Ministry of Information, Communications and Telecommunication
Telposta Towers, Kenyatta Ave. Koinange Street
P.O Box 30025-00100 Nairobi Kenya

Sent via email to dataprotectionregulations@odpc.go.ke

Attention: Hon. Joe Mucheru, EGH

11 May 2021

Dear Sir

Subject: Submissions on the Data Protection (General) Regulations 2021, Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021 and the Data Protection (Compliance and Enforcement) Regulations, 2021

Pursuant to the Public Notice released by the Cabinet Secretary of the Ministry of ICT, Innovation and Youth Affairs on 13 April 2021, and Article 118 (*Public Participation*) of the Constitution of Kenya, 2010, we, the American Chamber of Commerce, Kenya ("**AmCham**", "**We**"), are glad to submit the proposals below with regards to the draft 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 (together the "**Draft Regulations**").

The American Chamber of Commerce, Kenya is a membership organization with a diverse membership spanning multinationals, corporates, local SME's and not for profit organizations. Our members operate in various sectors including technology, oil and gas, renewable energy, manufacturing, infrastructure, healthcare and communication. We ensure that our members drive industry innovation and are at the heart of policy discussions affecting business.

We appreciate this opportunity to submit our proposals on how to enact the Draft Regulations in a manner that nurtures the growth of the Kenyan data protection environment. While protecting the data of Kenyan citizens is a necessary objective, the current Draft Regulations raise concerns about efficacy, feasibility and economic realities. Disrupting cross border flow of data and requiring annual registrations based on turnover has a serious detrimental impact on the economy and we hope that our proposal gives the Ministry a realistic account of our members views, to enable the Ministry to understand the economic impacts of the Draft Regulations as currently drafted.

Should you wish to discuss the contents of this letter, please do not hesitate to contact me on +254 733 787 416, Maxwell@amcham.co.ke at your convenience.

Yours faithfully,

Maxwell Okello
Chief Executive Officer

CC. Office of the Data Protection Commissioner
Taskforce on the Development of the Data Protection Regulations
30920 Waiyaki Way, Westlands, Nairobi, Kenya

Contents

Executive Summary of Key Issues

In order to attain the full benefits of the Draft Regulations, AmCham requests that the Ministry considers the following issues and proposed solutions. These will be explored more in depth in the analysis tables that follow this executive summary.

a. Adequacy of Cross Border Data Flows

i. Data processors or controllers who transfer personal data beyond Kenya's jurisdiction are prohibited from doing so unless the recipient country or territory is found to have compatible and comparable legal requirements. There is a need for immediate and clear advisory on the territories which meet adequacy requirements. There are no reciprocal data sharing agreements entered into as yet and the Regulations do not provide a framework to achieve reciprocity. We recommend that the ODPC establishes a reciprocity framework.

ii. The Draft Regulations impose obligations on entities who transmit data via Kenya but are not domiciled in-country and do not process personal data of data subjects in Kenya, and hence fall beyond the ambit of the Act. The definition of transferring entities should be amended to only affect entities resident in Kenya or entities processing the data of data subjects located in Kenya as per section 4 of the Data Protection Act, 2019.

iii. Appropriate safeguards should apply to transfers of ***all personal data*** and not exclusively to sensitive personal data. Thus, the ODPC needs to rectify contradictions between Regulation 41 and section 49 of the Data Protection Act, 2019.

iv. ODPC should provide further guidance on the transfers of personal data between group undertakings or enterprises in different jurisdictions. The mechanism to deal with such intra-group transfers in the European Union under the GDPR are Binding Corporate Rules approved by each relevant Regulatory Authority. ODPC should confirm if such arrangements will be allowed under the Act and General Regulations.

b. Data Localization

i. The Regulation should be re-drafted to provide a clearer list of activities that require local data server processing.

ii. The Regulations should focus on those activities that are of a public sector nature to avoid imposing an unduly onerous compliance burden on private sector entities.

iii. The Regulation goes beyond the limits of the Act by referring to "the purpose of actualizing a public good". This is wider than the specific grounds prescribed under section 50 of the Act which were limited to grounds of "strategic interests of the state or protection of revenue".

iv. The Cabinet Secretary may require a data controller who processes personal data outside Kenya to effect such processing via a server and data center located in Kenya in the event of a breach or failure to cooperate with the Data Commissioner. This Regulation fails to consider the difficulty involved in setting up a local delivery center with support staff and migrating customer data. This also raises grave concerns about how this would impact service availability in the event of such a forced localization. The Cabinet Secretary, prior

to exercising powers under Regulation 25, should be forced to consult with the data controller and processor on the same.

