DATA PROTECTION LAWS OF THE WORLD

Botswana

BOTSWANA

Last modified 12 January 2023

LAW

The Data Protection Act – Act No. 32 of 2018, (“the DPA”) is an Act which was assented to by Parliament on the 3rd August 2018 and came into effect on the 15th of October 2021.

The DPA regulates the protection of personal data and ensure that the privacy of individuals in relation to their personal data is maintained.

DEFINITIONS

Definition of personal data

Under the DPA, personal data means information relating to an identified or identifiable individual, which the individual can be identified directly or indirectly, in particular by reference to an identification number, or to one or more factors specific to the individual’s physical, physiological, mental, economic, cultural or social identity.

Definition of sensitive personal data

Sensitive Personal Data is defined to mean personal data which reveals a data subject’s:

- racial or ethnic origin;
- political opinions;
- religious beliefs or philosophical beliefs;
- membership of a trade union;
- physical or mental health or condition;
- sexual life;
- filiation; or
- personal financial information,

and includes:

- any commission or alleged commission by him or her of any offence;
- any proceedings for any offence committed or alleged to have been committed by him or her, the disposal of such proceedings, or the sentence of any Court in such proceedings; and
- genetic data, biometric data and the personal data of minors.

NATIONAL DATA PROTECTION AUTHORITY

A body known as the Information and Data Protection Commission (“**the Commission**”) as established under the DPA has been formed and is the designated body tasked with data protection and ensuring the effective application of, and

compliance with the DPA, and in particular, the right to protection of personal data, access rectification, objection and cancellation of such data.

REGISTRATION

The Commission is responsible for creating and maintaining a public register of all data controllers. There is, however, currently no prescribed method of registration.

A data controller is a person who alone or jointly with others determines the purposes and means of which personal data is to be processed, regardless of whether or not such data is processed by such person or agent on that person's behalf. Additionally, a data controller may engage a data processor, being a person who processes data on behalf of the data controller.

In terms of the DPA, data controllers are required to notify the Commissioner of the Commission (“**the Commissioner** ”) before carrying out any wholly or partially automated processing operation or set of such operations which are intended to serve a single purpose or serve several related purposes.

The notification should include the following details:

- The name and address of the data controller or data processor;
- The purpose of the processing;
- A description of the category or categories of a data subject and of the personal data or categories of personal data relating to the data subject;
- The recipients to whom personal data can be disclosed to;
- Proposed transfers of personal data to a third country; and
- A general description to allow the Commission to preliminarily assess the appropriateness of the security measures.

The requirement for notification does not apply to operations which have the sole purpose of keeping a register that is intended to provide information to the public by virtue of any law, and for which the register is open for public inspection. In addition, the notification will not be required where a data controller has appointed a data protection representative.

Data controllers are further required to immediately notify the Commissioner of any breach to the technical or organizational security safeguards for processing of personal data.

The Commissioner has the authority to grant an exemption for notification when satisfied that:

a. The personal data being processed has no apparent risk of infringement to the rights of the data subject;
b. The purposes of the processing, the category of processing, the category of a data subject, the category of a recipient, and the data retention period are specified; and
c. The data controller has appointed a data protection representative, and the Commissioner has been notified of such appointment.

DATA PROTECTION OFFICERS

A data controller has the option to appoint a data protection representative who holds the requisite qualifications, their role being to independently ensure that personal data is processed in a correct and lawful manner, and in accordance with good practice.

The data protection representative is responsible for keeping a list of the processing carried out and the list should be immediately accessible to any person applying for access. Upon identifying any inadequacies, the data protection representative should bring such inadequacies to the attention of the data controller and assist in ensuring that the data subject’s rights under the DPA are protected.

Where a data protection representative has been appointed, the notification to the Commissioner regarding wholly or partially automated processing operations is not required.

If a data protection representative has reason to suspect that the data controller is contravening the rules applicable for processing personal data, and if rectification is not implemented as soon as practicable after the contravention is pointed out, the

data protection representative must then notify the Commissioner.

