office that is independent and composed of human rights and privacy experts. This independence will enable the ODPC make decisions that ensure the rights of data subjects are protected without duress.
5	The regulations should strive to have simple, clear and effective processes and procedures, especially with respect to reporting, investigations, complaints handling, remedies and feedback. These can be done through online portals such as the NTSA/eCitizen.	As it stands, assumptions have been made that data subjects understand their rights and how to hold data processors and controllers responsible with respect to breaches or non compliance with the DPA. In addition, with respect to Data Subject Access Request, this should not be a statutory form. Leeway should be given to organisations to come up with their own forms or documents or procedures to receive and respond to these requests. This will streamline the process. Possibly have bare minimum that should be contained in the requests so as to standardise the form of requests. The regulations should take into account different types of data subjects and should be informed by different sectors.
6	Review the timelines for compliance for individuals and organizations.	The Act was not operational until recently despite the law being passed in 2019. The mechanisms for compliance were absent, until recently. For example, the regulations require online registration for data

		processors and controllers, yet it is not clear whether these are ready. The ODPC should regularly communicate the changes and timelines for compliance with the public to promote compliance.
7	The ODPC should include measures to educate the public and organizations on the application of the DPA and the Regulations	The ODPC has a responsibility to ensure that the public understands their rights as data subjects. They can begin sensitisation by, for example, partnering with key stakeholders such as NGOs, in educating the masses through social media and using language that is friendly to the majority of the populace e.g Kiswahili to demystifying the meaning of privacy.
8	The ODPC should comply with the principles under the DPA 2019, conduct a data protection impact assessment and develop and publish a privacy policy.	The office needs to come with a data protection policy and lead by example in demonstrating how to comply with the Data Protection Act and the privacy principles enshrined therein. It should conduct a data protection impact assessment and also have a privacy policy showing how the data collected is processed and stored in compliance with the DPA. The Taskforce should also review the nature and detail of information required to ensure respect for data minimisation principles.
9	The fees charged for registration or certification should be reasonable.	The fees of 250,000 are inordinately high and exorbitant and does not take into account the relative size and ability of various organizations and the amount of data collected. Given the costs associated with registering as a data controller and data processor, this requirement may discourage compliance or become a barrier to the establishment of startups. In the United Kingdom, there are three tiers based on size and turnover with fees ranging from £40 and £2,900, but for most organisations the fee ranges from £40 to £60. Also, some organisations such as Charities and small occupational pension schemes only pay £40 regardless of their size and turnover.
10	The Taskforce should conduct a needs assessment and environmental scan prior to adopting the regulations under the Data Protection Act.	The regulations would be better informed by a needs assessment, situational assessment and an environmental scan of the various practices of organizations relating to data in the country. This would have enriched the decisions to develop these regulations and informed the various choices made with respect to the framing of the provisions or the thresholds provided in the regulations. Comparatives would also have been made with benchmarks from other jurisdictions such as the European Union, United Kingdom and South Africa etc. Likewise, compliance with international human rights law, and in particular the three-part test - prescribed by law, pursuing a legitimate aim/interest, and is necessary and proportionate.

11	Review the obligations of the ODPC to prioritise quality assurance based on risk and efficiency.	The regulations should require that the ODPC have a sound data management and quality assurance system based on risk and efficiency. The regulations should focus more on the effectiveness of the procedures and processes of data controllers and processors to ensure they work, based on the risk levels. There should be procedures to ensure transparency so that the ODPC is required to document that it knows what it is doing, how they are doing it, and when they do it. If a situational risk assessment is done, the ODPC would need to fast-track the development of guidelines for the sectors that are most at risk given the nature of their current data collection and processing practices. Key sectors e.g. finance and banking sectors, government (Ministry of Interior - national registration bureau, Huduma Namba, and Kenya Revenue Authority, Ministry of Lands), health (hospitals and NHIF), social services - NSSF, insurance firms and Insurance Regulatory Authority, motor vehicle registration - NTSA TIMS, telecommunications - mobile operators and ISPs
12	Review obligations of data collectors and processors to prioritise quality assurance based on the data protection principles.	The regulations should focus on processes and procedures to ensure that data controllers and processors adopt and have in place a documented quality assurance system based on the data protection principles, and not just certification). In essence, the data controllers and processors should be required to have documentation that they understand their risks (e.g. data protection impact assessment), documentation of how they processes (e.g. privacy policy), and documentation of how they are complying (e.g. periodic reports). Thus the ODPC can focus on supervising data processors and controllers to ensure they complying with the standards, have in place adequate prevention measures and procedures to ensure safe and honest data management practices. Otherwise compliance could just be a box-ticking exercise.

THE DATA PROTECTION (GENERAL) REGULATIONS, 2021

Regulation	Provision	Proposal	Justification
8 (1 and 4)	A data subject may request to access their personal data in Form 3 set out in the First Schedule (4) A request for access to personal data may be declined on the grounds that (a) giving access would result to a serious threat to the life, health or safety of a data subject, or to public health or public safety; (c) the request for access is frivolous and vexatious;	Delete Regulation 8 (1 and 4)	These are not sufficient grounds for denying someone their right to access data. Clarity is needed on how requesting for one's personal data will lead to threat of life, health or safety of a data subject. Secondly, it should be clear as to what amounts to frivolous and vexatious, as this can easily be misinterpreted.
Regulation 4	Data Subject's Consent for processing	The regulations should specify that in the case of processing of sensitive information, the consent should be refreshed every year and for processing of general personal data, consent should be refreshed after two years.	There is no time period for refreshing consent. The danger is that the data subject is not granted an opportunity to withdraw or amend consent as per best practice. The ICO Guidelines 2018 recommendations have been proposed.