c. Registration of Data Controllers and Processors

i. The requirement to apply for renewal of registration annually imposes a significant compliance burden on data controllers, data processors and the ODPC. We propose an evergreen registration that is paid for annually (similar to the banking license issued by CBK).
ii. The third schedule of the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021 classifies data controllers and processors that must register due to the nature of their industry regardless of the turnover. This should be the primary criteria for registration.
iii. A notification of change should only be required for material changes (as specified by the ODPC).
iv. The ODPC should create an online portal for easier administration of applications, renewals and change notifications.
i. ODPC should reduce the fees for DPIA assessment significantly in order to reduce the costs of compliance for controllers and processors.
ii. Certification should be done by an independent third party.
iii. No fees should apply to compliance support and service provision as these are the responsibility of the ODPC.
iv. To avoid duplication of applications, only data controllers should be required to register with the Data Commissioner, as their applications requires them to disclose their processors.

d. Breach Notification

i. Under Schedule 2 of the Data Protection General Regulations, the categories of personal that would automatically amount to a notifiable data breach are very broad. The "risk of harm to a data subject" may vary depending on the nature of the specific circumstances. Data controllers should be granted appropriate time to determine the nature and extent of the breach and the potential risk of harm to the data subject and only notify the ODPC and the data subject in the event that there is a real risk of harm to the data subject.

e. Existing Gaps

The following matters should also be expounded under the Regulations as they are currently not addressed:

i. The roles, responsibilities, and training for Data Protection Officers;
ii. The data controllers and processors that need to appoint DPO's based on the registration thresholds;
iii. Safeguards to be applied during data processing activities relating to children and persons with disabilities; and
iv. Further clarification of the exemption criteria for the following types of processing: journalism, literature, art, scholarly research, history, data collection for statistics and household activities.

f. Privacy Accountability Frameworks

i. There is a need to encourage the use of privacy accountability frameworks within organizations whereby internal privacy management activities are set and continuously improved over time. This results in industry self-regulation and higher levels of accountability.

ii. The multiple forms in the Draft Regulations do not comply with the principles of data minimization. The ODPC should not be prescriptive and should simply set out minimum requirements for forms to be used by data controllers and processors. These can then be formulated by each data controller and processor based on the industry and the nature of the data collected.

iii. Need to omit or delete requirements to implement principle of accuracy, with specific regard to Regulation 33 (c). Burdensome process for data controllers and data subjects.

iv. Data controllers and processors should not be precluded from using their own templates and tools to conduct and document DPIAs, provided that the DPIAs meets the minimum requirements of the Regulations. Many organizations have developed extensive multi-jurisdictional processes for responding to data subject requests as well as for engaging in DPIAs. Requiring the use of a Kenya-specific form or template will create significant compliance burdens without any measurable increase in privacy protections.

g. Controllers v processors

i. The Regulations have been drafted to apply to data controls and processors alike. However, under the Act, data processors process personal data on behalf of data controllers and do not determine the purpose and means of processing personal data. ODPC should revisit all clauses where obligations are placed jointly on data controllers and processors and clearly distinguish between obligations on the data controller and processor.

ii. Suggest to change "without prior specific or general written authorisation of the controller". In case of general written authorisation, the data processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

h. Ambiguity

i. Processing operations taken to constitute high risks and require DPIA's are ambiguous. ODPC should reconsider wording of entire Regulation relating to activities that require DPIA's and include definitions where necessary (e.g. financial and reputational benefit).

ii. The suggested timeframes for responding to data subject requests by the ODPC lack consistency. A general rule should be applied.

iii. Neither of the terms "Commercial Purposes" or "Direct marketing" are defined in the Data Protection Act, 2019 or the Draft Regulations. The two terms appear to be used interchangeably, yet they are not synonymous. The plain meaning of "commercial purposes" is broader than "direct marketing". If the policy objective is to restrict "direct marketing" activities (as with GDPR), then that is the specific term that should be used to avoid ambiguity as to what other activities might be restricted.

i. Consent

iii. Avoid consent obligation and collection in case of new purposes. This should be changed into an obligation to inform, in line with article 14(4) GDPR:

"Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further

processing with information on that other purpose and with any relevant further information as referred to in this regulation."

iv. Regarding regulation (4), there is a need to expand the scope and legal basis of consent. The latter can be achieved through greater alignment with consent provisions stipulated in GDPR e.g. processing shall be lawful only if and to the extent that at least one of the following applies:

- Processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering a contract.
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, where the data subject is a child.

