No.1, Johnson Street, Yaba, Lagos

12 November 2021

The Chairman, House Committee on Science and Technology
Through the Office of the Clerk
The Lagos State House of Assembly
Alausa, Ikeja
Lagos State

Dear Sir,

COMMENTS AND RECOMMENDATIONS ON THE LAGOS STATE DATA PROTECTION BILL 2021

Ikigai Innovation Initiative (Ikigai Nation) is a non-profit organisation incorporated under the Laws of the Federal Republic of Nigeria. Ikigai Nation aims to advance information technology policy in Africa. We promulgate diverse research on technology policy and legal frameworks across Africa. We also engage relevant stakeholders around the intersection of law, business and technology and advocate for better policies for the ecosystem at large.

Tech Hive Advisory Limited is a technology advisory firm that provides advisory services to private and public organisations regarding the intersection between technology, business, and policy. We focus on how emerging and disruptive technologies alter and influence the traditional way of doing things while acting as an innovation partner to our clients.

This contribution is made to further the call for contributions and recommendations to the Lagos State Data Protection Bill.

contact@techhiveadvisory.org.ng policy@ikigaination.org

Lagos State Data Protection Bill

Reference (Section)	Issues	Comments	Recommendations
1	"Personal data" and "Personal information"	The Bill uses personal information and personal data interchangeably. Yet, the Bill does not state that the two terms are the same. Neither does the Bill define personal information.	The Bill should use either personal information or personal data all through the body. In the alternative, it should be stated that the two terms are synonymous.
1	Definition of "consent."	The definition fails to include the element of clarity in consent. It does not include the need for the consent to be express and explicit. Clarity of consent helps the data controller to demonstrate that a data subject gives consent to the processing.	The definition of consent should include the element of clarity.
	Demonstration of valid consent	The Bill does not require the controller to ensure that it can demonstrate that consent obtained is valid. This fosters accountability when documenting.	The Bill should require the demonstration of consent in furtherance of the controller's accountability obligation.
1	Definition of "sensitive personal data."	The definition provided in the Bill does not sufficiently communicate the risk and the degree of obligation attached to these categories of data.	A revision of the definition of sensitive personal data to show the risks attached to its processing.
	Example (i) under the definition of sensitive personal data	It is unclear who determines what is reasonably permissible and what standards are used to determine what is reasonably permissible.	The criteria to determine what would "reasonably" classify as sensitive personal data should be outlined.
1	Definition of "third	The definition of a third party by subsection	The definition should

	party"	(d) is heavy on the role of the data controller while neglecting the data processor.	include those taking instruction or acting on behalf of the processor. We recommend that the definitions should be redrafted as: ***"third-party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data."***
2(1)(b)	Territorial scope	In stating the territorial scope of the Bill, there is a failure to consider the domicile/residence or location of the data subjects.	The domicile/residence or location of a data subject should be considered. In addition, the territorial scope should be reconsidered to avoid conflict or legal impossibility under international law. We refer you to principles of passive personality, comity, horizontal federalism, and prescriptive jurisdiction under international law.
6(2)(c)& (f)	Inclusion of "a retired Commissioner of Police" in the composition of the Board. Inclusion of Commissioner for Science and Technology	This inclusion of a retired Commissioner of Police is irrelevant. The Bill does not show the relevant expertise that such an individual would bring to the Board. The inclusion of the Commissioner as a member of the executive negates the independence of the Commission. Global international instruments define the membership of the executive arm of the	The provision should be excluded from the composition of the Board. We recommend that the Commissioner be excluded from the Board.