Regulation 4(1)(d)	Subject to section 32 of the Act, a data controller or data processor shall, before processing personal data, inform the data subject —— (a) the nature of personal data to be processed; (b) the scope of personal data to be processed; (c) the reasons for processing the required personal data; and (d) whether the personal data processed shall be shared with third parties.	The subject should also be informed of the purpose, method, nature or type of processing of their data, to avoid loopholes that would lead to unfair and illegal processing of personal data.	The first part of Regulation 4 does not require a controller to specify the type of processing that the DC will process data. e.g as stipulated under Section 2 of the Data Protection Act on the definition of processing. In many instances, information is collected from people and the key aspects are not shared with the data subject. It is important for data controllers and processors to disclose this information as a matter of course.
Regulation 4(4)	A data subject may prior to the processing of their personal data give consent either orally or in writing, and may include a handwritten signature, an oral statement, or use of an electronic or other medium to signify agreement.	We propose that for sensitive personal data, the consent given must be explicit and in writing.	The threshold for consent for sensitive personal data should be higher than that of general personal data. Consent should not be the only lawful basis for processing, where there is a clear imbalance of power between the parties e.g in employment and processing by a public authority. In the EU, in employment and processing by

			public authorities, the legal basis is consent and legitimate interest or public interest etc. *Recital 43- GDPR
Regulation 5	The collection of personal data entails obtaining personal data directly from a data subject or by any means, including from— (e) biometric technology, such as voice or facial recognition.	The regulation should be expanded to require that before such processing a DPIA should be conducted. Further, any person collecting such sensitive information should be subject to higher protection thresholds.	Such collection is a form of processing as defined under Section 2 of the Data Protection Act, which may result in high risk..
Regulation 7	(5) Where right to object is not absolute in circumstances contemplated under paragraph (4) (b), the data subject shall demonstrate— (a) compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or (b) the processing is for the establishment, exercise or defence of a legal claim.	Substitute the phrase "data subject" in 4(b) with "Data Controller or Data Processor." The regulations should require that a Legitimate Interest Assessment be conducted before the data processor or controller overrides the interests of a data subject.	The first part corrects a typographic error. Data processors and controllers should be required to conduct a Legitimate Interest Assessment to show a record of such legitimate interests and the reasons for overriding the data subjects rights, before making the decision.
Regulation 9 (2) Rule 8	(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	The regulation should be expanded to enable lodging of a request electronically especially where companies collect data	As a general rule, data subjects should easily and quickly have access to means through which to rectify their data without any limitations.

	is untrue, inaccurate, outdated, incomplete or misleading. (2) A request for rectification may be made in Form 4 set out in the First Schedule. (3) An application for rectification of personal data may be supported by the necessary documents relevant to the rectification being sought. (5)Where a request for rectification is declined, a data controller or data processor shall notify a data subject of that refusal and provide reasons.	electronically. The forms should be limited and where possible indicate the minimum information required to effect the change. There should be an obligation on data processors or controllers to provide simple and effective means to facilitate this process. The Regulation should provide a time frame of say 14 days, to communicate the refusal to a data subject.	Otherwise documents may be rejected for want of form. This is drawn from best practices as seen in the EU-GDPR that advocates for this method of lodging a request. Section 40 stipulates that such communication should be made within a reasonable time. This is ambiguous and may be used to the detriment of data subjects. If, for any reason, legal or technical, that the communication cannot be made within this time period, the same should be communicated to the data subject within 14 days.
Regulation 11 (2)	A data subject may request for erasure of their personal data held by a data controller or data processor in Form 5 set out in the First Schedule.	This can be rephrased to allow deletion of data electronically without having to fill a form. The forms should be limited and where possible indicate the minimum information required to effect the change. The regulations should also add a regulation on the right to be forgotten. “A data subject should have the right to their personal data rectified or erased where the retention of such data subjects rights under the DPA”	Forms are bureaucratic and should be limited where possible, and the minimum information required be specified. Otherwise documents may be rejected for want of form. Review the provisions on the right to be forgotten as seen in the EU GDPR. Data controllers and Data processors should be obligated to ensure they have appropriate mechanisms, including technology to facilitate this.