Detailed Table of Issues

Data Protection (General) Regulations 2021

#	Regulation	Issue	Recommendation
Adequacy of Cross Border Data Flows (CBDFs)			
1	Deeming of appropriate safeguards 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.*	1. Section 49 of the DPA deals with the transfer of sensitive personal data outside of Kenya. By linking Regulation 41 to Section 49 of the Act, this implies that Regulation 41 will only apply to the cross-border transfer of sensitive personal data. 2. Apart from reference to the AU Convention, the ODPC has not provided any guidance on what territories meet adequacy requirements even though the DPA has been operational for two years. We also note that the Convention is not currently operative as the minimum number of AU members required to ratify it and bring it into force (15) has not been achieved. We further note that Kenya is one of the countries that is yet to ratify the Convention. 3. ODPC has not provided guidance on the transfers of personal data between group undertakings or enterprises in different jurisdictions. The mechanism to deal with such intra-group transfers in the EU under the GDPR are Binding Corporate Rules (BCRs).	1. It should be clear that safeguards need to be in place for the cross-border transfer of all categories of personal data. 2. Guidelines on territories which meet adequacy requirements to be published by the ODPC at the earliest convenience 3. The AU Convention should not be hard-wired into the regulations as an adequacy criterion. We recommend that be treated as an internal policy consideration for the ODPC when determining adequacy (in the same way that ODPC would consider a GDPR jurisdiction). 4. ODPC should confirm if BCRs will be allowed under the Act and Regulations. 5. We recommend that the ODPC establishes a reciprocity framework immediately. The APEC (Asia Pacific Economic Cooperation) Cross Border Privacy Rules (CBPR) system offers a model as a government-backed certification. The principle-based privacy framework is endorsed by the APEC economies to facilitate and encourage cross-border data flow in the context of privacy. This model would be particularly suited to the

#	Regulation	Issue	Recommendation
		4. There are no reciprocal data sharing agreements entered into as yet and the Regulations do not provide a framework to achieve reciprocity.	African context and ongoing efforts to harmonize ICT regulations across the continent.
2	Regulation 37 Interpretations *"transferring entity" —* *(ii) in relation to data in transit, means the entity that transfers the personal data through Kenya to the country or territory outside Kenya.*	Regulation 37 imposes obligations on transferring entities not resident in Kenya and who do not process the data of data subjects located in Kenya, who are only transmitting data through Kenya. This is beyond the scope of section 4 of the DPA and runs the risk of not being enforceable.	Definition of "Transferring entity" should exclude entities that transmit data through Kenya that are not resident in Kenya and who do not process the personal data of data subjects located in Kenya.
3	Legally enforceable obligations Regulation 40 *Despite provisions of this Part, the requirements for cross-border transfer may not allow restrictions on cross-border transfers where the transfer:* *(a) is permitted under section 48 (c) of the Act;* *(b) requirements arbitrarily or unjustifiably discriminate against any person;*	The language of this entire provision is ambiguous. Is the intention to set out situations in which cross-border transfers will not be restricted? In the case of (b), what is the criteria for determining "arbitrary or unjustifiable discrimination" and how makes the determination (the DPC or the controller? In the case of (c), what is "restriction on trade"? In the case of (d) what is the "objective" referred to there and whose objective is it? All in all, it is not clear what problem this particular Regulation is seeking to resolve.	The Regulation should be re-drafted in a clear and concise manner to set out situations in which cross-border transfers are not restricted (if that is the intention of the regulation).

#	Regulation	Issue	Recommendation
	(c) imposes a restriction on trade; and *(d) the restrictions on transfers of personal data is greater than are required to achieve the objective*		
Data Localization			
4	Requirement for specified processing data to be done in Kenya Regulation 25 (1) *(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.*	1. The Regulation goes beyond the limits of the Act by referring to "the purpose of actualizing a public good". This is wider than the specific grounds prescribed under section 50 of the Act which were limited to grounds of "strategic interests of the state or protection of revenue". 2. Commercial entities which operate electronic payment systems cannot be reasonably considered as being a "strategic interest of the state". Such commercial entities are not established to fulfill a state mission or a service. 3. The term "public good" is not defined and it is therefore not clear what it means to "actualize a public good". 4. "Serving Copy" is also not defined. Data controllers or data processors required to comply with this Regulation are unsure of the nature of the obligation to keep a serving copy in Kenya.	1. The Regulation should be re-drafted to provide a clearer list of activities that require data localization and these should be in line with section 50 of the Act. The Regulations should focus on those activities that are of a public sector nature to avoid imposing an unduly onerous compliance burden on private sector entities. 2. The protection of personal data should be the same regardless of whether the controller is a public or private sector entity and only processing matters that affect strategic interests of the state or protection of revenue should be localized. 3. Commercial entities that operate a business-to-business payment system be excluded from Regulation 25. 4. In alignment with international best practices, the ODPC should refrain from creating subsets of personal data (besides sensitive data) that would

