DEMOCRACY REPORT

SPECIAL BRIEFING REPORT NOVEMBER 2022

Photo by Taylor Vick on Unsplash

Not fit for purpose

– THE DATA PROTECTION BILL, 2021

CONTENTS

This briefing paper was compiled by ALT Advisory, First Floor, 20 Baker St, Rosebank, Johannesburg, 2196, South Africa. An adapted version of this paper was submitted as the ACTION Coalition input to the consultations around the draft Data Protection Bill to the Ministry of Information, Communication and Technology (MICT) on 30 November 2022.

Democracy Report is a regular publication featuring analysis and commentary relating to the legislative agenda of the Parliament of the Republic of Namibia. It is produced by the Institute for Public Policy Research (IPPR), PO Box 6566, Windhoek, Namibia. Tel: +264 61 240514, info@ippr.org.na. The publication is also available as a PDF download from http://www.ippr.org.na. Democracy Report is funded by the Embassy of Finland.

Embassy of Finland Windhoek

SUMMARY OF KEY SUBMISSIONS AND RECOMMENDATIONS

The following constitutes a summary of the key submissions and recommendations contained in these submissions:

General recommendations

1. The Bill, while ensuring public participation and the full and proper protection of data subjects, should be fast-tracked to ensure that constitutional obligations, in this instance the protection and promotion of the right to privacy, are performed diligently and without delay.

2. The Bill should be further developed following this public participation process and further opportunities to provide written submissions on future versions of the Bill should be provided to all stakeholders, including civil society.

Prior consent

3. Adding the element of prior consent to all data subjects strengthens the definition of "consent" in **section 1** of the Bill and ensures that data subjects must consent to the processing of their personal data prior to processing.

The rights of data subjects

4. The Bill should reintroduce **Part III of the 2020 version of the Bill** as a new Part 2 in the present Bill, with the "Data Protection Supervisory Authority" part becoming a new Part 3. This will correctly give prominence to the primary rights holders in the Bill: data subjects.

Independence of the Supervisory Authority

5. **Part 2** of the Bill needs to be substantially redrafted in line with the 2020 version of the Bill to ensure that appointments, removals, and the remuneration of board members of the Supervisory Authority are determined by Parliament as opposed to the Minister, and that board members, including the chairperson and the vice-chairperson, are afforded security of tenure and are shielded from undue political influence. Additionally, in appointing board members, Parliament should be directed to seek public nominations before initiating any appointment processes.

Enforcement powers of the Supervisory Authority

6. Section 4(h) should be amended to read: "be responsible for investigating contraventions of, and enforcing compliance with, this Act . . .". Additionally, the MICT may consider defining, or providing further clarity on, "the Court" in **section 5(1)(h)** and including additional enforcement-related provisions within **sections 4 and 5** which explicitly empower the Supervisory Authority to issue sanctions, in the form of fines and other administrative penalties, for non-compliance with the Act.

Offences, penalties, and administrative fines

7. **A new Part or Chapter** — based on Part VIII of the 2020 version of the Bill but developed as necessary — should be included in the Bill which refers directly to offences, penalties, and administrative fines. This Chapter should consolidate the offences and administrative fines referenced in the Bill and:

    7.1 Expressly create an offence for any person who hinders, obstructs, or unlawfully influences the Supervisory Authority; who fails to comply with an assessment or enforcement notice; or who obstructs the execution of a warrant, among others.

    7.2 Establish criminal penalties for offences which may include fines or imprisonment, or both.

    7.3 Create administrative penalties, in the form of fines, which may be issued by the Supervisory Authority for non-compliance with the Act.

Civil liability

8. Either in **sections 4 and 5 or in a new Part or Chapter**, the power of the Supervisory Authority, or an individual, to institute civil action should be prescribed.

Exceptions

9. **Section 43(1)** does not contain a subsection (e) and **section 43(2)** refers to a "regulation" in **section 43(1)**, which is unclear and unspecified. The Bill should be amended accordingly.

10. Sufficiently detailed regulations should be published in terms of **section 43(1)** providing clear and precise definitions, objective and adequate safeguards, and further general guidance on the application of the exceptions contained in **section 43(1)** of the Bill, particularly **sections 43(1)(a), (c), (d), and (i)**. Alternatively and preferably, the Bill itself should be developed to provide further guidance on the exceptions.