		government to be inconsistent with the principle of independence of a data protection authority. We refer to the ECOWAS Supplementary Data Protection Act, Africa Union Convention on Cybersecurity and Personal Data Protection and Council of Europe Convention 108.	
13	Power to delegate	The delegation of the Commission's investigative and enforcement powers should be limited to persons with expert knowledge on information security, data protection and privacy. A Police Officer may not be so knowledgeable on such topics.	A revision of this provision is necessary.
17(a)	Prior security checks	The check should not be limited to security because security is a principle of data protection. Security threat is just one out of many threats that could confront personal data. The limitation of such checks to security will lead to an omission in identifying the data protection measures that can remedy the risks to the privacy rights of the data subjects.	That the provision should include the power of the Commission to conduct an assessment of risk to processing activities.
20	"Entry and search"	The construction of the provision appears to give the authorised officer the power to enter and search like some law enforcement agencies, which creates an image of coercion in the reader's mind.	We recommend that the provision is constructed to seem less coercive. Rather, a phrase like "obtain access" may be used.
23(2)	Timing of the privacy information	The provision says the information be provided "at the time" of collecting personal data. This creates an ambiguity as to timing and the position of the privacy information.	We recommend that the phrase be changed to "prior to collecting" personal data, emphasising the need for the information before the data subject attempts to give personal data.
	Contents of the privacy information	The information provided does not include the lawful bases for processing the personal data, retention period, basis for the cross-border transfer, some other data subject rights, and the specification of the type of	The provision on the content of the privacy information should be exhaustive to give data subjects adequate information.

		personal data collected.	
23(3)(a)(i)	"Material difference"	The provision does not define what "material difference" meant to exempt a controller from providing privacy information to the data subject.	We recommend that the provision should define "material difference" to prevent abuse.
23(3)(b)(ii)	The use of the word "used."	The provision exempts the controller from providing privacy information where the data is "used" in a form in which the data subject cannot be identified. The provision fails to consider the form of the personal data at the point of collection. That the personal data will be used in a form that removes identifiability does not mean the data was not originally collected in an identifiable form before being de-identified. The collection of personal data is also a form of processing.	If personal data is collected in an identifiable form, the privacy information should be provided even though the actual use will be de-identified.

25(1)	Elevation of the relevance of consent.	Consent was set-out as the most important lawful basis and other lawful bases as exceptions. No lawful basis is more important than the other.	We recommend that consent be set out like any other lawful basis and not elevated as more important than others.
25(2)	Absence of legitimate interest as a lawful basis	Legitimate interest is not included as a lawful basis for data processing. Instead, legitimate interest is a flexible ground for processing and covers processing that the data subject will ordinarily expect from the controller. This is so long as the processing is necessary to achieve the legitimate interest and the legitimate interest is weighed against the rights and interests of the data subjects. Legitimate interest also fosters ease of doing business because it removes restrictiveness that may not be necessary to protect personal data. The absence of legitimate interest of a data controller or third party as a legal basis for processing will make operationalising the Bill difficult. Things like fraud prevention, network and information security or some business to business contact will typically leverage legitimate interest, and the other lawful bases are not appropriate.	We recommend that legitimate interest be included as a lawful basis for processing personal data.
	Vital interest	Processing based on vital interest is limited only to that of the data subject. This ties the controllers' hands where a data subject's data is needed to save another person's life.	We recommend that the vital interest of "other persons" be included on a lawful basis.
27(7)	Notification of data subject	The notification of a data subject where a data breach occurs is required only where the Commission requires it. The time between the notification of the Commission and the Commission's determination of data subjects' notification puts the data subjects at risk if the breach poses a high risk to the data subject's rights and freedom. The ability to notify the data subject timely	The Bill should expressly lay down the condition to be considered by the controller to notify the data subjects of a data breach without waiting for the Commission's determination.

