FACTSHEET: BOTSWANA

Last updated: 31 March 2020
Prepared by Justin Bryant
Revised by Tshepiso Hadebe

FAST FACTS

Population: 2,336,621
Capital: Gaborone
President: Mokgweetsi Masisi
2019 Freedom House Score: 72/100
Data protection law? Exists, not enforced

LAW

The Data Protection Act 2018 (DPA) was assented to by the Botswanan Parliament in order to realise the right to privacy guaranteed in the Constitution.

The Information and Data Protection Commission (Commission), which has not yet been formed, is established under this law. It is not an independent body, but under the direction of the Minister, to whom the members of the Commission must swear an oath of secrecy.

Data subjects have the following rights under the DPA:

- the right to access personal data through subject access requests;
- the right to obtain a copy of the personal data held by a data processor or a data controller;
- the right to object, for legitimate reasons, to the processing of personal data concerning them;
- the right to oppose the processing of their personal data for direct marketing; and
- the right to correct, update, lock, or delete personal data where it is inaccurate or incomplete.

PERSONAL DATA

Personal data is information related to an individual who can be identified directly or indirectly by reference to an identification number, or to one or more factors specific to his, her or their physical, physiological, mental, economic, cultural, or social identity.

Sensitive data processing is prohibited barring certain exceptions. It is defined as personal data relating to a data subject that reveals any of the following:

- racial or ethnic origin;
- political opinions;
- philosophical or religious beliefs;
- trade union membership;
- physical or mental health or condition;
- sexual life;
- filiation;
- personal financial information;
- health;
- any commission or alleged commission by him, her or they of an offence;
- judicial proceedings, or criminal or administrative sanctions; or
- genetic data, biometric data, and the personal data of minors.

COLLECTION AND PROCESSING

Data controllers must ensure that personal data is:

- processed fairly, lawfully, and where appropriate, the data is obtained with the knowledge or consent of the data subject;
- adequate and relevant in relation to the purposes of its processing;
- accurate, complete, and updated to the extent necessary for processing;
- collected for specific, explicitly stated, and legitimate purposes;
- not processed for other purposes incompatible with those aforementioned;
- protected by reasonable security safeguards against risks such as loss, unauthorised access, destruction, use, modification, or disclosure;
- made complete, corrected, blocked, or deleted if it is incomplete or incorrect, taking into account the purposes of processing;
- kept for no longer than necessary regarding the purposes for which it is processed; and
- processed in accordance with good practice.

Personal data may be processed where:

- there is written consent from the data subject;
- processing is necessary to commence or perform of a contract in the data subject's interests or to which he is a party;
- processing is necessary for compliance with a legal obligation to which the data controller is subject;
- processing is necessary for the performance of a public interest activity or the exercise of official authority vested in the data controller or in a third-party recipient of the data; or
- processing is necessary to advance the legitimate interest of the data controller or a third-party recipient of the data, unless this interest is overridden by the interest in protecting the fundamental rights and freedoms of the data subject, particularly the right to privacy.

REGISTRATION AND ENFORCEMENT

The Commission is established as a public office, and shall:

- ensure compliance with the provisions of the Statistics Act when statistical data is being collected and statistical secrecy is necessary;
- instruct data controllers to take necessary measures to comply with the DPA;
- provide guidance and instructions on appropriate measures to ensure the security of personal data;
- provide information to persons about their rights connected to the processing of personal data;
- receive reports and claims from data subjects about violations of the DPA and take any necessary remedial action;
- investigate and respond to complaints from data subjects;
- authorise the cross-border flow of personal data and facilitate international cooperation on personal data protection;
- create and maintain a public register of all data controllers;
- obtain information from data controllers necessary for the exercise of the functions of the Commission;
- prepare and disseminate a code of practice for data controllers;

- issue, where applicable, enforcement notices and instructions required to bring processing operations in line with the principles of the DPA;
- publicise the existence of personal data files, and regularly publish a list of such files, and any other information that the Commission deems necessary;
- record all directions received from the Minister in the course of the year; and
- perform any other functions that may be conferred on it by the Minister.

Data controllers may appoint a data protection representative to ensure compliance with the DPA and good processing practices. The Commissioner should be notified of such an appointment, which will exempt a data controller from notifying the Commissioner before processing personal data except in special circumstances.

Various offences are articulated under the DPA which carry certain penalties. Data subjects can also file actions for damages against data processors who violate their rights under the DPA.

CROSS-BORDER TRANSFER

Transfer of personal data to another country is prohibited unless that country provides an adequate level of protection, which will be determined by the Commissioner.

SECURITY AND BREACH PROTOCOL

A data controller must notify the Commissioner of any breach to the security safeguards of personal data, without delay.

A data processor must, without delay, notify a data controller of any breach to the security safeguards of personal data held on behalf of the data controller.

Violating these requirements constitutes an offence punishable by a fine of up to P100,000, a prison sentence of up to three years, or both.

Read the legal notice and terms of use for this factsheet.