Regulation 12	(1) Subject to section 27 of the Act, where a person duly authorized by a data subject seeks to exercise the rights on their behalf, the data controller or data processor shall consider the best interests of the data subject. (2) In relation to processing personal data relating to 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 there is doubt as to the existence of a relationship between the duly authorized person and a data subject, the data controller or data processor may halt the request of exercising a right on behalf of the data subject until evidence to the contrary is adduced	There should be a higher standard for the use of children's data for commercial purposes. Data controllers or processors intended to use children data, should justify how the intended use is in the best interests of the child irrespective of any business model or commercial interests of the organisation. The ODPC should come up with appropriate guidelines regarding handling of children's data. The regulation should require data controllers and processors to come up with appropriate age verification mechanisms. Where the target subject is a minor the data controller should use language that the data subject can understand in their contracts.	There is a need for a robust data protection framework when it comes to the data of children. Although direct marketing is prohibited, the nature of some applications, especially social media ones, directly market to children without providing a proper mechanism for opting out. The rules need to be clear when it comes to a child's data. In addition, companies may need to set up proper mechanisms to show consent was obtained from the guardians before children's data was collected or processed. Further, that the children understood how their data will be being used as they are the data subjects. The language used by data controllers needs to be one that the guardians can understand. Review the best practice emanating from legislation and case law emanating from Ghana, USA, UK and Ireland. The ODPC can borrow a leaf from the Data Protection Commission Office of Ireland that published guidelines for the processing and commercialization of Children's Data. The use of the term "May" in ss.3 means that the DC has an option to stop and not honour the request or continue whether sufficient evidence has been adduced or not.

Regulation 13	Pursuant to section 37 of the Act, a data controller or data processor shall be deemed to use personal data for commercial purposes where the data controller or data processor — (a) sends a catalogue through any medium addressed to a data subject; (b) displays an advertisement on an online media site a data subject is logged on using their personal data, including data collected by cookies, relating to a website the data subject has viewed; or (c) sends 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. (2) Marketing is not direct, if personal data is not used or disclosed to identify or target particular recipients.	Provide a complete definition of terms such as 'direct marketing' and 'commercial purposes'. Define the phrase "online personal identifiers" to include cookies, IP addresses, radio frequency identification tags, metadata etc. Use broad terminology so as not to be restrictive with technology changes. Data subjects should be provided with fair processing information explaining how their data will be used for direct marketing.	There is no definition of direct marketing. The wording of (2) may be inferred to be the definition, premised on targeting as the sole determinant of direct marketing. No definition of commercial purposes. Direct marketing messages do not need to offer something for sale. It may include information sent for information purposes only e.g status of an order etc. The above are included in the GDPR Article 4(1) and Recital 30. From "Article 29 Data Protection Working Party, WP It was noted that the definition of direct marketing is broad. Direct marketing also involves digital and non-digital marketing. In this case, does the wording of Regulation 13 include non-digital marketing e.g SMS, telemarketing etc. On (b) the wording used may be interpreted to only cookies and personal data defined under the Act.

			Also, assuming that the Act is technology neutral, the wording should not be specific so as to encompass changes in the tech that may result in creation of personal data. E.g Apple's move from IDFA to its own SKAd Network or Google's intention to move from using cookies to the Federated Learning of Cohorts, or FLoC. It uses an algorithm to look at your browser history and place you in a group of people with similar browsing histories so that advertisers can target you.
Regulation 16	In each direct marketing communication with the data subject, a data controller or data processor shall include a prominent statement, or otherwise draw the data subject's attention 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 can opt out of receiving future messages by replying with a single word instruction in the subject line;	This should be amended to state that a data controller obtains an explicit **opt-in** consent from the data subject. Also, that the data subject has a right to **opt out** or withdraw this consent anytime.	The reading of this regulation is that the information on opting out of direct marketing is included with the information on marketing. Further, the practice is to provide for opt in requests and not opt out. This has been regarded as best practice internationally and the ODPC should adopt the same requirement under the regulations. The information on opting out should be separate from the content in a clear and legible manner.

	b) ensuring that a link is prominently located in the email, which takes a data subject to a subscription control centre; c) clearly indicating that a data subject can opt out of future direct marketing by replying to a direct marketing text message with a single word instruction; d) informing the recipient of a direct marketing phone call that they can verbally opt out from any future calls; and e) including instructions on how to opt out from future direct marketing, in each message. f) 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 paragraph (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.		
Regulation 7	(1) A data subject may request a data controller or data processor not to use or disclose personal data about the data subject for the purpose of facilitating direct marketing by a third party.	The regulation should provide that, as a general rule, the personal data of a data Subject shall not be disclosed without the express consent of a data subject. The Regulation should provide that in the event of disclosing data to third parties, the consent of the data subject should be obtained and they be provided with information on the third party to whom such personal data has been disclosed to. The regulations should provide that the third party has obligations to data subjects e.g information obligations etc.	The wording of this regulation implies that where such express request has not been made then the personal data will be shared.
Regulation 21	(1) In this regulation	The regulations should adopt the general rule that has been set by the GDPR quoted below:	Before such processing, the data subjects' consent should be obtained.