11. An express exemption for journalistic, literary, or artistic purposes should be recognised in the Bill, either in **section 34(1)(f)** or **section 43**, and should provide that "The Act does not apply to the processing of personal data solely for the purpose of journalistic, literary, or artistic expression to the extent that such an exclusion is necessary to reconcile, as a matter of public interest, the right to privacy with the right to freedom of expression, including press freedom." (Additionally, an express exemption for processing personal data for academic purposes, with sufficient safeguards, should be considered by MITC.)

Exemption applications

12. **Section 43** does not empower the Supervisory Authority to grant additional "exclusions" or exemptions for the processing of personal data. While this may perceivably fall within the remit of "Codes of Conduct" in **sections 44 to 52**, an express enabling provision should be included in the Bill within **section 43**, alternatively a new **section 44**, to enable the Supervisory Authority to grant an exemption to a responsible party to process personal information if it is in the public interest to do so, and there is a clear benefit to the data subject or a third party that outweighs, to a substantial degree, any interference with the privacy of the data subject or third party that could result from such processing.

Interaction with the Information Commissioner

13. Sections should be expressly included in both the Bill and the Access to Information Bill to delineate how the mandates of the Supervisory Authority and the Information Commissioner will interact in order to ensure that both oversight bodies are able to function cohesively and effectively.

Additional recommendations

14. To ensure consistency in the Bill, **section 30** should be re-titled or renamed "Personal data breach notifications" to align with the definition of a "personal data breach" in **section 1**.

15. A new subsection in **section 30** should provide for offences, penalties, and/or administrative fines in the event that a data controller does not provide the required notification of a personal data breach. Alternatively, the suggested **new Part or Chapter** on offences, penalties, and administrative fines should expressly list a failure to notify a data subject of a personal data breach as an offence warranting a penalty or administrative fine.

16. Unsolicited direct marketing — by any means or form of electronic communication, including automatic calling machines, facsimile machines, SMSs, or e-mail — should be expressly prohibited in the Bill due to its intrusive, unwanted, and non-consensual nature. As a result, a new section should be introduced in the Bill which expressly prohibits unsolicited direct marketing, without consent, and enables the Supervisory Authority to issue administrative fines against responsible parties.

17. To foster transparency, **section 5(1)(c)** of the Bill could include a further subsection stating that "The duties and functions of the [Supervisory] Authority in terms of this Act are to monitor and enforce compliance by prescribing the use of terms of service icons on applicable websites, applications, and other internet-enabled platforms, and providing guidance to controllers on the use of terms of service icons on these platforms."

18. In order to ensure that the Supervisory Authority is established within the one-year time period stipulated in **section 75** of the Bill, practical steps should be taken to fully establish, fund, and staff the Supervisory Authority following the commencement of the Act, including taking pre-emptive measures to ensure that there are no delays with the establishment of the Supervisory Authority following the commencement of the Act.

I INTRODUCTION AND OVERVIEW OF SUBMISSIONS

1. The Institute for Public Policy Research (IPPR) welcomes the opportunity to provide submissions to the Ministry of Information and Communication Technology (**"Department"** or **"MICT"**) on the draft Data Protection Bill, 2021 (**"Bill"**).

2. We are encouraged by the call for public participation and engagement on the Bill and, more broadly, to witness Namibia edge closer to enacting data protection legislation. The further development of the Bill is indicative of Namibia's efforts to protect and promote the constitutional right to privacy; a right that we hope will receive greater and more nuanced attention across the region and the continent in the short and medium terms.

3. However, we note the unduly protracted process which has led to the publication of the Bill and the enactment of data protection legislation in Namibia. The absence of a data protection framework puts Namibia in a minority of states both globally and regionally. Given the mass collection and use of personal information in Namibia — most notably the introduction of biometric identity card systems for all Namibian citizens and permanent residence permit holders (16 years or older) in 2005,[1] the use of biometric voter verification machines during the 2014 elections,[2] and the use of data processing in response to the COVID-19 pandemic[3] — **the Bill, while ensuring public participation and the full and proper protection of data subjects, should be fast-tracked to ensure that constitutional obligations, in this instance the protection and promotion of the right to privacy, are performed diligently and without delay.**

About IPPR

4. The IPPR4 is a not-for-profit organisation that seeks to deliver independent, analytical, critical yet constructive research into social, political, and economic issues that affect development in Namibia. Since its establishment in 2001, the IPPR has developed a team of independent, highly-qualified researchers working across three core areas: democracy and governance research, public opinion, and public policy analysis. Privacy and data protection have increasingly become prominent areas of interest within the IPPR's core areas.

