FACTSHEET: TOGOLESE REPUBLIC

Last updated: 31 March 2020
Prepared by Tshepiso Hadebe

FAST FACTS

Population: 7,798 Million
Capital: Lomé
President: Faure Gnassingbe
2019 Freedom House Score: 43/100
Data protection law? Exists

Disclaimer
The Law No. 2019-014 is only available in French. For the purposes of compiling this factsheet reference was made to a translated version of the law and a publication by One Trust Data Guidance. The factsheet will be updated as soon as the English version of the law is available.

LAW

Law No. 2019-014 (DPA Law) relating to the protection of personal data was published on the 29 October 2019. The DPA Law currently only available in French. It regulates the collection, processing, transmission, storage and use of personal data. It applies to natural persons, the state, local authorities, legal entities governed by public or private law, as well as automated or non-automated processing of data carried out in territory of Togo or in any jurisdiction where Togolese Law applies.

Under the DPA Law, data subjects' rights include the:

- right to information;
- right to access information;
- right to object;
- right to rectification and deletion of personal data; and
- right to erasure.

PERSONAL DATA

Personal data refers to any information relating to an identified or identifiable natural person directly or indirectly, by reference to one or more identification elements, specific to his physical, physiological, genetic, psychic, cultural, social or economic identity.

Personal data includes, but is not limited to:

- Genetic data – any data concerning the hereditary characteristics of an individual or groups of individuals who are related.

- Sensitive data – all personal data relating to racial or ethnic origin, opinions or religious affiliations, political activities, union, sex life, health, prosecution and criminal or administrative sanctions.
- Health data – any information concerning the physical and mental state of a person concerned, including genetic data.

COLLECTION AND PROCESSING

The DPA Law sets out basic principles that govern treatment of personal data:

- The principle of consent and legitimacy, which includes:
  - The processing of personal data is considered legitimate if the data subject gives his consent.
  - However, this requirement may be waived when the treatment is necessary for:
    - compliance with a legal obligation;
    - the execution of a public interest;
    - the performance of a contract to which the person concerned is a party or the execution of pre-contractual measures taken at his request; or
    - to safeguard the interest or fundamental rights and freedoms of the data subject.
- The principle of lawfulness and loyalty:
  - The collection, recording, processing, storage and transmission of personal data must take place lawfully, fairly and not fraudulently.
- The principle of purpose, relevance and conservation:
  - The data must be collected for a specific purpose and cannot be processed later in a manner incompatible with this purpose.
  - The processing of data must be adequate, relevant and not excessive with regard to the purpose for which it was collected.
  - The data must be kept for a period that does not exceed the period necessary for the purpose for which the data was collected or processed. Beyond this period data cannot be subject to conservation.
- The principle of accuracy:
  - The data collected must be accurate and if necessary must be updated.
  - All reasonable steps must be taken so that the inaccurate or incomplete data, with regard to the purpose for which it is collected and processed, is deleted or corrected.
- The principle of confidentiality and security
  - Personal data must be processed in a confidential and protected manner in accordance with the provisions of the Law.
- The principle of transparency:
  - The party responsible for processing the data must inform the data subject of any processing of their personal data.
- The principle of choosing the subcontractor:
  - When any processing is carried out on behalf of the person responsible for the processing they must choose a sub-contractor which provides sufficient guarantees of compliance with security measures defined by the Law.
  - The sub-contracting must be governed by a contract which provides in particular that the sub-contractor acts on the sole instruction of the person in charge of the processing.
- The principle of prohibition:

- It is prohibited to carry out the collection and any processing which reveal racial, ethnic origin, parentage, political opinions, religious or philosophical convictions, union membership, sex life, genetic data and data relating to the health condition of the data subject concerned.
- The prohibition is not applicable when:
  - the processing of personal data carries on data manifestly made public by the data subject; the data subject has given his consent;
  - the processing of personal data is necessary to safeguard the vital interests of the person concerned or another person in case the person concerned is incapacitated;
  - the processing is necessary for the observation and the exercise or the defence of a legal claim;
  - legal proceedings or criminal investigation is opened;
  - the processing of personal data proves necessary for a reason of public interest, for historical purposes, scientific or cultural statistics;
  - processing is necessary for the performance of a contract to which the person concerned is a party or to the execution of pre- contractual measures taken at the request of the data subject;
  - the processing is necessary to comply with an obligation that the data controller has; or
  - the processing is necessary for the performance of an assignment in the public interest or s carried out by a public authority.

REGISTRATION AND ENFORCEMENT

The DPA Law establishes the Personal Data Protection Authority (PDPA), an independent administrative authority responsible for ensuring that the processing of personal data is done in accordance with the of the DPA Law. The PDPA is empowered to issue a warning to a data controller if it does not comply with the obligations set out in the DPA Law and to issue a formal notice to the controller to put an end to any breaches concerned within the set time limits.

Before they can collect or process any data, all data controllers and processors must file requests for opinions, declarations and requests for authorisation with the PDPA. If the controller does not comply to the formal notice addressed to him, the Authority can pronounce against him the following sanctions:

- a temporary withdrawal of authorization granted for a period of 3 months at the end of which if corrective measures are not taken, the withdrawal becomes final; or
- a fine not exceeding one hundred million CFA francs.

CROSS-BORDER TRANSFER

The controller cannot transfer personal data to a third country unless that state ensures an adequate level of protection of life, privacy, fundamental rights and freedoms of individuals with regard to the processing of the data. Before any transfer of personal data to a third country is undertaken the controller must first inform the PDPA.

SECURITY AND BREACH PROTOCOL

The DPA Law does not specify any security and breach protocol.

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