

REGULATORY

## Further into Africa...Botswana enacts a “new” Data Protection Act. Does this spell a new dawn?

18 December 2024 6 min read

On 29 October 2024, Botswana’s “new” Data Protection Act 18 of 2024 (“**the new DPA**”) was published in the government gazette and came into effect. Prior to the enactment of the new DPA, a different, less stringent piece of data privacy legislation applied, the Data Protection Act 32 of 2018 (“**the old DPA**”). The new DPA was published as a result of – and in an attempt to address – various shortcomings and inadequacies of the old DPA.

### The new DPA

The new DPA contains various revisions to the old DPA including extending the application of the new DPA to apply to processing activities of data controllers and data processors who are not established in Botswana<sup>[1]</sup> in circumstances where –

- the activities of an establishment of the data controller or data processor are in Botswana irrespective of whether such processing takes place in Botswana; or
- the processing activities relate to the –
  - offering of goods or services to data subjects in Botswana, irrespective of whether payment by a data subject is required; or
  - monitoring of data subjects’ behaviour, insofar as the behaviour takes place within Botswana.

Notably, the above application provision of the new DPA mirrors the application or territorial scope provisions of the General Data Protection Regulation 2016/679 (“**GDPR**”).<sup>[2]</sup>

The new DPA also extends the application of the new DPA to the State of Botswana (“**the State**”) and “*binds the State*”.<sup>[3]</sup> However, it ought to be noted that although the new DPA “*binds the State*”, the DPA does not apply to the processing of personal data by or on behalf of the State where the processing –<sup>[4]</sup>

- involves national security, defence or public safety;
- is for the prevention, investigation or proof of offences, the persecution of offenders or the execution of sentences or security measures;
- is for economic or financial interest, including monetary, budgetary and taxation matters; and
- is for a monitoring, inspection or regulatory function connected with the above.

Consequently, the binding application of the new DPA to the State is internal (or inside) looking meaning that the State must comply with the new DPA insofar as its own operations are concerned subject to the above exceptions. What this means is that the State must implement a data protection governance framework wherein, amongst others, –

- the lawful grounds that the State relies on to process personal data are set out;
- data subjects’ rights are given effect to by the State, particularly the data subject rights of the State’s employees; and
- the data processors that are appointed by the State from time to time are done so in compliance with the new DPA.

The new DPA also contains slightly revised wording and expands (although to a limited degree) on existing data protection principles such as data minimisation, accuracy and storage limitation providing that –

- in relation to **data minimisation**, personal data must be adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed;<sup>[5]</sup>
- in relation to **data accuracy**, personal data must be accurate and, where necessary, kept up to date. The new DPA further provides that a data controller or data processor must take reasonable steps to ensure that personal data that is inaccurate, having regard to the purpose for which it is processed, is erased or rectified without delay;<sup>[6]</sup>
- in relation to **storage limitation**, a data controller or data processor must ensure that personal data is kept in a form which permits the identification of data subjects for no longer than is necessary for the purpose for which the personal data is processed.<sup>[7]</sup>

In relation to administrative fines, the new DPA introduces a percentage (%) based fine, notably of worldwide turnover, for certain contraventions and provides that –<sup>[8]</sup>

- an administrative fine not exceeding P10 000 000, or in the case of an undertaking, not exceeding two per cent of the total worldwide annual turnover of the preceding financial year, whichever is higher, shall apply to a contravention of the obligations of the data controller and data processor under sections 29 (conditions applicable to children in relation to information society services) and 52 (data protection by design and by default);
- an administrative fine not exceeding P50 000 000, or in the case of an undertaking, not exceeding four per cent of the total worldwide annual turnover of the preceding financial year, whichever is higher, shall apply to a contravention of –
  - the basic principles for processing, including conditions for consent;
  - the right of data subjects;
  - the transfers of personal data to a recipient in a third country or an international organisation;
  - any obligations pursuant to law adopted;
  - an order or a temporary or definitive restriction on processing or the suspension of data flows by the Information and Data Protection Commission (“**Commission**”) or failure to provide access; and
  - an order by the Commission.

When the new DPA was still in Bill format, the Vice President of Botswana His Honour Slumber Tsogwane (as he then was) said that –<sup>[9]</sup>

*“the Bill ensured effective data protection that helped to prevent misuse of data by both state and non-state actors, including curbing surveillance and ensuring that data was not used for discriminatory practices, thereby protecting citizens’ rights and freedoms.”*

### Conclusion

In recent years gone by, various African jurisdictions enacted their own data privacy regime. This is a step in the right direction as it reflects a recognition of the importance of data privacy legislation and, importantly, also aligns with the approach adopted by the European Union with the GDPR. Indeed, the data privacy regimes as adopted in these various African countries mirror, to a material degree, the principles contemplated in the GDPR. In particular, countries such as Eswatini, Zambia, South Africa, Zimbabwe, Nigeria, Rwanda, Egypt and others have enacted their own data privacy regimes and, Botswana, by revamping and toughening its data privacy regime, has joined suit.

---

<sup>[1]</sup> See section 4(2) of the new DPA.

<sup>[2]</sup> See Article 3 of the GDPR.

<sup>[3]</sup> See section 5 of the new DPA.

<sup>[4]</sup> See section 4(3) of the new DPA.

<sup>[5]</sup> See section 21 of the new DPA.

<sup>[6]</sup> See section 22 of the new DPA.

<sup>[7]</sup> See section 23 of the new DPA.

<sup>[8]</sup> See section 83 of the new DPA.

<sup>[9]</sup> Please refer to the news article at <https://dailynews.gov.bw/news-detail/81081>, accessed on 18 December 2024.



**Ahmore Burger-Smidt**

Head of Regulatory

[View Profile](#)



**Dale Adams**