DATA PROTECTION LAWS OF THE WORLD

Lesotho

DLA PIPER

LESOTHO

Last modified 20 December 2021

LAW

The right to privacy is recognized and protected under the Constitution of the Kingdom of Lesotho.

Lesotho has established a Data Protection Act, 2013 (the DP Act). The DP Act provides principles for the regulation of the processing of any personal information in order to protect and reconcile the fundamental and competing values of personal information privacy.

DEFINITIONS

Definition of personal data

The DP Act defines personal data or information as being information about an identifiable individual that is recorded in any form, including:

- Information relating to the race, national or ethnic origin, religion, age or marital status of the individual
- Information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved
- Any identifying number, symbol or other particular assigned to the individual
- The address, fingerprints or blood type of the individual
- The name of the individual where it appears with 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 of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence
- The views or opinions of any other person about the individual

Definition of sensitive personal data

The DP Act defines sensitive personal information as any of the following:

- Genetic data, data related to children, data related to offenses, criminal sentences or security measure, biometric data as well as, if they are processed for what they reveal, 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
- 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.

Section 29 prohibits a data controller from processing sensitive personal information, unless specifically permitted under the DP Act.

Section 36 contains general exemptions to the prohibition on processing sensitive personal information. These include instances where:

- Processing is carried out with prior parental consent where the data subject is a child and is subject to parental control in terms of the law
- The processing is necessary for the establishment, exercise or defense of a right or obligation in law
- Processing is necessary to comply with an obligation of international public law
- The Commission has granted authority in terms of section 37 for processing in the public interest, and appropriate guarantees have been put in place in law to protect the data subject's privacy
- Processing is carried out with the consent of the data subject
- The information has deliberately been made public by the data subject

NATIONAL DATA PROTECTION AUTHORITY

The Data Protection Commission (Commission).

Part 2 of the DP Act provides for the establishment of a Data Protection Commission, an independent and administrative authority established to have oversight and control over the DP Act and the respective rights of information privacy.

The powers and duties of the Commission are set out in section 8 of the DP Act.

REGISTRATION

The DP Act (section 25(5)) requires that a data controller process personal information only upon notification to the Commission.

DATA PROTECTION OFFICERS

The DP Act (section 58) authorizes the head of a data controller to designate, by order, one or more officers or employees to be Data Protection Officers of that controller. In terms of that order, the Data Protection Officers may exercise, discharge or perform any of the power, duties or functions of the head of the data controller under this Act.

COLLECTION & PROCESSING

The DP Act defines processing as an operation or activity or any set of operations, whether or not by automatic means relating to any of the following:

- The collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation or use
- Dissemination by means of transmission, distribution or making available in any other form
- Merging, linking, as well as blocking, degradation, erasure, or destruction, of information

Under the DP Act (section 15(2)), personal information may only be processed where one of the following applies:

- The data subject provides explicit consent 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 public law duty by a public body
- Processing is necessary for pursuing the legitimate interests of the data controller or of a third party to whom the information is supplied

Regarding the collection of data, the DP Act requires that a person shall collect personal information directly from the data subject, except where:

- The information is contained in a public record or has deliberately been made public by the data subject
- The data subject has consented to the collection of the information from another source
- Collection of the information from another source would not prejudice a legitimate interest of the data subject
- Collection of the information from another source is necessary:
    - To avoid prejudice to the maintenance or enforcement of the law and order
    - For the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated
    - In the legitimate interests of national security
    - To maintain the legitimate interests of the data controller or of a third party to whom the information is supplied
- Compliance would prejudice a lawful purpose of the collection
- Compliance is not reasonably practicable in the circumstances of the particular case

TRANSFER

The DP Act distinguishes between the transfer of personal information to a recipient in a Member State of the South African Development Community (SADC) that has transposed the SADC data protection requirements and the transfer of personal information to a Member state that has not transposed the SADC data protection requirements or to a non-Member State.