	"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 making automated decisions shall— (a)inform a data subject when engaging in an automated processing; (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) if 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;	"The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." [Article 22(1)] Given the extreme repercussions of such decision making, such processing should only be allowed: a) With the explicit consent of the data subject. b) Where it is necessary for entering into or performance of a contract c) Where it is authorised by law. For sensitive personal data, such processing should only be allowed where there is explicit consent and the processing is necessarily of substantial public interest. Also, a DPIA should be mandatory as opposed to optional.	The wording under this regulation does not require consent but allows such processing as long as the data subject has been informed of such processing. Also, a DPIA should be mandatory as opposed to optional because it may be difficult to ascertain risk before automated decision making. At this point a Data Controller or Processor may choose not to conduct a DPIA since when they began, the processing was not high risk

	(e)ensure the prevention of errors, bias and discrimination; (f)use appropriate mathematical or statistical procedures; (g) put appropriate technical and organizational measures in place to correct inaccuracies and minimize the risk of errors; (h) process personal data in a way that prevents discriminatory effects; and (i) ensure that a data subject can obtain human intervention and express their point of view.		
Regulation 25	(1) Pursuant to section 50 of the Act, a data controller or data processor who processes personal data for the purpose of actualising a public good set out under paragraph (2) shall be required to ensure that— (a) such processing is effected through a server and data centre located in Kenya; and (b) at least one serving copy of the concerned personal data is stored in a data centre located in Kenya.	Instead of a blanket ban on transfer of data it should be weighed on a case by case basis, depending on how much data is being collected and how data centric is the entity collecting the data. We also recommend removal of restrictions such as Regulation 25 (2) on facilitating access to primary and secondary education in Kenya (c)	The restriction of processing some personal data to Kenya may act as an impediment to the growth of the IT and ICT sector. For example, in the education sector some data controllers may process and store the data in cloud servers not located in Kenya. It may also raise the cost of setting up and running a business in these areas in which transfer of data is restricted. The exemptions should be analyzed again.

	(2) The purpose contemplated under paragraph (1) that require processing in Kenya includes— (a) administering a national civil registration system including registrations of births and deaths, persons, adoption and marriages; (b) operating a population register and identity management system including any issuance of any public document of identity; (c) managing personal data to facilitate access of primary and secondary education in the country; (d) the conduct of elections in the country; (e) managing any electronic payments systems licensed under the National Payment Systems Act; (f) any revenue administration system for public finances; (g) processing health data for any other purpose other than providing health care directly to a data subject; or (h) managing any system designated as a protected computer system in terms of		The list may lock out other data controllers who, depending on the nature of their business, should be on the list but are not. In addition, according to the African Union Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019, States shall not adopt laws or other measures prohibiting or weakening encryption, including backdoors, key escrows and **data localisation requirements**, unless such measures are justifiable and compatible with international human rights law and standards.

	section 20 of the Computer Misuse and Cybercrime Act, 2018		
Regulation 41	For the purpose of confirming the existence of appropriate data protection safeguards anticipated under section 49 (1) of the Act, 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) reciprocal data protection agreement with Kenya; (c) an adequate data protection law as shall be determined by the Data Commissioner.	Kenya should ratify the African Union Convention on Cyber Security and Personal Data Protection. The threshold for an adequate data protection law be clearly stated. Consider the wording under GDPR Article 45 to determine adequacy.	Kenya has not ratified the African Union Convention on Cyber Security and Personal Data Protection. On (c) it is not clear from the regulations what an adequate data protection law is. Further, it is not clear how the ODPC will determine adequacy.
Regulation 46	(1) For the purposes of section 51(2) (b) of the Act, the processing of personal data by a national security organ mentioned in Article 239 (1) of the Constitution in furtherance of their mandate constitutes a processing for national security (2) Despite paragraph (1), a data controller or data processor who processes personal data for national security and wishes to be exempt on that ground shall	Delete the provision and the blanket exemptions for national security from all provisions of the regulations. Exemptions should be for very specific aspects and grounds, with the application made to the ODPC, and not the Cabinet Secretary. Consider best practice in the United Kingdom that has taken a similar approach with their Data Protection Act.	The term sufficient grounds can easily be interpreted to justify any exemption under the guise of National Security. The discretion of granting an exemption is left to the Cabinet Secretary. It is not clear why or where the CS gets powers to grant exemptions given that Section 51 of the Act does not state who should make these exemptions.

	apply to the Cabinet Secretary for an exemption. (3) The Cabinet Secretary shall, upon being satisfied that 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 it was issued no longer apply.	Further guidelines should be drafted on what will constitute sufficient grounds under national security to provide these exemptions. A standard form should also be drafted for application of the exemption and a certificate granted to the data controller or processor to indicate this exemption.	Section 54 of the Act is clear that the ODPC may prescribe instances where compliance with certain provisions of the Act may be given. Therefore, the duty of granting exemptions lies with the ODPC, and not the Cabinet Secretary. In addition, Principle 41 of the African Union Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019 declares that States shall not engage in or condone acts of indiscriminate and untargeted collection, storage, analysis or sharing of a person's communications. However, this blanket exemption will violate this principle.
Regulation 47 (2) and 49	A permitted health situation mentioned under regulation 41 (b) exists in relation 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;	Regulation 47 (2) and 49 need to be deleted altogether given that health data is classified as sensitive. The only exemptions that should be there when it comes to health data is the refusal to disclose the data, which is already provided for in the regulations. There is a need for detailed regulation focusing on health data including how such data can be used during a pandemic as COVID-19.	Under the DPA, health data is classified as sensitive data and providing an exemption to such data may result in abuse and misuse of health data. This may lead to health care providers not having appropriate mechanisms to ensure the data they are given is used safely and used appropriately. Further, some health data for example one's HIV status may cause stigma if the data is leaked and the data subject may not have any recourse given that the health care provider is exempted from these rules.