5. In recent years, the IPPR has closely monitored and detailed several concerns regarding public and private entities and persons processing personal information outside of the bounds of a legal framework. Most recently, in September 2022, IPPR met with a network of civil society organisations to engage on and discuss Namibia's digital rights landscape across several areas, including data protection, cybercrimes, and communications surveillance, particularly in connection with national security and policing. In anticipation of these discussions, the IPPR commissioned an advocacy report to analyse digital rights issues in Namibia.[5]

1 Privacy International, 'The right to privacy in Namibia,' 2015, accessible here.
2 Id.
3 CIPESA and ISOC Namibia, 'Data protection and privacy in Namibia: an exploratory study in the context of COVID-19', 2021, at para 10, accessible here.
4 More information about the IPPR may be accessed on its website: https://ippr.org.na/.
5 The report is available on request.

The 2020 Bill and the 2021 Bill

6. While acknowledging the slow progress in enacting a data protection framework in Namibia, we note that the present iteration of the Bill (as circulated in October 2022 and dated 2021[6]) appears to be substantially different in comparison to previous versions of the Bill, particularly the draft 2020 version of the Bill which was subject to a multi-stakeholder engagement in February 2020. **The present iteration of the Bill is of concern and, in multiple instances, removes or amends necessary and important sections from the 2020 version of the Bill**, including, among others:

   6.1 Removing Part III of the 2020 Bill which affirms the rights of data subjects.

   6.2 Removing Parts VII and VIII, which relate to recourse to the judicial authority and offences and penalties.

   6.3 Substantially reducing the institutional independence of the Data Protection Supervisory Authority (**"Supervisory Authority"**) by reducing parliamentary involvement in the appointment, removal, and remuneration of board members.

7. While the reason for these sweeping changes remains unclear, they are addressed, in part, in these submissions. However, as a result of these changes, the Bill should be further developed following this public participation process and further opportunities to provide written submissions on future versions of the Bill should be provided to all stakeholders, including civil society.

Overview of submissions

8. On the face of it, the Bill appears to include several essential components of a data protection framework but, distinct from the 2020 Bill, it removes some key sections and seeks to include some essential elements in a piecemeal fashion. We are pleased by the establishment of the Supervisory Authority (although concerned by its institutional independence); provisions dealing with authorisation prior to the collection of special personal information; the provision prohibiting the processing of children's personal information; and provisions pertaining to transborder data flows. However, the Bill should, among others, more explicitly detail and affirm the rights of data subjects, establish offences, penalties, and administrative fines, and better equip and empower the Supervisory Authority to issue sanctions.

9. We also note that certain aspects of the Bill still require further development to align with best practices, which we detail below, and in some instances the provisions of the Bill should be more clearly drafted. Accordingly, we have identified the following **seven areas** which, among others, warrant further consideration by the MICT:

   9.1 **First**, prior consent should be required for the processing of personal data.

   9.2 **Second**, the rights of data subjects must be expressly detailed and affirmed.

   9.3 **Third**, the institutional independence of the Supervisory Authority must be guaranteed, its powers, duties, and functions need to be further clarified, and offences, penalties, and fines must be expressly included in the Bill.

   9.4 **Fourth**, the exceptions are overbroad and insufficiently detailed.

   9.5 **Fifth**, there is a lack of clarity regarding exemption applications.

   9.6 **Sixth**, there is a lack of clarity regarding the interaction with the Office of the Information Commissioner established in terms of the Access to Information Bill.

   9.7 Finally, we list additional practical matters for further consideration.

10. These are dealt with in turn below.

6 See https://action-namibia.org/government-seeks-public-input-on-draft-data-protection-bill/. The Bill accessible at this hyperlink forms the basis for these submissions.

II PRIOR CONSENT

11. In its present definition of "consent" in section 1, the Bill provides that '"consent" means any freely given, specific, informed, and unambiguous indication of the data subject's wishes'. While this accords with comparable legislation, the Bill may benefit from the insertion of the word "prior" after "informed". Adding the element of prior consent to all data subjects strengthens the definition of "consent" in section 1 of the Bill and ensures that data subjects must consent to the processing of their personal data prior to processing. Notably, in section 42 of the Bill, it is only the processing of the personal information of children which is currently subject to "prior consent" requirements.