Personal information shall only be transferred to recipients in a Member State that has transposed the SADC data protection requirements:

- Where the recipient establishes that the data is necessary for the performance of a task carried out in the public interest or pursuant to the lawful functions of a data controller, or
- Where the recipient establishes the necessity of having the data transferred and there is no reason to assume that the data subject's legitimate interests might be prejudiced by the transfer or the processing in the Member State

Further to the above, the DP Act requires that the controller make a provisional evaluation of the necessity for the transfer of the data. The recipient shall ensure that the necessity for the transfer of the data can be subsequently verified. The data controller shall ensure that the recipient shall process the personal information only for the purposes for which they were transferred.

Personal information may only be transferred to recipients, not SADC Member States subject to national law adopted pursuant to the SADC data protection requirements, if an adequate level of protection is ensured in the country of the recipient and the data is transferred solely to permit processing otherwise authorized to be undertaken by the controller.

The adequacy of the level of protection afforded by the relevant third country in question shall be assessed in the light of all the

circumstances surrounding the relevant data transfer(s), particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing, the recipient's country, the relevant laws in force in the third country and the professional rules and security measures which are complied with in that recipient's country.

SECURITY

The DP Act regulates security measures on integrity of personal information processed by a data controller and security measures regarding information processed by an agent.

The DP Act (section 20) gives the data controller the duty to secure the integrity of personal information in its possession by taking appropriate measures to prevent the loss, damage to or unauthorised destruction of personal information and prevent the unlawful access to or processing of personal information. In order to give effect to this, the data controller should take the following reasonable measures:

- Identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;
- Establish and maintain appropriate safeguards against the identified risks;
- Regularly verify that the safeguards are effectively implemented; and
- Ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

The DP Act (section 21) states that any personal information processed by an agent should only be done with the knowledge and authorization of the data controller. Secondly the personal information should be treated as confidential unless the law or the performance of their duties requires disclosure. The following security measures are in place for information processed by an agent:

- A data controller should ensure that the agent processing the personal information establishes and maintains the security measures referred to in the DP Act.
- A written contract between the data controller and agent governs the processing of personal information by the agent.
- If the agent is not domiciled or does not have its principal place of business in Lesotho, the data controller should take reasonable steps to ensure that the agent complies with the laws relating to the protection of personal information of the territory in which the agent is domiciled.

BREACH NOTIFICATION

Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by an authorized person, the data controller, or any other third party processing personal information under the authority of a data controller, shall notify:

- The Commission, and
- The data subject, unless the identity of such data subject cannot be established

The notification shall be made 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 compromise and to restore the integrity of the data controller's information system.

The data controller, in terms of section 23(3), 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.

The breach notification to a data subject shall be in writing and communicated to the data subject in one of the following ways:

- Mailed to the data subject's last known physical or postal address
- Sent by email to the data subject's last known email address
- Placed in a prominent position on the website of the party responsible for notification

- Published in the news media
- As may be directed by the commission

The notification is required to provide sufficient information to allow the data subject to take protective measures against potential consequences of the compromise, including, if known to the data controller, the identity of the unauthorized person who may have accessed or acquired the personal information.

Mandatory breach notification

See above.

ENFORCEMENT

The Commission is responsible for the enforcement of the DP Act.

The DP Act (section 49) also permits a data subject to institute a civil action for damages in a court having jurisdiction against a data controller for breach of any provision of this Act.

ELECTRONIC MARKETING

Under section 50 of the DP Act, direct marketing is defined in as a communication by whatever means of any advertising or marketing material which is directed to particular data subjects.

A data subject is entitled any time to require the data controller to cease, or not to begin, processing of personal data in respect of which he is the data subject for the purposes of direct marketing.

ONLINE PRIVACY

There are no sections of the DP Act which regulate privacy in relation to cookies and location data. These issues may be dealt with in future regulations, which the DP Act permits the Minister to make on the recommendations of the Commission.

KEY CONTACTS

Monique Jefferson
Director
T +27 11 302 0853
monique.jefferson@dlapiper.com

DATA PRIVACY TOOL

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