	(c) the use or disclosure of genetic information if 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 paragraph (1) applies when 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 career is aware or of which the career 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		

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

Clause	Provision	Proposal	Issue and Justification
Preamble	IN EXERCISE of the powers conferred by section 18 (2) of the Data Protection Act, 2019, the Data Commissioner makes the following Regulations—	Replace the word "Data Commissioner" with "Cabinet Secretary for Information, Communication, Technology, Innovation and Youth Affairs".	Section 18(2) of the Data Protection Act, 2019 does not confer powers on the Data Commissioner to make regulations. It provides that the Commissioner "shall prescribe thresholds" as such, not law making power. Likewise, it offends the principle of separation of powers, as the enforcer of laws, cannot purport to make laws they are to enforce. Section 71(1) of the Data Protection Act, 2019 is specific that the power to make regulations generally for giving effect to this Act, and for prescribing anything required or necessary to be prescribed by or under the Act lies with the Cabinet Secretary.
Regulation 3	(1) These Regulations shall 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.	The Regulation should adopt a notification system as opposed to a rigorous and bureaucratic registration process. Delete clause 3(2) entirely.	The registration process should be simple, seamless and swift. The Regulation cannot purport to exempt what the Data Protection Act has not exempted. Section 51(1) of the Data Protection Act provides that "Nothing in this Part shall exempt any data controller or data processor from complying with data protection principles relating to lawful

			processing, minimisation of collection, data quality, and adopting security safeguards to protect personal data".
Regulation 4	(1) For purposes of the Act, a person shall register as a— (a) data controller, if that person determines the purpose and means for processing personal data; or (b) data processor, if that 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 manner in which processing of personal data and the purpose in which the personal data shall be used. (2) Despite paragraph (1) (a), a data controller may apply for registration as both a data controller and a data processor with regards to any processing operations.	Amend and redraft the entire provision. We propose that the focus should be on Data Economy Player instead of focusing on the number of employees an entity has, i.e. how data driven an entity is. This is the same approach taken by the GDPR which does not require the registration of data controllers and processors but depending on how data driven the entity is the more stringent the rules apply. Provide clarity on the exclusion under this regulation. For an organisation registering as both a Data Controller and Data Processor, the amount of fees payable should be lower as opposed to double, since the organisation would be making an individual application for both.	This provision is not clear in terms of what the objective under section 18(2) of the Data Protection Act, and the criteria is and shall open the door for confusion in implementation. These regulations appear to have borrowed a leaf from the UK Data Protection (Charges and Information) Regulations 2018 which are almost similar to these proposed regulations. In subsequent paragraphs it appears that whoever qualifies to register to be a Data Controller or Processors has been interpreted to mean the number of employees one has and turnover but not the amount of data they handle or collect as a company and how data driven the entity is. This is seen in various instances such as the exemption from registration that provides if one has less than ten employees and an annual turnover of less than five million shillings (Regulation 9). The fees one is required to pay for registration is pegged on the number of employees and not the nature of business and

	Despite paragraph (1) (b), where a data processor processes personal data other than as instructed by the data controller, such a data processor shall be considered to be a data controller in respect of that processing activity.		amount of data collected. They are also pegged on annual turnover. Does the exclusion of employees mean exclusion of processing of the personal data of employees of the data controller? With respect to Regulation 4 (2) it may be interpreted to mean that the organisation is required to pay double the fees for such registration. It may also be interpreted to mean that in this circumstance there is no requirement for registration of a DP as a DC.
Regulation 8	Issue the applicant with a certificate of registration and may specify any conditions thereof; Certification fees: 250,000/=	The fees for certification should be lowered or removed altogether. The fees can be broken down into categories or tiers to take into account the relative size and ability of various organizations and the amount of data collected or processed by the organization. Clarity is needed as to whether the cost of renewal is the same as the initial certification.	The fees set for certification is exorbitant and does not take into account the relative size and ability of various organizations and the amount of data collected. In the United Kingdom, there are three tiers based on size and turnover with fees ranging from £40 and £2,900, but for most organisations the fee ranges from £40 to £60. Also, some organisations such as Charities and small occupational pension schemes only pay £40 regardless of their size and turnover.
Regulation 9	(1) A data controller or data processor shall display the certificate of registration	Regulation 9 (1) should be deleted and replaced with “the ODPC shall have a portal	This equates the certificate to be a trade license and one that must also be displayed along with a

	and any change of particulars of a certificate if any, at a conspicuous place at the principal place of business or on its official website and a certified copy of the certificate of registration for each branch, where applicable. (2) Despite paragraph (1), a data controller or data processor shall display such other information as the Data Commissioner may from time to time require. (3) The Data Commissioner may impose an administrative fine for a breach under this regulation, in accordance with section 63 of the Act and any Regulations enacted therefrom.	where one can view who is registered as a data controller or processor." This draws from best practices from the United Kingdom where one can view registered data controllers in the Information Commissioner's Office website which has a portal to enable data subjects to search for Data controllers.	trading license. The registration is enough and a portal can be established by the Office of the Data protection officer where one can just check if one is registered or not. Further, the regulation should recognise that some businesses do not have offices in Kenya and thus can not display such a certificate.
Regulation 5	Application Form (Form A) for renewal is similar to that of initial application	We recommend that the application Form for renewal of the certificate should be simpler and shortened unless processing activities have changed or the data being processed has changed which necessitates additional information. In which case, the renewal form should have an annexure to include these details.	In the case for renewal of the certificate, the ODPC already has all these details in record. Further it is not clear whether the Data Controller or Data Processor will have to pay the certificate fees every year of renewal or is this a one-off cost.