		could make a difference in a case of financial fraud, where a password reset could protect the data subject. However, the latency may deprive the data subject of this benefit.	
28	Age of a child	The provision addresses the processing of a child's data but fails to define a child's age.	We recommend that the age of a child should be defined. A reference could be made to the State's Child Rights Law.
32	Withdrawal of consent to direct marketing	The provision does not require that the process of withdrawing consent must be as easy as the process of collection. This helps to simultaneously fight dark patterns and protect data subjects' rights.	We recommend that the provision state that withdrawing consent to direct marketing should be as easy as collecting consent.
33(1)	Transfer of Personal Data	It may not be best for a state to create rules to regulate the international transfer of data. This is because it may be impossible to enforce it under international law norms. Thereby creating operationalisation problems for organisations subject to the law. This could even become more chaotic if more states regulate cross-border data transfer. The requirement of the written authorisation of the Commission to transfer personal data outside the State seems to be too strict. As long as the State where the personal data is to be transferred to is considered to have adequate safeguards or the conditions in subsection (2) are complied with, the requirement seems unnecessary. Also, data by its nature requires free flow; requiring authorisation could hurt commercial interests before approval.	We recommend the exclusion of this provision.
33(2)(b)	Conditions for transfer	This section does not acknowledge that transfers may be necessary based on the vital interest of the data subject.	Transfers based on vital interests should be included.
37	Registration of data controllers and	Aside from the financial benefit to the State and the creating a database of processors	We recommend that the registration requirement

	processors	and controllers, it does not appear that there is any regulatory or operational benefit for registration. There is no evidence that it helps the regulator enforce the law better or keep compliance optimal.	be expunged as it could be difficult for small and medium-sized businesses already exposed to multiple statutory payments and the high cost of running the business. Instead, effort should strengthen the Commission, raise awareness, and encourage the implementation of a privacy program.
38(2)	Providing information about data subject to the Commission	The provision mandates that a processor or controller register each purpose of processing distinctly and does not have any economic or operational benefit. Moreover, although part of the information required for the register includes disclosing the identity of data subjects whose data is processed, such disclosure is an infringement of the privacy rights of the data subjects involved.	We recommend that the requirement should be expunged.
45(1)(b) &(4)	Access to personal data	This section provides that a data subject would only have access to data held about them where a fee is paid. This would most likely discourage data subjects from exercising their right to access their data.	The fee requirement should be excluded, and if at all a fee should be paid, it should be where the request is made frequently, unreasonably or requires much time and effort.
Part VII (45-47)	Rights of data subjects	The Bill only recognises a data subject's right to access personal data and rectify personal data. It ignores the data subject's right to erasure, portability, restriction of processing, and object.	We recommend that other data subject rights be included in the Bill to reflect the global and evolving State of data subject rights.
48	Exclusive power of the Governor to determine and declare what constitutes national	The exercise of this power without oversight could lead to abuse of power.	We recommend that the power should be exercised with parliamentary or judicial oversight.

	security		
49	Exemption of lawful basis for processing data under section 25 and lack of limitations on exemption after data has been processed for its original purpose	Of particular concern is section 25, which section 49 seeks to exempt. Section 25 provides for the lawful basis for processing data, and 25(2)(e) & (f) provide for the administration of justice and public interest, respectively, as a lawful basis for processing data. Crime investigation and tax administration are matters that fall within the public space and involve judicial processes. As such, exempting crime and tax-related data from the provisions of Section 25 may create room for rights abuse concerning the personal data of suspects. These provisions can serve as guardrails in the investigative process without running counter to other exemptions. The section also fails to state whether or not the exemption still applies after the data has been processed for crime prevention or taxation activity and is no longer used for that purpose.	The exemption in section 49 should be reviewed to accommodate the applicability of Section 25 or to accommodate the applicability of section 25(2)(e) & (f) in particular. It should also be expressly provided that the exemptions no longer apply where data originally obtained in connection to crime or tax matters is no longer used for that purpose. This is in line with international best standards, like the UK Data Protection Act 2018 (Using the crime and taxation exemptions – s.29)
50(2)	Grants the Governor exclusive power to waive the obligation to grant access to personal data concerning social work.	This section weakens the proposed Lagos Data Protection Commission by giving what should be one of its powers to the Governor, without balancing it with the requirement to solicit recommendations from the Commission, or other agencies in the State related to social work, such as the Office of the Public Defender, or the Lagos State Domestic and Sexual Violence Response Team, for instance. This is also contrary to the spirit of independence of data protection authority under international human rights norms. Furthermore, the Commission's action should not be interfered with by members of the executive.	This subsection should be reviewed to either vest the Commission with the power to waive the obligation, or on the recommendation of the relevant social work agency in the State, on a case-by-case basis. This was the case under the Brazilian General Data Protection Law 2018, where Article 13(3) provides that access to health and sanitation data is subject to