The appointment and removal of a data protection representative must be notified to the Commissioner.

COLLECTION & PROCESSING

Processing means any operation or a set of operations which is taken in regard to personal data, whether or not it occurs by automatic means, and includes the collection, recording, organization, storage, alteration, retrieval, gathering, use, disclosure by transmission, dissemination or otherwise making information available, alignment, or combination, blocking, erasure or destruction of such data.

Processing personal data

Prior to undertaking the processing of personal data, data controllers are generally required to obtain written consent from the data subjects. Consent is not required in instances authorised by any written law. In addition, a data subject who has given consent for processing of personal data may at any time, in writing, revoke the consent for legitimate, reasonable, and compelling reasons at that particular time.

Alternatively to where written consent is obtained, personal data may further be processed where the processing is necessary for:

- the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject entering into a contract;
- compliance with a legal obligation to which the data controller is subject;
- protecting the vital interests of the data subject;
- performing an activity that is carried out in the public interest or in the exercise of an official authorization vested in the data controller, or of a third party to whom the data is disclosed; or
- a purpose that concerns a legitimate interest of the data controller, or of a third party to whom personal data is provided, except where such interest is overridden by the interest to protect the fundamental rights and freedoms of the data subject and in particular, the right to privacy.

Where personal data is processed for historical, statistical or scientific purposes, the data controller must ensure that there are appropriate security safeguards in place in instances where the personal data may be kept for a period longer than necessary, having regard to the purpose for which it is processed or the personal data kept is not used for any decision concerning the data subject.

In the event that processing is for direct marketing, the data controller must, at no cost, inform the data subject of the right to oppose the processing. Processing for such purposes will be prohibited where the data subject has given a notice of objection to the processing of the personal data. A data controller who processes the data despite the objection made by the data subject commits an offence which is punishable by fine not exceeding BWP500 000 or to imprisonment for a term not exceeding nine years, or to both.

Processing sensitive personal data

Processing sensitive personal data is heavily restricted thereby requiring the data controller to ensure that appropriate security safeguards have been adopted. The processing of sensitive personal data is generally be prohibited save for where:

- the processing is specifically provided for under the DPA;
- the data subject has given consent in writing;
- the data subject has made the data public;
- the processing is necessary for national security, for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment, or where the processing is authorized by any other written law for any reason of substantial interest to the public; or
- the processing is necessary to protect the vital interest of a data subject and another person in a case where consent cannot be given by or on behalf of the data subject, the data controller cannot be reasonably expected to obtain consent

or the consent by or on behalf of the data subject has been unreasonably withheld.

Bodies or entities, not being a commercial bodies or entities, which have political, philosophical, religious or trade union objects are allowed to process sensitive personal data relating to the political, philosophical, religious or trade union objects concerning the members of that body or entity, or any other person who the body or entity regularly exchanges information with. Such processing by an entity or body is allowed if it is done in the course of its legitimate activities and with appropriate guarantees. It should also be noted that this sensitive personal data may be provided to a third party only where the data subject has given written consent.

Furthermore, processing of sensitive personal data for health or medical purposes is allowed where the processing is done by a health professional and is necessary for preventative medicine as well as protection of public health, medical diagnosis, health care or the management of health and hospital care services.

Processing sensitive personal data is also allowed where it is for research, scientific and statistics purposes so long as the processing is compatible with specified, explicitly stated and legitimate purposes. In the case of research and scientific purposes, the Commissioner must have approved the processing on the advice of a committee responsible for research and scientific ethics, whilst in the case of statistics, the processing must be necessary for the purposes provided under the Statistics Act (Cap 17:01).

There is a general prohibition against processing genetic and biometric data for what it reveals or contains. The prohibition does not apply where such data is processed in accordance with the general requirements for processing sensitive personal data as outlined above. Where genetic and biometric data is processed for medicinal purposes and the consent of the data subject has been granted, the processing must only be effected where a unique patient identification number is given to the data subject. This patient number must be different from any other identification number possessed by the data subject.