#	Regulation	Issue	Recommendation
		5. The ability of Kenyan servers to host the data provided for is in question and raises cybersecurity issues. 6. No reassurance or clarification given as to the protocols and mechanisms the OPDC will adopt to facilitate local server storage and processing activities. 7. Localization requirements will ultimately impact the government's ability to use advanced technology solutions that are not available in Kenya. 8. The Cabinet Secretary may require a data controller who processes personal data outside Kenya to ensure that such processing is effected through a server and data center located in Kenya in the event of a breach or failure to cooperate with the Data Commissioner. This Regulation fails to consider that it is difficult to set up a local delivery center with support staff and migrate customer data. This typically takes years. This also raises grave concerns about how this would impact service availability in the event of such a forced localization. 9. Given the current and future implications of Covid-19, especially around the ability to provide proof of vaccinations or test results to facilitate travel, the requirement to process health data in Kenya will prevent the processing of this data	be subject to different management guidelines. The ODPC should exclude personal information collected in the context of education and the processing of financial payments from the data localization. The management of personal data in financial services falls under the responsibility of the Central Bank of Kenya (CBK) and the proposed provisions of the Regulations clashes with the risk-based approach of CBK regarding the processing of data and outsourcing activities of banks. 5. The Regulations should consider the use of privacy and security certifications. The EU is now increasingly leveraging privacy security certifications to ensure data protection, instead of restrictions on the processing and sharing of data. Improving security hygiene and data governance should be the main objective of the Regulations. In this regard, international standards security, privacy standards and codes of practices have proven their efficiency as an appropriate mechanism to demonstrate compliance with privacy legislation. 6. Regulation 25(2)(g) should be clarified to accommodate considerations arising from global health pandemics. 7. The Cabinet Secretary, prior to exercising powers under Regulation 25, should be forced to

#	Regulation	Issue	Recommendation
		offshore to facilitate the cross-border travel of Kenyan residents. 10. The rationale for localizing data processing in respect of some the activities listed in Reg 25(1) is not clear eg: managing personal data to facilitate access of primary and secondary education in the country; managing any electronic payments systems licensed under the National Payment Systems Act; processing health data for any other purpose other than providing health care directly to a data subject; managing any system designated as a protected computer system in terms of section 20 of the Computer Misuse and Cybercrime Act, 2018. These activities cover the businesses carried out by a broad range of private sector institutions such as: private/international schools; authorized payment service providers; multinational insurance entities; multinational banks and underwriters, brokers and agents. The Regulation would impose a significant compliance burden (in terms of cost, time and human resource allocation) on these private sector entities. 11. list should only cover public data processing, not processing by private companies.	consider the factors of the data controller and consult with the data controller on the same.

#	Regulation	Issue	Recommendation
Automated Decision Making			
5	Automated individual decision making. Regulation 21 *(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;*	1. Demarcation of automated individual decision making too broad (no restriction to legal effect). 2. The obligation to inform data subjects of decisions made pursuant to automated decision-making process is placed on data controllers and processors. This should be the responsibility of data controllers. 3. Some automated decision-making processes have a minimal impact on data subject rights.	1. Clarify the form and type of 'automated decision making' in question 2. This Regulation should only apply to data controllers. 3. The obligation to inform a data subject when engaging in automated decision making should only apply when the automated processing will result in a decision with significant legal effects for the data subject.
High Risk Processing Activities			
6	Processing activities requiring data protection impact assessment. Regulation 42 (b) *For the purpose of section 31 (1) of the Act, processing operations taken to constitute high risks and that shall require conducting a data protection impact assessment prior to processing include —*	The high-risk activities listed in this Regulation are undefined and ambiguous.	The Regulation should be amended to provide a clearer set of high-risk activities that are easy to comprehend Suggest deleting the following from the list: (b) use of personal data on a large-scale for a purpose other than that for which it was initially collected; (d) a single processing operation or a group of similar processing operations; (h) combining, linking, or cross-referencing separate datasets where the data sets are combined from different

