FACTSHEET: LESOTHO

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

FAST FACTS

Population: 2,136,821
Capital: Maseru
President: Tom Thabane
2019 Freedom House Score: 63/100
Data protection law? Exists, not enforced

LAW

Lesotho's constitution protects the right to privacy, and in 2012, the Data Protection Act, 2011 (the Act) became law, after being published in the Lesotho Government Gazette as Act, No. 5 of 2012. The Act attempts to bring Lesotho into compliance with EU standards and to reflect the South African Development Community (SADC) data protection standards.

Lesotho's Data Protection Commission (Commission) has not yet been appointed to enforce the Act, and when it is appointed, the body will have considerably less enforcement power than analogous bodies in other jurisdictions given its stipulated powers in the Act (such as its lack of ability to impose fines on entities that violate the Act). Also, the law does not explicitly state that the Commission is independent, which potentially leaves it open to undue influence from the Prime Minister.

Under the Act, data subjects have the right to:

- have their personal data corrected;
- access their personal data;
- prevent the processing of personal data that causes or is likely to cause them unwarranted damage or distress;
- prevent processing of personal data for purposes of direct marketing;
- not be subject to a decision by a data controller that would significantly affect them or have adverse legal repercussions if the decision was solely based on automatic processing; and
- correct or delete personal data when it is inaccurate.

PERSONAL DATA

Personal information is information about an identifiable individual in recorded form, such as:

- information relating to race, national or ethnic origin, religion, age or marital status;
- information relating to education level, or medical, criminal or employment history;
- information relating to financial transactions;
- any identifying number, symbol or other particular assigned to the individual;
- an address, fingerprints, or blood type;

- an individual's name alongside other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual;
- correspondence sent to a data controller by the individual that is explicitly or implicitly private or confidential, and replies to such correspondence that would reveal the contents of the original correspondence; and
- the views or opinions of any other person about the individual.

Sensitive personal information may not be processed unless specifically permitted under the Act or covered by an exemption. This category includes:

- genetic data;
- data related to children;
- data related to offenses, criminal sentences, or security measures;
- biometric data;
- personal information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, affiliation, trade-union membership, gender, and data concerning health or sex life (if they are processed for what they reveal); and
- any personal information otherwise considered by Lesotho law as presenting a major risk to the rights and interests of the data subject, in particular unlawful or arbitrary discrimination.

COLLECTION AND PROCESSING

Personal information processing shall abide by the following principles:

- ***Purpose specification and further processing limitation:*** collection of personal data is required to be for a specified, explicit and legitimate purpose and not to be further processed in a way incompatible with those purposes.
- ***Minimality:*** processing of personal data is required to adequate, relevant and not excessive.
- ***Data retention:*** records of personal data shall not be retained any longer than is necessary.
- ***Information security:*** data controllers are required to secure the integrity of personal data against loss, damage, unauthorised destruction, and unlawful access.
- ***Quality of information:*** personal information collected must be complete, not misleading and kept up to date, where necessary.
- ***Automated processing control:*** processing of personal information solely based on automated means is prohibited except under conditions provided in the Act.

Personal information processing shall be automated,* processed, and kept in:

- a filing cabinet; and
- electronic form.

Personal information shall be processed given one of the following:

- the data subject explicitly consents to the processing;
- processing is necessary for the conclusion or performance of a contract to which the data subject is a party;

- processing is necessary for compliance with a legal obligation to which the data controller is subject;
- processing is necessary to protect the legitimate interests of the data subject;
- processing is necessary for the proper performance of a public law duty by a public body; or
- processing is necessary for pursuing the legitimate interests of the data controller or of a third party to whom the information is supplied.

** By requiring data processing to be automated as a general condition for processing, it narrows the scope of the Act, which extends to manual processing of personal data as well. The overall effect of this limitation is to make the Act weaker by default unless the Commission or courts decide to take a broader approach.*

REGISTRATION AND ENFORCEMENT

Some of the major responsibilities of the Commission include:

- educating and increasing and public awareness and acceptance of information protection principles;
- monitoring and enforcing compliance with the Act by public and private bodies;
- researching and monitoring developments in information processing and technology to mitigate adverse effects on data subjects;
- conducting personal information policy reviews, and reporting to the Minister or Parliament;
- auditing data controllers to ascertain whether they are complying with the Act;
- consulting and cooperating with people and bodies concerned with protection of personal information;
- receiving, investigating, and resolving complaints through mediation and reconciliation on alleged violations of this Act;
- reporting to Parliament on whether Lesotho should accept certain international instruments relating to the protection of personal information; and
- making guidelines to assist public or private bodies to develop and apply codes of conduct.

A data controller must only process personal information upon notification to the Commission, and the head of a data controller must designate, by order, one or more officers or employees to be data protection officers of that data controller to oversee its obligations under the Act.

CROSS-BORDER TRANSFER

The Act allows personal information to be transferred to recipients in a member state that has adopted the SADC data protection requirements if:

- the recipient demonstrates that the data is necessary for a task carried out in the public interest or pursuant to the lawful functions of a data controller; or
- the recipient demonstrates a need for the transfer and there is no reason to assume that the data subject's interests would be prejudiced by the transfer or processing in the member state.

In either scenario, the data controller must make a provisional evaluation of the necessity for the transfer, and the recipient must ensure that the necessity can be subsequently verified. The data controller must ensure that the recipient processes the personal information only for the specified purposes.

Personal information may only be transferred to recipients outside of the SADC if an adequate level of protection is ensured in the recipient's country, and the data is transferred solely to permit processing otherwise authorised by the controller.

SECURITY AND BREACH PROTOCOL

In the event that the personal data of a data subject is believed to have been accessed or acquired by any unauthorised person, the data controller or authorised third party must notify the Commission and the data subject as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the breach and to restore the integrity of the system.

The data controller shall delay notification to the data subject where the Lesotho Mounted Police Service, the National Security Service or the Commission determines that notification will impede a criminal investigation.

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