Regulation 10	Application Form (Form A) for renewal is similar to that of initial application	Abolish the renewal form. Renewal can also be done through an online portal in a simple, effective and transparent manner. For example, the NTSA portal.	A different form is needed for the renewal of the certificate. If the data controller or data processor is not making any significant changes to what they had shared with the OPDC when registering they should be allowed to easily renew their certificate. Further having to fill the form every time one is required to renew their certificate will lead to the OPDC having a lot of duplicate data that is unnecessary.
Regulation 11 (2)(b)	Lack of "appropriate safeguards" as a ground for refusal of renewal.	The term appropriate safeguards should be defined.	The term appropriate safeguards has not been defined under the Act or the Regulations. The issue with this is that DC and DPs will not be aware of what bare minimum standards are they required to achieve for them to be registered. Further the lack of a bare standards minimum may result to varying degrees of what is seen as appropriate safeguards
Regulation 12	(1) A data controller or a data processor— (a) whose annual turnover is below five million shillings or whose annual revenue is below five million shillings; and (b) who employs less than ten people, is exempt from the mandatory registration under these Regulations.	The criteria should focus on registration of data controllers and processors based not on the size of their organisation but on the nature of their activities. The schedule should quote the correct regulation. ie the third schedule has quoted regulation 10 instead of regulation 12	The criteria for registration of data controllers and processors is based on the United Kingdom criteria. Registration should focus on the nature of the activity of the business. In this case the nature of activities would be the volume of data processed per month or per year as criteria for being a Data Controller or Processor. With the current provision, everyone i.e. every employer may end up being classified as a data

	(2) The exemption provided under paragraph (1) shall not apply to a data controller or data processor whose annual turnover is below five million shillings and employs less than ten people, processing personal data for purposes specified under the Third Schedule. (3) For the avoidance of doubt, the data controllers and data processors contemplated under paragraph (2), shall be required to undertake mandatory registration in accordance with Part III of the Act and these Regulations.	We recommend that a provision be included in the third schedule where processing activities, by the data controller or processor, include processing of sensitive personal data.	controller or processor even if they are not a highly data driven company. For example, why would a carpenter who has an annual turnover of 10 million but with 10 employees require to be registered as a data processor or data controller. Third Schedule: quotes Regulation 10 instead of Regulation 12 The exceptions suggest that data controllers and processors processing sensitive personal data, falling within the threshold set, may be exempt as long as they fit within the required threshold.
Regulation 16	(1) The Data Commissioner may charge a fee— (a) for approval of Data Impact assessment provide under section 31 of the Act; (b) to provide a compliance support to any person; (c) to conduct a compliance audit;	Regulation 16 should state the prescribed fees charged for the services in a schedule and not be left to discretion. The regulation should be amended to provide a licensing framework to permit third parties licensed by the ODPC to conduct data impact assessments, as opposed to the ODPC.	Under the Data Protection Act Section 71 (e), it is the Cabinet Secretary who is tasked with coming up with levies and charges. Prescribing fees in regulations or legal notices ensures predictability and removes the discretion as in the current provision. A licensing framework approach similar to that in the Environment Management and Coordination Act, 2003 which permits third parties to conduct

	(d) facilitate a third party due diligence; and (e) facilitate inspection or search on the register.		environmental impact assessments could be considered. The ODPC does not have the capacity to conduct DPIA for all data collectors and processors.
Regulation 18	Replacing a lost certificate.	Delete provision. The certificate should be given in an electronic manner and one should not be penalised for losing the certificate	The Regulations should specify whether the cost of replacement is similar to that of application of a certificate. In addition, the mode of application for replacement should be stated clearly. The cost of replacement has not been specified under the schedules.
Regulation 20	Penalty on processing data beyond the scope registered. 20. (1) A person commits an offence if that person — (a) processes personal data outside their scope;	Deletion of Regulation 20	The DPA and in particular Part IV solely puts emphasis on the position of a data subject, principles, rights and obligations. This regulation implies that processing personal data should be at the permission of the ODPC and not by the consent of the data subject or in line with the legal basis laid out under the Data Protection Act. If the intention is to punish excesses of a data controller or processor, then there is already a

	(b) processes personal data for any purpose, other than the purpose for which they are registered to process;		general offence under the Act for the violation of any of its provisions.
First schedule Form A	One will be required to indicate where applicable if they have a data protection officer and who they are.	In line with principles of data minimisation we can restrict the data collected from Data controllers and Data Processors to: 1. Name 2. Address 3. Number of employees 4. Annual turnover The ODPC also needs to establish its independence; this calls for an amendment of the DPA Act to state that the OPDC shall be financed directly by parliament.	The regulations appear to have borrowed from the UK Data Protection (Charges and Information) Regulations 2018 which are almost similar to these proposed regulations. The amount of information that is being asked in the forms is a lot. For example: a. description of personal data to be processed (e.g. name, address, identification number etc.) b. category of data subjects (e.g. employee, client, students, supplier, shareholder, etc.) c. purpose of processing (e.g. for payroll, invoicing, know your customer (kyc), registration, etc.) recipient (s) d. to whom personal data is (are) disclosed (e.g. kra, cbk They will also be collecting data on: a. Identify risks to personal data (E.g. unauthorized access/disclosure, theft, etc.)