#	Regulation	Issue	Recommendation
	d) a single processing operation or a group of similar processing operations; *e) financial and reputational benefits, demonstrating accountability and building trust and engagement with data subjects;* *m) any similar or related processing activity.*		sources and where processing is carried out for different purposes; (i) large scale processing of personal data; - add "sensitive"
Direct Marketing			
7	Modes of direct marketing 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*	1. Neither of the terms "Commercial Purposes" or "Direct marketing" are defined in the Act or the Regulations. The two terms appear to be used interchangeably, yet they are not synonymous. The plain meaning of "commercial purposes" is broader than "direct marketing". If the policy objective is to restrict "direct marketing" activities (as with GDPR), then that is the specific term that should be used to avoid ambiguity as to what other activities are restricted.	1. Replace the term "commercial purposes" with "direct marketing" in the Act and Regulations. Ensure that the term "direct marketing" is defined in the Act and the Regulations.

#	Regulation	Issue	Recommendation
	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.* *Regulation 14* *Permitted commercial use of personal data* *(b) a data subject is notified that direct marketing is one of the purposes for which personal data is collected.* *(i) the data subject has consented to the use or disclosure of the personal data for that purpose.*	2. Opt-in mechanism	2. Suggest permitting companies to send direct marketing to their existing customers based on opt-out rather than opt-in mechanism.

#	Regulation	Issue	Recommendation
Consistency on time periods for entities to respond to data subject requests			
8	Data Access Request Regulation 8(2) *A data controller or data processor shall —* *(a) on request, provide access to a data subject of their personal data in its possession;*	1. The time periods for responding to data subject requests are not consistent and appear to be arbitrary. We propose that save for the request for data portability, a general rule should be applied. 2. Organizations that are building their privacy compliance programs may need to manually search their databases in order to identify appropriate information, and then review such information on a case-by-case basis to determine whether any exceptions apply, for example whether providing access to the data could adversely impact the rights and freedoms of others.	General Rule: all data subject requests should be acknowledged within two business days and the requisition should be acted on within thirty days. The controller should be able to extend the response period by two further months where necessary, with the controller obligated to inform the data subject of any such extension, as well as the reasons for the delay, within thirty days of receipt of the initial request.
Data Controller vs Data Processor			
9	Consent by data subject, Collection of personal data, Restriction to processing, Objection to processing, Data access request, Rectification of personal data, Data portability request, Right of erasure, Exercise of rights by others, Modes of direct marketing, Permitted commercial use of personal data Rectification of personal data	These Regulations have been drafted to apply to data controls and processors alike. However, under the Act, data processors process personal data on behalf of data controllers and do not determine the purpose and means of processing personal data. As such, it would not be appropriate to have these provisions of the Regulations apply directly to processors. In the cloud computing context, for example, data processors – being the cloud services provider – often have no visibility or control on the data being processed (including the lack of ability to distinguish personal data	1. ODPC should revisit all clauses where obligations are placed jointly on data controllers and processors and distinguish clearly between obligations of the controller and processor. The controller/processor distinction is meaningful and important from a practical perspective and the responsibilities tied to each role should reflect the actual activities and level or control each party has over personal data. 2. Data processors should only be expected to:

#	Regulation	Issue	Recommendation
	Regulation 9(4-14)	from other types of data) and it would therefore be inappropriate for them to have the same obligations as a data controller.	• Implement reasonable and appropriate security measures for their electronic systems; • Ensure their contracts with data controllers contain adequate safeguards; and • provide reasonable assistance to the data controllers to enable the latter to comply with their obligations, where applicable. 3. Specifically, the following obligations ought to rest with the data controller and not the data processor: • Informing the data subject of the processing (Reg.4 (1)); • Obtaining consent from the data subject (Reg.4 (3)) or fresh consent (Reg.5); • Collection of personal data (Reg.5) and correcting inaccuracies (Reg.21); • Managing data subject's restriction requests (Reg.6) or data subjects' objection to processing (Reg.7); • Managing data subjects' requests to access data (Reg.8), rectify the data (Reg.9), erase data (Reg.11), anonymize/pseudonymize data (Reg.19) cease marketing activity (Reg.17) • Opt out mechanisms for data subjects (Reg. 15 and Reg.16)