III THE RIGHTS OF DATA SUBJECTS

12. Dissimilar to the 2020 version of the Bill, the Bill does not clearly and cogently identify the rights of data subjects and removes Part III of the 2020 version of the Bill in its entirety. On a full reading of the Bill, which only addresses the rights of data subjects in a limited and piecemeal fashion, the rationale for removing Part III of the 2020 version of the Bill is unclear.

13. Cognisant that the nature of data protection legislation is the protection and promotion of the right to privacy, and a balancing of how privacy intersects with other rights, including freedom of expression and access to information, **the Bill should be approached from a rights-based lens. Accordingly, the Bill should reintroduce Part III of the 2020 version of the Bill as a new Part 2 in the present Bill, with the "Data Protection Supervisory Authority" part becoming a new Part 3. This will correctly give prominence to the primary rights holders in the Bill: data subjects.**

IV INDEPENDENCE, DUTIES, AND FUNCTIONS OF THE SUPERVISORY AUTHORITY

14. As a point of departure, the IPPR acknowledges the utility in the establishment of the Supervisory Authority. The importance of this office, which is primarily tasked with monitoring and enforcing compliance with data protection legislation, cannot be gainsaid. The General Data Protection Regulation (**"GDPR"**), which is largely regarded as the model data protection law[7] includes the establishment of properly resourced supervisory authorities composed of suitably qualified data protection experts. Similarly, comparative legislation in other comparable jurisdictions, such as South Africa and Kenya, have followed a similar approach.

Independence of the Supervisory Authority

15. Despite the important need for the establishment of a Supervisory Authority, the Bill regresses from the 2020 version of the Bill in terms of the institutional independence of the Supervisory Authority, which is considered best practice in contemporary data protection frameworks. The 2020 version of the Bill provides that, among others, the Supervisory Authority is operationally and financially independent from the Executive; that it must report annually to Parliament and its decisions may be reviewed by the courts; and that it is led by a board of five members, who are appointed by Parliament from a pool of ten candidates nominated by the Minister through a "transparent meritocratic recruitment procedure".[8] Notably, the 2020 version of the Bill provides some security of tenure[9] and states that the members of the Supervisory Authority should be remunerated "to guarantee financial independence."[10]

16. Comparatively, **sections 6 and 10** of the Bill provide that board members, including the chairperson and vice-chairperson, are appointed by — and may be removed by — the Minister. Additionally, **section 12** provides that the remuneration of the board is to be determined by the Minister, without mention of financial independence, and there are no provisions detailing and safeguarding the security of tenure of board members or specifying timeframes in office. The need for an institutionally independent Supervisory Authority is of paramount importance and it is essential to the proper functioning of a data protection framework. The present Bill substantially reduces this independence, compared to the 2020 version of the Bill, and vests the Minister with ultimate power over the Supervisory Authority as opposed to Parliament.

17. **As a result, Part 2 of the Bill needs to be substantially redrafted in line with the 2020 version of the Bill to ensure that appointments, removals, and the remuneration of board members of the Supervisory Authority are determined by Parliament as opposed to the Minister, and that board members, including the chairperson and the vice-chairperson, are afforded security of tenure and are shielded from undue political influence. Additionally, in appointing board members, Parliament should be directed to seek public nominations before initiating any appointment processes.**

7 While the GDPR is recognised as a model data protection law, national data protection frameworks should be developed cognisant of domestic and cultural contexts, customs, and practices.
8 See section 28(1) of the 2020 version of the Bill.
9 Id at section 29.
10 Id at section 31

The power to sanction

18. The Bill provides insufficient information on precisely how compliance will be monitored and enforced by the Supervisory Authority. More specifically, **sections 4 and 5** detail the Supervisory Authority's powers, duties, and functions which non-exhaustively include: being responsible for investigating contraventions of the Act; consulting with interested parties on the protection of personal data; handling complaints by various stakeholders; monitoring and enforcing compliance through a number of actions; and conducting research and reporting it to the MICT.

19. While these duties and functions are legitimate, the IPPR is concerned that vague and imprecise language has been used particularly with respect to monitoring and enforcement. Although the reality is that monitoring and enforcement will be a case-by-case exercise, the Bill, as it currently stands, does not provide sufficient guidance on how the Supervisory Authority will proactively monitor and enforce compliance. This is not an issue that is unique to Namibia's proposed framework. In South Africa,[11] there has been concern over the Information Regulator (which is South Africa's equivalent of the Supervisory Authority) only intervening where there has been non-compliance.