			b. Safeguards, security measures and mechanisms implemented to protect personal data This raises the issue of if it is appropriate to a certain extent for the government to have all this data on business entities. Will the OPDC have appropriate safeguards to ensure that this data is only used by the office of the Data protection officer and that it will not be misused or shared with other agencies under the guise of national security.
Second schedule: fees charged by office of the office	The wording of the title is wrong The regulations propose a raft of fees that may further escalate the cost of doing business in Kenya. These are: 1. Base payment (all data controllers and processors unless exempted) ranging from Ksh. 1,000 to Ksh. 12,000 2. Annual Turnover (excludes public authorities and charities) ranging from Ksh. 1,000 to Ksh. 20,000	Revise the title from the current "SECOND SCHEDULE FEES CHARGED BY OFFICE OF THE OFFICE" to "SECOND SCHEDULE FEES CHARGED BY THE ODPC" Shelve the Certification Option until 4-5years when the industry has matured. Promote qualifications and skill sets for DPOs - particularly in high volume data companies - to create a culture of compliance that Certification may have intended to have. Abolish the certification fees.	Should the ODPC 'Certify' Data Controllers & Processors as being compliant, then the ability of the ODPC to adjudicate complaints against those organisations so certified may be complicated. Whereas the Certification exercise could be outsourced, it may be too early in the industry to focus on Certifications since it may be counterproductive as companies begin to pay and demand to be certified - when really most do not have capacity /DPOs etc.

	3. Special Category Data Charge (Personal Data intensive sectors)/ Risk exposure Ksh. 20,000 In addition, given that this is a regulation it is important that specific fees are given for certain matters and not left to chance. Therefore, a proper fees of fee scale needs to be provided for 1. Compliance support fee 2. Audit fee 3. Third party Due Diligence fee Certification fee of KES 250,000	State what sectors may be deemed "Personal Data Intensive Sectors"	
Third Schedule (R. 10): Thresholds for Mandatory Registration	A data controller or data processor processing personal data following purposes shall register as a data controller or a data processor as provided for under these Regulations—	Refinement of schedule three in general.	In general, the challenge with providing a list, any list, is that whoever is NOT on the list will find a way to escape responsibility/liability. It may be better to list but have a clause that describes other potential candidates NOT currently listed**.** The approach the regulations adopt to warrant or require registration should be based on the risk level, the nature of the data collected, and the method of processing. The regulations should therefore provide a threshold and a criteria for registration, as opposed to a listing of the sectors

			as provided in the schedule 3. If any listing should be done, it should be of those sectors that pose the highest risk to personal data, given the amount of data they collect, process and store. This would have been informed by a proper situational risk assessment of data management practices in the country in the various sectors.

THE DATA PROTECTION (COMPLIANCE AND ENFORCEMENT) REGULATIONS, 2021

Clause	Provision	Proposal	Justification
Preamble	IN EXERCISE of the powers conferred by section 31, 54, and 61 of the Data Protection Act, 2019, the Data Commissioner makes the following Regulations—	Replace the word "Data Commissioner" with "Cabinet Secretary for Information, Communication, Technology, Innovation and Youth Affairs".	Section 31, 54 and 61 of the Data Protection Act, 2019 do not confer powers on the Data Commissioner to make regulations. It provides that the Commissioner shall "shall prescribe thresholds. This is not in our view a law making power. Likewise, it offends the principle of separation of powers, as the enforcer of laws, cannot purport to make laws they are to enforce. Section 71(1) of the Data Protection Act, 2019 is specific that the power to "make regulations generally for giving effect to this Act, and for prescribing anything required or necessary to be prescribed by or under the Act lies with the Cabinet Secretary.
General Comment		The regulation may need to have a requirement that an entity that is not located in Kenya should have a representative to enable compliance with the Act and regulation.	Section 4 of the Data Protection Act states that the DPA and by extension its regulations shall apply to data controllers and data processors where the Act shall apply to the processing of personal data by a data controller or data processor who a. is established or ordinarily resident in Kenya and processes personal data while in Kenya; or

			b. not established or ordinarily resident in Kenya, but processing personal data of data subjects located in Kenya. Enforcing the regulations may prove to be a challenge where the data controllers and processors are not located in Kenya. This is because the contracts that Kenyan citizens get into in order to access these services are governed by the laws that are most favorable to the data controller or processors e.g. the United States and the place of dispute resolution is normally the USA. Also, most of the alternative dispute resolution mechanisms provided by the Regulations under Rule 14 viz negotiation, mediation and conciliation are governed by the laws of the country in which the data controller and data processor indicate in their contracts.
General Comment		The Regulations should provide a timeframe in which entities should comply with the regulation.	It is important that the regulation provide a timeframe for compliance, and for clarity.
Regulation 4	Regulation 4: Lodging a complaint (c): online by email,	We recommend the use of alternative modes of lodging complaints e.g written complaint.	Due to advancements in technology, there should be alternative ways of lodging complaints such as using an SMS or phone