			national authorities and authorities within their scope of competencies
51(2)	Extends the scope of the journalistic exemption to section 27, thus freeing journalistic, literary, and artistic purposes from the obligation to keep personal data secure.	The nature of journalistic work keeps evolving with digital tools and smart devices that allow journalists to work from anywhere under different work arrangements. Work started on an office computer can be continued on a personal smartphone or home computer with less secure protocols. Because of this, section 27(2) is more relevant as it requires data controllers or processors to take reasonable steps to ensure that their employees are aware and comply with relevant security measures. This might include media houses instructing employees not to work with public wi-fi when away from the office or introducing encryption measures to devices. Consequently, the exemption will further guarantee the rights to freedom of expression and privacy.	51(2) provisions should be amended to delete section 27 from the exemption scope to ensure personal data security.
59	Service of notice: exclusion of digital means of communication and failure to provide information about the nature of the violation	This section fails to provide that the notice to be served should state the alleged breach under the Act. It also fails to accommodate service of notice by alternative means where personal service cannot be affected. The Supreme Court of Nigeria, in *CE & MS Ltd v. Pazan Services Ltd,*[1] recognised service of processes by SMS as valid where personal service cannot be affected. In Lagos State, the *High Court of Lagos State (Civil Procedure) Rules 2019* permits service by email, where personal service cannot be effected, under Order 9, Rule 5.	This section should be amended to provide that the notice served provides details of the breach. It should also be amended to support service of notice by email or SMS, where any of the already specified modes of service cannot be affected. This is in line with the latest judicial and legal position in Nigeria and Lagos State.

[1] (2020) 1 NWLR (Part 1704) 70

60	Absence of administrative power	The Bill fails to include the exercise of administrative control by the Commission.	We recommend that the Commission should be granted corrective and advisory powers. Not all violations of the law should result in punitive fines when they can be warned or advised.
	Omission of the principle of accountability	The Bill omits accountability as a principle. Instead, accountability implores controllers and processors to demonstrate compliance with the law. This is attained through the appointment of a data protection officer, documentation of processing activities, implementation of data protection by design and default, undertaking data protection impact assessment, and implementing modalities and procedures for the exercise of data subject rights. The failure to include accountability may make the implementation and operationalisation of the proposed law difficult.	We recommend that the principle of accountability should be included and the obligations required specifically spelt out.
	Lack or insufficient definition of terms	The lack of or the definition of certain words are defective and could lead to poor implementation of the law. For instance, the word 'reasonably' as used in Section 25, which provides instances where seeking consent to process data is not required, is a subjective term that can be misinterpreted. This is recommended to avoid being missing in context or subject to misinterpretation.	We recommend that words and terminologies should be sufficiently defined.
	Failure to define the basis for sanctions	While the Bill is clear on sanctions and penal regime, it fails to specifically provide for the basis for imposing fines, which could assist in determining the severity of imposition or otherwise.	We recommend that when imposing fines, the Commission should consider other factors. For example, the nature, gravity and duration of the infringement; the purpose of the processing; the number

			of the data subject concerned; level of damage and damage mitigation measures implemented; intent or negligence; degree of cooperation with the Commission; and categories of personal data.
	Right to a judicial remedy	The Bill omits the inclusion of the data subject's right to a judicial remedy.	We recommend that it should be expressly included in the Bill.

Conclusion

The Bill is an improvement on the current Data Protection Regulations in Nigeria. However, there are some flaws and inconsistencies that may create challenges in the implementation of the Bill. Thus, we have set out our recommendations to improve the overall quality of the legislation and correct the identified flaws and inconsistencies. We are also happy to support the work of the committee if need be.

Accept our highest professional regards.

Tech Hive Advisory
Ikigai Innovation Initiative