20. Further, the provisions in the Bill dealing with monitoring and enforcement do not impose any time periods for the Supervisory Authority to fulfil its duties. Notably, the Bill also does not require the Supervisory Authority to educate and empower members of the public on their rights under the Bill.

21. **Resultantly, and at the very least, section 4(h) should be amended to read: "be responsible for investigating contraventions of, and enforcing compliance with, this Act . . .". Additionally, the MICT may consider defining, or providing further clarity on, "the Court" in section 5(1)(h) and including additional enforcement-related provisions within sections 4 and 5 which explicitly empower the Supervisory Authority to issue sanctions, in the form of fines and other administrative penalties, for non-compliance with the Act.**

Offences, penalties, and administrative fines

22. Read with the above, **sections 54 to 71** pertain to enforcement and empower the Supervisory Authority to investigate and "settle" complaints and apply for warrants. However, dissimilar to the 2020 version of the Bill,[12] the Bill is largely silent on explicit criminal and administrative sanctions, including offences, penalties, and administrative fines for non-compliance, save for brief references in, among others, section 52 and in section 73(2)(l) on "matters incidental to the imposition of administrative fines". This is a notable omission from the Bill, which renders its application limited and is unlikely to lead to compliance with it by data controllers.

23. **As a result, a new Part or Chapter — based on Part VIII of the 2020 version of the Bill but developed as necessary — should be included in the Bill which refers directly to offences, penalties, and administrative fines. This Chapter should consolidate the offences and administrative fines referenced in the Bill and:**

    23.1 **Expressly create an offence for any person who hinders, obstructs, or unlawfully influences the Supervisory Authority; who fails to comply with an assessment or enforcement notice; or who obstructs the execution of a warrant, among others.**

    23.2 **Establish criminal penalties for offences which may include fines or imprisonment, or both.**

    23.3 **Create administrative penalties, in the form of fines, which may be issued by the Supervisory Authority for non-compliance with the Act.**

24. These offences, penalties, and administrative fines should be comprehensively and precisely detailed to avoid ambiguity, and should detail the responsible authorities, including the Supervisory Authority.

11 See AfricanLii, 'POPIA: Progress and Problems', 9 June 2021, accessible here.
12 See Part VIII of the 2020 version of the Bill.

Civil liability

25. Another notable omission from the Bill pertains to civil liability. As has been noted:

> "One of the most important accountability mechanisms available to a data subject is civil liability. This allows a data subject to institute legal proceedings against a data controller if the controller violates the law and causes the data subject harm or loss. The data subject can use this legal action to claim a monetary amount from the data controller in damages for the harm or loss they suffered. Such a court action is time-consuming and expensive, and will likely carry significant reputational harm for a data controller.[13]

26. While civil liability may be accommodated elsewhere in Namibian law, contemporary data protection frameworks, including in South Africa, often include reference to civil liability and civil remedies in their data protection legislation, both for the Supervisory Authority and for individuals. **As a result, either in sections 4 and 5 or in a new Part or Chapter, the power of the Supervisory Authority, or an individual, to institute civil action should be prescribed.**

V OVERBROAD "EXCEPTIONS"

General exceptions

27. **Section 43(1)** of the Bill contains nine "exceptions" to the processing of personal data. These exceptions (which must pursue a legitimate purpose and be necessary and proportionate) may relate to the protection of: (a) **national security**; (b) **defence; (c) public safety**; (d) **important economic and financial interests of the State**; (f) the impartiality and independence of the judiciary of Namibia; (g) the prevention, investigation, and prosecution of criminal offences; (h) the execution of criminal penalties; (i) **other essential objectives of general public interest**; or (j) the protection of the data subject or the rights and fundamental freedoms of others. **Notably, section 43(1) does not contain a subsection (e) and section 43(2) refers to a "regulation" in section 43(1), which is unclear and unspecified. The Bill should be amended accordingly.**

28. The IPPR does not contend that exceptions, on the whole, are inherently problematic. However, the IPPR is concerned about the broadness of the exceptions contained in the Bill. In particular, the exceptions listed in **sections 43(1)(a), (c), (d), and (i)** are inherently vague, open to a wide interpretation, and may potentially be misused. Notably, none of the exceptions are defined in the Bill, which may lead to diminished and inconsistent application of the law.