Sensitive personal data may also be processed for legal purposes where it is necessary in connection with any legal proceedings including prospective proceedings, for the purposes of obtaining legal advice, for establishing, exercising or defending legal rights, or for the administration of justice.

With respect to a data subject’s identity card number, processing in the absence of the data subject’s consent is only allowed where the processing is clearly justifiable having regard to the purpose of the processing, the importance of a secure identification or any valid reason as may be prescribed.

During the processing operation where personal data is obtained directly from the data subject, the data controllers and data processors are required to furnish to the data subject with the following information, except where the data subject already has the information:

- The identity and habitual residence or principal place of business;
- The purpose of the processing;
- The existence of the right to object to the intended processing if the processing is for purposes of direct marketing;
- Any other additional information if it will ensure fair processing, which may include the recipient or category of recipients, whether the reply to any question posed is obligatory or voluntary and the possible consequences of failure to reply as well as the existence of the right to access, rectify, delete the data concerning the data subject; or
- Any other information necessary for the specific nature of the processing, to guarantee fair processing in respect of the data subject.

A person who has access to personal data and is acting under the authorisation of the data controller or the data processor must process personal data only as instructed and without prejudice to any duty or restriction imposed by law. A contravention of this amounts to an offence which is punishable by a fine not exceeding BWP 20,000 or to imprisonment for a term not exceeding one year, or to both.

Where personal data is processed without the required authorisation, such processing amounts to an offence which is punishable by a fine not exceeding BWP 100, 000 or to imprisonment for a term not exceeding three years, or to both.

It is mandatory to safeguard the security of personal data by taking appropriate technical and organisational security measures necessary to protect the personal data from negligent or unauthorised destruction, negligent loss or the alteration, unauthorised

access and any other unauthorised processing of personal data.

When taking appropriate technical and organisational security measures necessary to protect the personal data, the person doing so must ensure an appropriate level of security by taking into account:

- technological developments of processing personal data, and the costs for implementing the security measures; and
- the nature of the personal data to be protected and the potential risks involved.

Additionally, when outsourcing processing of personal data, the data processor to be chosen must be one who gives sufficient guarantees regarding the technical and organisational security measures in place for the processing to be done. The data controller or processer who outsources must ensure that the said measures are complied with.

TRANSFER

The transfer of personal data from Botswana to another country is prohibited save for transborder transfers to countries that have been designated by the Minister through an Order published in the Government Gazette.

Transborder transfers of personal data require prior authorisation to be granted by the Commissioner so as to assess and ensure that adequate levels of protection are provided by the country receiving the personal data. The assessment is in light of all the circumstances surrounding the data transfer operation and particular consideration is given to:

- the nature of the data;
- the purpose and duration of the proposed processing operation;
- the country of origin and the country of final destination;
- the rule of law, both general and sectoral, in force in the third country in question; and
- the professional rules and security safeguards which are complied with in that country.

Notwithstanding the above, transborder transfers to countries which do not offer an adequate level of protection are allowed where the data subject consents to the proposed transfer or, where the transfer is:

- necessary for the performance of a contract between the data subject and the data controller, or the implementation of pre contractual measures taken in response to the data subject’s request;
- necessary for the performance or conclusion of a contract in the interests of the data subject between the data controller and a third party;
- necessary or legally required for the public interest, or for the establishment, exercise or defence of a legal claim;
- necessary to protect the vital interests of the data subject; or
- made from a register that is intended to provide the public with information and is open to public inspection.

Regardless of the above mentioned restrictions, transborder flow of personal data to a country without adequate levels of protection may be authorised where consent is obtained from the data subject and the data controller provides adequate safeguards which may be by means of appropriate contractual provisions, with respect to the protection of the privacy and fundamental rights and freedoms of individuals.