	web posting, complaint management information system; d) by appropriate electronic means	A DPIA be conducted to ascertain the risk level of data subjects lodging complaints using the Complaints Management Information System. The ODPC put in place a privacy policy on how the personal data of data subjects, in this case, will be processed with respect to dealing with complaints. We recommend the use of phone calls or SMS USSD code to make this system simpler for the "common mwananchi".	calls. This will take into consideration those who can not write but can talk. Also, for this regulation to be fully complied with, in the best interest of data subjects, the Complaint Management Information System should be put in place as soon as possible. Its mode of construction should adhere to the provisions of Sec 41 of the Data Protection Act on data protection by design and default.
Regulation 6	Declining to admit a complaint	The ODPC should admit and respond to each complaint made. The grounds under rule 6(3) should only apply upon consideration of the merits of the complaint.	The ODPC is an oversight body to ensure checks and balances. Anyone aggrieved by its decision should have a right to appeal to the High Court in line with international principles i.e Article 7 of the African Charter on Human and People's Rights.
Regulation 11	Section 57 read together with Regulation 11: Upon admission of a complaint, the Office shall notify the respondent in Form 4 set out in the Schedule and require the respondent within fourteen days to— make	There is a need to make sure that the regulations are in harmony with other existing legislations to avoid a conflict of laws.	The ODPC requires the provision of evidence which may be limited by the provisions of the Access to Information Act Kenya Section 6.

	representations and provide any relevant material or evidence in support of its representations; Regulation 12- Requirement to produce evidence.		
Regulation 14 (1)	Where the complaint is to be determined through negotiations, mediation or conciliation, the provisions of these Regulations shall apply.	The regulations should include in Arbitration.	The regulation has not factored in Arbitration. This is because arbitration is also a recognised form of dispute resolution relied on by data controllers and processors rely on arbitration to resolve disputes.
Regulation 16(1)	Service of enforcement notice: it is deemed to be duly served if: an electronic copy of enforcement notice is sent through the concerned person's registered email address;	We recommend addition of modes of service premised on The Civil Procedure (Amendment) Rules, 2020 (the "Amendment Rules"), published on 26 February 2020 which provides for alternative modes of service including: Courier Service Providers, Service by mobile-enabled messaging etc.	The proposed modes of service are limiting.
Regulation 16(2)	The enforcement notice shall take effect from the date of service contemplated under paragraph (1)	This provision is ambiguous given the new modes of service, different time zones etc. The notice should take effect on the date it is issued and give a timeframe for compliance.	it is not clear what the "date contemplated" means. This opens it up to various interpretations. Such notices should give a reasonable period for compliance.

Regulation 15 **Regulation 16(2)** **Regulation 17(2)** **FORM 7: clause E**	Section 58: Where the Data Commissioner is satisfied that a person has failed, or is failing, to comply with any provision of this Act, the Data Commissioner may serve an enforcement notice on that person requiring that person to take such steps and within such period as may be specified in the notice. 2(c) specify a period which shall not be less than twenty-one days within which those measures shall be implemented;	The provision should state clearly the time required under the notice and amend the stipulation in Form 7.	The time period enumerated here seems to be varying or on a case-to-case basis but not less than 21 days as stated under section 58 (2)(c), while the form states 30 days and 4 days. The ODPC should clarify the timelines stated across the board to avoid inconsistency of application and contradictions in the provisions.
Form 1: Part 12	The Data Commissioner treats all complaints confidentially. However, the investigation of your complaint may require disclosing your identity and the allegations you made to the institution against which you complained and, if necessary, for the investigation, to the third parties involved, including other	Adopt whistleblowing guidelines and protections for those lodging complaints as whistleblowers.	This defeats the purpose of whistle blowing as it puts a burden on whistleblowers to explain themselves on why they are whistleblowers and secondly, to state the kind of protection they seek. Review the European Data Protection Supervisor Guidelines on processing personal information within a whistle blowing context.

	national regulatory authorities where relevant. Do you accept this standard confidential treatment of your complaint? If not and you wish to remain anonymous to the institution concerned, to the relevant DPO or to third parties, please explain the reasons for your request. Please also explain which additional safeguards you would like us to take. We will consider how far we can implement these requests and will keep you informed. *		
Form 7	Enforcement Notice in Terms of Section 58 Of The Data Protection Act, 2019	Have a blank section under Part A of the form since the list of violations thereunder are not exhaustive, to allow the ODPC discretion to list any violation of the Data Protection Act or regulations thereunder that have not been complied with.	The data subject should be at the center of these regulations. The list of violated rights of the data subject are very limited. They should be expanded to include the Data Subject Rights as provided for by Part IV (Principles and Obligations of Personal Data Protection under the Data Protection Act. The forms should focus on ensuring they are geared towards protecting the rights of the data subject in this case by expanding the list of violated rights in the form, to factor in the

			breaches related to Data Protection Principles.
General Comment	Detail of the Forms	Simplify the forms to only have the key information necessary to achieve the desired effect. The forms should at most be 1-2 pages long.	The forms are quite detailed, extensively long and could easily become quite burdensome to fill and bureaucratic.