29. **The IPPR recommends that sufficiently detailed regulations should be published in terms of section 43(1) providing clear and precise definitions, objective and adequate safeguards, and further general guidance on the application of the exceptions contained in section 43(1) of the Bill, particularly sections 43(1)(a), (c), (d), and (i). Alternatively and preferably, the Bill itself should be developed to provide further guidance on the exceptions.** Through developing these regulations or developing the Bill, the IPPR takes the view that any exceptions which cannot be reasonably justified should be removed. Ultimately, exceptions should apply in narrowly circumscribed instances and in a manner that promotes progressive democratic constitutionalism.

Exemption for journalistic, literary, or artistic purposes

30. While referencing an exception for communications between legal advisers and clients in **section 67** and general authorisations specified in **section 34**, the Bill does not contain an express exemption, exclusion, or authorisation for journalistic, literary, or artistic purposes, contrary to contemporary trends in data protection legislation which seek to balance and reconcile the right to privacy with the right to freedom of expression.

31. **As a result, an express exemption for journalistic, literary, or artistic purposes should be recognised in the Bill, either in section 34(1)(f) or section 43, and should provide that "The Act does not apply to the processing of personal data solely for the purpose of journalistic, literary, or artistic expression to the extent that such an exclusion is necessary to reconcile, as a matter of public interest, the right to privacy with the right to freedom of expression, including press freedom." (Additionally, an express exemption for processing personal data for academic purposes, with sufficient safeguards, should be considered by MICT.)**

13 Tara Davis, 'Data Protection in Africa: A Look at OGP Member Progress,' August 2021, at page 44, accessible here.

VI EXEMPTION APPLICATIONS

32. **Section 43 does not empower the Supervisory Authority to grant additional "exclusions" or exemptions for the processing of personal data. While this may perceivably fall within the remit of "Codes of Conduct" in sections 44 to 52, an express enabling provision should be included in the Bill within section 43, alternatively a new section 44, to enable the Supervisory Authority to grant an exemption to a responsible party to process personal information if it is in the public interest to do so, and there is a clear benefit to the data subject or a third party that outweighs, to a substantial degree, any interference with the privacy of the data subject or third party that could result from such processing.**

33. Given the fast-moving and unforeseen nature of data protection, the Supervisory Authority should be permitted to grant exemptions, on application from an individual or a data controller, where it is in the public interest to do and where unforeseen instances arise. This may include, for example, retaining (for an extended period) educational and employment data of children (who are permitted to work from age 14 onwards) to assist them in seeking additional educational or employment opportunities.

VII INTERACTION WITH THE INFORMATION COMMISSIONER

34. A potential lack of alignment and harmonisation exists, or may be created, between the mandate of the Supervisory Authority and the mandate of the Office of the Information Commissioner established in terms of the **Access to Information Bill**.[14] The Information Commissioner is mandated to enforce the right of access to information in general contexts, which may include evaluating whether a request for information relating to personal information or data was properly decided. The Supervisory Authority is mandated to enforce data subjects' rights in the context of processing personal data, which may include enforcing the right of a data subject to access personal data about themselves that is held by another partner or to access information about how their personal information has been or is being processed.

35. **As a result, sections should be expressly included in both the Bill and the Access to Information Bill to delineate how the mandates of the Supervisory Authority and the Information Commissioner will interact in order to ensure that both oversight bodies are able to function cohesively and effectively.**

VIII ADDITIONAL MATTERS FOR CONSIDERATION

Breach notifications

36. **Section 1** defines a "personal data breach" as a "breach of security leading to the accidental or unlawful use, destruction, loss, alteration, disclosure of, or access to, personal data transmitted, stored, or otherwise processed". However, outside of this section, it does not again appear in the text of the Bill. **Section 30**, which presumably deals with personal data breaches, is titled "Notification of security compromises", a term which is not defined in section **1. To ensure consistency in the Bill, section 30 should be re-titled or renamed "Personal data breach notifications" to align with the definition of a "personal data breach" in section 1.**

37. Additionally, **a new subsection in section 30 should provide for offences, penalties, and/or administrative fines in the event that a data controller does not provide the required notification of a personal data breach. Alternatively, the suggested new Part or Chapter on offences, penalties, and administrative fines should expressly list a failure to notify a data subject of a personal data breach as an offence warranting a penalty or administrative fine.**