#	Regulation	Issue	Recommendation
			• Data retention (Reg.18) • Informing the data subject when engaging in automated processing (Reg. 21)
Ambiguity			
10	Data Access Request Regulation 8(4)(f) *A request for access to personal data may be declined on the grounds that—* *(f) giving access would likely reveal evaluative information generated by the data controller or data processor in connection with a commercially sensitive decision-making process.*	The terms "evaluative information" and "commercially sensitive decision-making process" are undefined, which results in this Regulation being ambiguous.	ODPC should provide further guidance on what evaluative information regarding a commercially sensitive decision making process is.
Privacy Accountability Frameworks			
11	Form 1- Request for Restriction or Erasure Form 2 - Data Portability Request Form	The multiple forms do not comply with the principles of data minimization. Data Portability Requests	1. The ODPC should not be prescriptive and simply set out minimum requirements for forms. These can then be formulated by each data controller. This will encourage industry self-regulation.

#	Regulation	Issue	Recommendation
	Form 3 - Request for access to personal data Form 4 - Request for rectification of personal data Form 5 - Request for erasure form *Regulation (10) Data Portability Request* *(1) A data subject may apply to transfer or copy their personal data from one data controller or data processor to another.* *(6) Where a data controller or data processor declines the portability request, it shall within seven days notify, in writing, the data subject of the decision and the reasons for the decisions.*		2. Data controllers and processors should not be precluded from using their own templates and/or tools to conduct and document DPIAs, provided that the DPIAs meets the minimum requirements of the Regulations. This could be handled instead by requiring companies develop **an Art 30 GDPR records** of processing type document which could be required to be provided to the authority on request. 3. Data Portability Requests: 1) suggest adding "where the processing is carried out by automated means and where a transfer is technically feasible". (6) this time period is too short. This should be within one month of receipt of the request.
Breach Notification			
12	SECOND SCHEDULE The circumstances amounting to a notifiable data breach.	1. The categories of personal that would automatically amount to a notifiable data breach are very broad. The "risk of harm to a data subject" may vary depending on the nature of the specific circumstances.	1. The notification and communication of breach requirements should not automatically apply in equal measure to all circumstances listed in the Second Schedule. Data controllers should be granted appropriate time to determine the

#	Regulation	Issue	Recommendation
		2. The Regulations should incorporate and encourage best practices in incident management by encouraging organizations to take effective remedial action. Where prompt and effective action is taken or where the data is rendered unintelligible (e.g. encryption), there would not be a real risk of harm to data subjects. Notification to data subjects in such instance will only result in notification fatigue.	nature and extent of the breach and the potential risk of harm to the individual and only notify the ODPC and the data subject in the event that there is a real risk of harm to the data subject. 2. We recommend that Regulation 35(2) be amended as follows: *(2) A breach of any personal data envisaged under paragraph (1) amounts to notifiable data breach under section 43 of the Act unless the data controller or data processor has taken remedial action to reduce the real risk of harm to the affected data subject, or has implemented technological protection that is of a reasonable security standard such that the data breach is unlikely to result in real risk of harm to the affected data subject.*
Consent as a lawful basis for processing data			

#	Regulation	Issue	Recommendation
13	Regulation 4 Consent by Data Subject	The ODPC has, in the Regulations and in the Guidance Note on Consent, not provided adequately for the grounds of deemed or implied consent. Written and oral consent may not be always be practicable and overly stringent requirements for consent will slow the provision of goods and services to consumers and increase compliance costs without necessarily increasing security for data subjects. In practice the legal requirements for consent also lead to 'consent desensitization', which ultimately undermines privacy protection and trust in data processing.	1. ODPC should expand the grounds for processing of personal data to incorporate deemed or implied consent. For example, when a data subject hands over a credit card to a retailer to process a payment, their consent for the collection, use and disclosure of their personal data (i.e. credit card payment data) for the purposes of processing the payment can be implied through their actions. 2. The Singapore Personal Data Protection Act (2012), includes deemed consent bases under which a data subject's consent can be "deemed" if the data subject voluntarily provides the data for a purpose and it is reasonable that the data subject would do so. 3. Singapore has also introduced the notions of "notification for purpose" and "business and legal purpose" as alternative frameworks under which personal data can be processed and collected. "Notification of Purpose" refers to notifying individuals of the purpose of the handling and "Legal or Business purpose" refers to the handling of personal data for a legal or business purpose. We recommend the inclusion of additional bases for processing to ensure that developments in technology, particularly IoT, are supported by the lawful collection of personal information.