Currently, personal data may be freely transferred to the following countries:

1. Austria
2. Belgium
3. Bulgaria
4. Croatia
5. Cyprus
6. Czech Republic
7. Denmark
8. Estonia
9. Finland
10. France

11. Germany
12. Greece
13. Hungary
14. Ireland
15. Italy
16. Latvia
17. Lithuania
18. Luxembourg
19. Malta
20. Netherlands
21. Poland
22. Portugal
23. Romania
24. Slovakia
25. Spain
26. Slovenia
27. Sweden
28. Norway
29. Liechtenstein
30. Iceland
31. The United Kingdom
32. New Zealand
33. Israel
34. Japan
35. Isle of Man
36. Guernsey
37. Switzerland
38. Uruguay
39. Republic of Korea
40. Andorra
41. Argentina
42. Foroe Islands
43. Jersey
44. South Africa
45. Kenya

SECURITY

Data controllers are required to take appropriate technical and organisational security measures necessary to protect personal data from negligent or unauthorised destruction, negligent loss, as well as unauthorised access, alteration and processing of personal data.

The measures are influenced by technological developments of processing personal data and the costs for implementing the security measures, as well as the nature of the personal data and the potential risks involved.

Failure to implement the security safeguards amounts to an offence and will render the data controller liable to a fine not exceeding BWP 500 000 or to imprisonment for a term not exceeding nine years, or to both.

BREACH NOTIFICATION

Data controllers and data processors are required to immediately notify the Commissioner of any breach to the security safeguards of personal data. A failure to do so amounts to an offence punishable by a fine not exceeding BWP 100 000 or to imprisonment for a term not exceeding three years, or to both.

ENFORCEMENT

As mentioned earlier, the Commission is the competent authority that is tasked with protection of personal data through effective application and compliance with the DPA.

ELECTRONIC MARKETING

Marketing by means of electronic communication is governed by the Electronic Communications and Transactions Act – Act No 14 of 2014 (“**ECTA**”).

An originator, who carries out marketing by means of electronic communication must provide the addressee with the originators’ identity and contact details including the place of business, e-mail, addresses and telefax number, as well as a valid and operational opt-out facility from receiving similar communications in future, and additionally, the identifying particulars of the source from which the originator obtained the addressee’s personal information.

In terms of the ECTA, unsolicited commercial communication must only be sent where the opt in requirement has been met and this includes:

- the addressee’s email address and other personal information was collected by the originator of the message in the course of a sale or negotiations for a sale;
- the marketing relates to similar products or services;
- when the personal information and address was collected by the originator, the originator offered the addressee the opportunity to opt-out, free of charge except for the cost of transmission, and the addressee declined to opt- out; and
- the opportunity to opt-out is provided with every subsequent message.

Failure to provide the addressee with an optional opt-out facility is an offence which is punishable by a fine not exceeding BWP 10 000, or to imprisonment for a term not exceeding five years, or to both. Furthermore, an originator who persists in sending unsolicited commercial communications to an addressee who has opted-out from receiving such through the originator’s opt out facility commits an offence and is liable to a fine not exceeding BWP 50 000, or to imprisonment for a term not exceeding eight years, or to both.

Also noteworthy is the DPA requirement that where personal data is processed for direct marketing purposes, the data controller must, at no cost, inform the data subject of the right to oppose the processing. Processing for such purposes will be prohibited where the data subject has given a notice of objection to the processing of the personal data. A data controller who processes the data despite the objection made by the data subject, commits an offence which is punishable by fine not exceeding BWP 500 000 or to imprisonment for a term not exceeding nine years, or to both.

ONLINE PRIVACY

There is currently no specific online privacy legislation and no provision in the DPA and the ECTA regarding such.

KEY CONTACTS

Minchin & Kelly (Botswana)

Isaac Ntombela
Partner
Minchin & Kelly (Botswana)
T +267 391 2734
intombela@minchinkelly.bw

Namie Modiri
Associate
Minchin & Kelly (Botswana)
T +267 391 2734
nmodiri@minchinkelly.bw

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.