Direct marketing

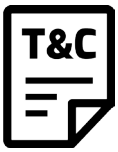
38. The Bill makes limited reference to direct marketing in **section 20(6)** stating that "A data subject may object, at any time, to the processing of personal data for the purposes of direct marketing other than direct marketing by means of unsolicited electronic communication." However, the Bill goes no further. **Unsolicited direct marketing — by any means or form of electronic communication, including automatic calling machines, facsimile machines, SMSs, or e-mail — should be expressly prohibited in the Bill due to its intrusive, unwanted, and non-consensual nature. As a result, a new section should be introduced in the Bill which expressly prohibits unsolicited direct marketing, without consent, and enables the Supervisory Authority to issue administrative fines against responsible parties.**

14 Section 9 of the Access to Information Bill B4-2020.

Terms of service icons

39. In order to foster greater transparency and participation of data subjects, information about the processing of personal data may be disseminated to data subjects through a combination of text and icons, particularly in online spaces such as websites. The effective use of terms of service icons depends on their standardisation and identifiability. Generally, terms of service icons will appear on a website and enable ease of access to terms and conditions, particularly in relation to the processing of personal information.

40. **To foster transparency, section 5(1)(c) of the Bill could include a further subsection stating that "The duties and functions of the [Supervisory] Authority in terms of this Act are to monitor and enforce compliance by prescribing the use of terms of service icons on applicable websites, applications, and other internet-enabled platforms, and providing guidance to controllers on the use of terms of service icons on these platforms."**



Effective functioning of the Supervisory Authority

41. Practically, the Bill establishes the Supervisory Authority in **section 3** and provides in **section 75** that a one-year "grace period" applies following the commencement of the Act. As a result, the Supervisory Authority is expected to be fully operational within one year of the commencement of the Act to ensure that it can monitor and enforce compliance with it. **In order to ensure that the Supervisory Authority is established within the one-year time period stipulated in section 75 of the Bill, practical steps should be taken to fully establish, fund, and staff the Supervisory Authority following the commencement of the Act, including taking pre-emptive measures to ensure that there are no delays with the establishment of the Supervisory Authority following the commencement of the Act.**

IX CONCLUSION

As detailed above, the Bill, in its present form, requires further development to ensure that it meets the requirements of a contemporary data protection framework. Notably, the sections on the independence of the Supervisory Authority need to be reconsidered and substantially redrafted, and sections concerning offences, penalties, and administrative penalties need to be re-introduced and developed, among others. In its present form, the Bill is not fit for purpose.

IPPR remains available to assist and support the MICT as it further develops the Bill, and reaffirms the need to fast-track the Bill given the slow progress in enacting a data protection framework and the inherent need to protect and promote the rights of data subjects in Namibia.

About ALT Advisory

ALT Advisory is a public interest advisory and research firm based in South Africa which questions convention and works for positive change in Africa, and the world. ALT Advisory assists socially responsible organisations with advisory, analysis, research, training, impact, and communications services in the areas of public law and policy, information rights, data privacy, and emergent technology and innovation. ALT Advisory works in association with Power Singh Inc. and ALT Design to provide comprehensive and diversified services to our clients, which includes strategic and test case litigation and communications support.
Since 2017, ALT Advisory has worked in 24 countries, across 5 continents.

About Democracy Report

Democracy Report is a project of the IPPR which analyses and disseminates information relating to the legislative agenda of Namibia's Parliament. The project aims to promote public participation in debates concerning the work of Parliament by publishing regular analyses of legislation and other issues before the National Assembly and the National Council. Democracy Report is funded by the Embassy of Finland. The contents of this briefing paper do not necessarily reflect the views of the Embassy of Finland.

About IPPR

The Institute for Public Policy Research (IPPR) is a not-for-profit organisation with a mission to deliver independent, analytical, critical yet constructive research into social, political and economic issues that affect development in Namibia. The IPPR was established in the belief that free and critical debate informed by quality research promotes development.

Institute for Public Policy Research (IPPR)
House of Democracy
70-72 Frans Indongo Street
PO Box 6566
Windhoek
Namibia
info@ippr.org.na
www.ippr.org.na
Tel: +264 61 240514

Incorporated Association Not for Gain Registration Number 21/2000/468
Directors: M M C Koep (Chairperson), D Motinga, A. Du Pisani, J Ellis, G Hopwood (ex-officio)