#	Regulation	Issue	Recommendation
Others			
14	Restriction to processing Regulation 6 *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* *(c) the data subject no longer needs their personal data but the requires it to be kept in order to establish, exercise or defend a legal claim; or*	Regulation 6 (c) erroneously refers to the data subject	Regulation 6(c) to be amended to refer to the data controller and not the data subject.
15	Objection to processing 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*	Regulation 7 (5) erroneously refers to the data subject. The data controller should be obligated to demonstrate these provisions to override the right to object to processing.	Regulation 7 (5) to be amended to refer to the data controller and not the data subject.

#	Regulation	Issue	Recommendation
16	Data Access Request Regulation 8 *(2) 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 electronic or manual mechanisms to enable a data subject access their personal data; or* *(c) provide the data subject with—* *(i) a copy of their personal data; and* *(ii) details of the use and disclosure of their personal data.* *(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;* *(b) giving access would have an unreasonable impact on the privacy of any other data subject;* *(c) the request for access is frivolous and vexatious;*	1. The drafting of Regulation 8 (2) and the use of "and" and "or" is unclear. 2. Each data controller should determine appropriate methods of verification or authentication that reflect the services or products required (as personal identity may not always be sufficient to verify account ownership). 3. Two important exceptions to access requests are when responding to such requests would interfere with CSEAI (child sexual exploitation and abuse material) and digital safety policies or would interfere with ongoing criminal investigations.	1. Regulation 8(2): (a) and (b) should be provided as two options for the data controller in responding to access requests, and (c) should apply for data subjects using either the (a) or (b) mechanisms. 2. Each data controller should determine appropriate methods of verification or authentication that reflect the services or products required. 3. Regulation 8(4) should allow a controller to deny an access request "in instances where it interferes with a criminal investigation". 4. ODPC should provide clarity on what "*evaluative information generated by the data controller or data processor in connection with a commercially sensitive decision-making process" means.* 5. Suggest changing this to categories of recipients rather than including the actual recipients.

#	Regulation	Issue	Recommendation
	(d) giving access would be unlawful; *(e) denial of access is authorised by an order of the court; and* *(f) giving access would likely reveal evaluative information generated by the data controller or data processor in connection with a commercially sensitive decision-making process*		
17	Automated Decision Making Regulation 21 *(2) Pursuant to section 35 of the Act, a data controller or data processor making automated decisions shall—* *(e) ensure the prevention of errors, bias and discrimination;* *(h) process personal data in a way that prevents discriminatory effects.*	An organization cannot "ensure" prevention of errors, but instead should be obligated to take all appropriate measures to prevent errors, bias, and discrimination.	21 (2) (e) to be delated as this is adequately covered in 21(2)(g) and (h) or 21 (1) add "that results in legal or similarly significant effects".

#	Regulation	Issue	Recommendation
18	Data Protection Policy Regulation 22 *22. (1) A data controller or data processor shall make, publish and regularly update a policy reflecting their personal data handling practices.* *(2) A policy under paragraph (1) shall include—* *(e) obligations or requirements to transfer personal data outside the country, to third parties, or other data controllers or data processors located outside Kenya and where possible, specify such recipients*	Many smaller companies rely on several processors and sub-processors and it may be particularly challenging for them to maintain a complete and up-to-date list of processors/sub processors.	The requirement to disclose the recipients should allow for disclosure of categories rather than individual recipients.
19	Requirement prior to transfer Regulation 38 *(1) A data controller or data processor who is a transferring entity shall before transfer personal data out of Kenya ascertain that—* *(b) subject to paragraph (2), the data subject consents to the transfer of their personal data to that recipient in that country or territory;* *(2) A data subject shall be duly informed of the safeguards and*	1. If a data subject has notice of potential transfer (via an organization's privacy policy) and the organization has ascertained that the recipient has in place appropriate protections for the data, requiring additional consent for the transfer will not provide significant additional privacy protection and will likely lead to "consent fatigue." 2. The data controller should provide notice of the cross-border transfer and the safeguards that have been implemented with respect to such cross-border transfer. It is not clear what "risks" are inherently involved in cross-border transfer given the appropriate implementation of safeguards.	1. Regulation 38(1)(b) to be deleted. 2. Suggest deleting the reference to informing data subjects of "risks" in Regulation 38(2)

#	Regulation	Issue	Recommendation
	implications including the risks involved on cross-border transfer of their personal data.		
20	Provisions for the agreement to cross boarder transfer. Regulation 39 *A transferring entity shall enter into a written agreement with the recipient of personal data, which contract shall contain provisions relating to—* *(a) the unlimited access by the transferring entity to ascertain the existence of a robust information technology system of the recipient for storing the personal data; and*	"Unlimited access" to the recipient's information technology system is disproportionate and poses confidentiality and security problems for the recipient and the recipient organization's other business partners.	The recipient must allow for audits by the controller or independent third party rather than "unlimited access".

