FACTSHEET: CAPE VERDE

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

FAST FACTS

Population: 554,035
Capital: Praia
President: Jorge Carlos Fonseca
2019 Freedom House Score: 90/100
Data protection law? Enforced

LAW

Cape Verde provides individuals with several constitutional and statutory rights to personal data protection. Major provisions in the data protection laws are effectively reproduced in the Constitution, which provides an additional layer of legitimacy. The constitutional right of *habeas data* grants the right to a citizen request, update or even to destruct any personal data, and Law No. 109 articulates the conditions by which a party may bring a *habeas data* case.

Law No. 133, passed in 2001, was Cape Verde's original data protection law. It closely mirrored European data protection laws at the time, as Cape Verde's legal system largely draws from that of the Portuguese. Law No. 41 was passed in 2013 to supplement and update Law No. 133, and Law No. 42 was subsequently passed to detail the responsibilities of the Cape Verdean data protection authority, known as the *Comissão Nacional de Proteção de Dados Pessoais* (CNPD).

Under Cape Verdean law, an individual has the right to:

- be informed by any data controller if he holds personal data about that individual;
- access and know how personal data concerning them is being processed;
- object, for legitimate reasons, to the processing of personal data concerning them;
- oppose the processing of their personal data for marketing or advertising;
- have a data controller correct, supplement, update, lock, or delete personal data concerning them, if the data is inaccurate, incomplete, equivocal or out of date, or if its collection, use, communication, or conservation is prohibited; and
- not be subject to a decision made on the sole basis of an automated processing that would produce adverse legal ramifications for them.

PERSONAL DATA

Personal data is any information, regardless of its nature or the media on which it is stored, relating to an identifiable natural person.

Sensitive data is personal data about an individual's:

- philosophical or political convictions;
- party or union affiliation;
- religious faith;
- private life;
- ethnic origin;
- health;
- sex life; or
- genetic information.

COLLECTION AND PROCESSING

Personal data processing may only occur if there is consent from the data subject or if processing is necessary for:

- compliance with a legal obligation to which the controller is subject;
- the performance of a public interest mission or the exercise of public authority;
- the commencement or performance of a contract in the data subject's interests or to which he is a party;
- safeguarding the interests or fundamental rights and freedoms of the data subject; or
- the pursuit of legitimate interests of the controller or third-party data processor, provided these interests preserve the fundamental rights and freedoms of the data subject.

Personal data must be:

- processed legally, lawfully, and abiding by the principle of good faith;
- collected for specific, explicit, and legitimate purposes and may not be further processed in any manner incompatible with these purposes;
- adequate, relevant, and not excessive relative to those purposes in terms of collection and further processing;
- accurate and updated, if necessary;
- stored in such a way that allows for the identification of data subjects only for the period necessary for the purposes for which the data was collected or processed; and
- treated confidentially and be adequately protected, in particular where the processing includes data transmissions in a network.

Interconnection of personal data shall:

- be limited to what is necessary and appropriate to the pursuit of legal or statutory purposes and legitimate interests of those processing;
- not discriminate against or infringe on the fundamental rights, freedoms, and guarantees of holders of the data; and
- ensure the use of appropriate safety measures.

REGISTRATION AND ENFORCEMENT

Law No. 42 establishes the CNPD as an independent administrative authority responsible for enforcing the data protection laws of Cape Verde. The body is given:

- investigative powers, and may have access to data undergoing processing and can collect all the information necessary for the performance of its supervisory duties;

- powers of authority, particularly those of ordering the blocking, erasure, or destruction of data, or imposing a temporary or permanent ban on the processing of personal data anywhere on Cape Verdean territory;
- the power to give opinions before processing is carried out and to ensure their publication; and
- the power to apply sanctions and fines on data controllers who violate data protection laws.

Law No. 41 sets out obligations for data controllers to notify the CNPD before processing personal data, and mandates that each data controller appoint a data protection officer responsible for managing compliance with the law. Refusal to cooperate with provisions of the law or otherwise comply with the instructions of the CNPD may result in the commission of one of several offences under Law No. 41 that carry fines or terms of imprisonment.

CROSS-BORDER TRANSFER

The transfer of personal data outside of Cape Verde may be carried out with respect to the provisions of applicable domestic data protection law and is only permissible if the foreign country ensures an adequate level of protection.

The transfer of personal data to a country which does not ensure an adequate level of protection may be permitted by CNPD if the data subject has given consent to the transfer or whether such transfer is:

- necessary for the commencement or performance of a contract between the data subject and the data controller, or at the data subject's request;
- necessary for the execution or conclusion of a contract awarded or to be granted, in the interest of the data subject, or between the data controller and a third party;
- required for the protection of an important public interest, or for the declaration, exercise, or defence of a right in judicial proceedings;
- necessary to protect vital interests of the data subject; or
- made from a public register open to consultation with the general public or anyone who proves a legitimate interest, provided that that the conditions laid down by law for the consultation are met in the particular case.

SECURITY AND BREACH PROTOCOL

Data controllers must implement proper technical and organisational measures, taking into account the risk of processing and the nature of the data being handled, to ensure the data is safe from destruction, loss, alteration, or unauthorised dissemination or access. The data controller must also contractually enforce these obligations on the data processor. There are no legal requirements mandating breach notification.

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