#	Regulation	Issue	Recommendation
21	Compounding of offences Regulation 50 *(1) The Data Commissioner may, with the concurrence of the Director of Public Prosecutions and with the written consent of the person who commits an offence—* *(a) compound an offence under section 58 (8) and section 74 of the Act*	Section 58 (8) and Section 74 of the Act are incorrectly referenced. Section 74 relates to codes, guidelines and certification. Section 58(8) relates to enforcement notices.	Referencing error to be rectified.

Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021

#	Regulation	Issue	Recommendation
Registration of data controllers and data processors			
1	Exemption from Registration 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 Act, in section 18(2), requires the Data Commissioner to prescribe thresholds for mandatory registration considering the *nature of the industry* and the *volume of personal data processed*. The current mandatory thresholds set out in Reg 12(1) are not based on industry or volume of data processed but are based on annual turnover.	1. The third schedule classifies data controllers and processors that must register due to the nature of their industry regardless of the turnover. This should be the primary criteria for registration. 2. To avoid duplication of applications by data processors who process data on behalf of data controllers, only data controllers should be required to register with the Data Commissioner, as their applications requires them to disclose their processors. 3. Delete Section 2; as obligation to include retention schedule in privacy policy is burdensome. Retention schedules often challenging to capture given for example a time limit in view of the data stored related to active members.
Certificate of Registration			
2	Certificate of Registration Regulation 8 (2) *A certificate of registration issued under paragraph (1) (a) shall be valid for a period of one year.*	1. The requirement to apply for renewal of registration annually imposes a significant compliance burden on data controllers, data processors and the ODPC. 2. Registration requirements will significantly increase the cost of compliance and reduce the ease of doing business, thus hampering regulated	We propose an evergreen registration that is paid for annually (similar to the banking license issued by CBK)

		entities, especially Kenya's start-ups and SMEs from being able to innovate and participate effectively in digital economy activities	
Change of Particulars			
3	Change of Particulars Regulation 14 *Subject to section 19 (2) of the Act, a data controller or a 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.*	Due to the broad information required to be provided by a data controller or processor under Regulation 19(2), to require any updates to be notified to the Data Commissioner is extremely onerous to the data controllers/processors as well as administratively burdensome to the ODPC.	1. A notification of change should only be required for material changes (as specified by the ODPC). 2. The ODPC should create an online portal for easier administration of applications, renewals and change notifications. 3. Greater clarification needed on the mechanism to facilitate requests regarding regulation (19) treating data anonymously or pseudonymously. Link to cessation of services
Fees			
4	Second Schedule Fees Charged by the ODPC	1. Third party due diligence, compliance audit, compliance support not defined. 2. The fee for approvals of DPIAs is unduly high and prohibitive to businesses undertaking multiple processing operations 3. Potential conflict of interest in having the DPC as the certification entity as well as the enforcing entity.	1. Third party due diligence, compliance audit, compliance support and certification to be defined. 2. Provide for a substantially lower fee for DPIAs 3. Certification should be done by an independent third party. 4. No fees should apply to compliance support and service provision as these are the responsibility of the ODPC. Data controllers and processors should not be precluded from using their own templates and/or tools to conduct and

			document DPIAs, provided that the DPIAs meets the minimum requirements of the Regulations.

Data Protection (Compliance and Enforcement) Regulations, 2021

#	Regulation	Provisions of the Regulation	Proposed Regulation
Online Management Tool			
1	We propose the website of the ODPC provide for an online complaint management system.		
Principle of Internal Exhaustion			
2	Data controllers and processors should be free to set out a complaints handling mechanism in their privacy policy and statement. As part of complaint investigation, the ODPC should assess whether the data subject engaged the data controller or processor to resolve the matter before escalating it to the ODPC. If not, the ODPC should require that internal complaint mechanisms be exhausted before stepping in. As currently drafted, the Regulations and Complaints Guideline do not require parties to use internal mechanisms to resolve issues first.		