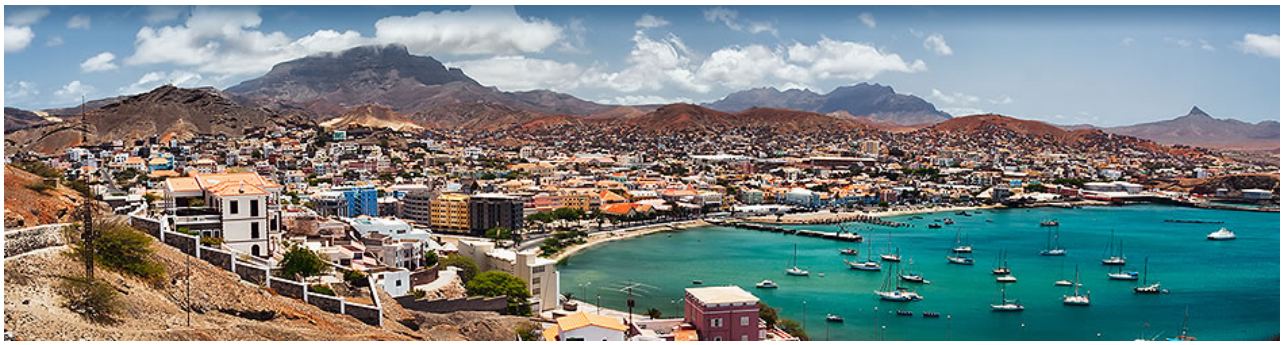
DATA PROTECTION LAWS OF THE WORLD

Cape Verde

CAPE VERDE



Last modified 8 January 2022

LAW

Data Protection Law (Law 133/V/2001 (as amended by Law 41/VIII/2013, Law 121/IX/2021 of 17 March 2021) and Law 132/V /2001, of 22 January 2001.

DEFINITIONS

Definition of personal data

Personal data is defined as any information, regardless of its nature or the media on which it is stored, relating to an identifiable natural person (referred to as 'the data subject'). Natural persons are deemed to be identifiable whenever they can be directly or indirectly identified through such information.

Definition of sensitive personal data

Sensitive data is defined as personal data that refers to a person’s:

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

NATIONAL DATA PROTECTION AUTHORITY

The national data protection authority in Cape Verde is the *Comissão Nacional de Proteção de Dados Pessoais* ('data protection authority').

REGISTRATION

Pursuant to the Data Protection Law, before starting the processing of personal data (and considering the specific categories of personal data), prior authorization or registration with the data protection authority is required.

Specific prior written registration (ie authorization) granted by the data protection authority is necessary in the following cases:

- the processing of sensitive data (except in certain specific cases eg if the processing relates to data which is manifestly made public by the data subject, provided his consent for such processing can be clearly inferred from his/her statements) and only in cases where the data subject has given his/her consent to the use of such data
- the processing of data in relation to creditworthiness or solvency
- the interconnection of personal data
- the use of personal data for purposes other than those for which it was initially collected.

DATA PROTECTION OFFICERS

The appointment of a data protection officer is mandatory when:

- processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 8 (sensitive data) or personal data relating to criminal convictions and offences referred to in Article 11 (criminal convictions and offences).

COLLECTION & PROCESSING

The collection and processing of personal data is subject to the rules laid down in the Data Protection Law. As a general note, personal data processing operations may only be undertaken once one of the following requirements are met:

- lawfulness;
- consent;
- performance of a contract;
- legitimate interests, public interests, vital interests of data subject or legal duty.

Moreover, as previously stated, there are some cases (referred to above) in which the collection and processing of personal data is subject to prior authorization from the data protection authority.

TRANSFER

The Data Protection Law stipulates that the international transfer of personal data is only permitted if the recipient country is considered to have a sufficient level of protection in respect of personal data processing.

The sufficient level of protection for foreign countries is defined by the data protection authority.

As a general rule, the transfer of personal data to countries that do not provide for an adequate level of protection of personal data can only be permitted if the data subject has given his consent or in some specific situations, namely if the transfer:

- is necessary for the performance of an agreement between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject’s request
- is necessary for the performance or execution of a contract entered into or to be entered into in the interest of the data subject between the controller and a third party
- is necessary in order to protect the vital interests of the data subject
- is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, provided the conditions laid down in law for consultation are fulfilled in the particular case.

SECURITY

The Cape Verdean Data Protection Law stipulates that data controllers must implement technical and organizational measures so as to ensure the confidentiality and security of the personal data processed. Such obligations must also be contractually enforced by the data controller against the data processor. Moreover, certain specific security measures must be adopted regarding certain types of personal data and purposes (notably, sensitive data, call recording, video surveillance etc.).

BREACH NOTIFICATION

There a duty to notify CNPD in case of a data breach no later than 72 hours after becoming aware of the same, unless it is considered that such breach does not pose a risk to the rights, freedoms and warranties of the data subjects.

ENFORCEMENT

Enforcement of the Data Protection Law is done by the data protection authority – CNPD.

Moreover, the Data Protection Law sets out criminal and civil liability as well as additional sanctions for breaches of the provisions of said statute.

Civil Liability

Any person who has suffered pecuniary or non-pecuniary loss as a result of any inappropriate use of personal data has the right to bring a civil claim against the relevant party. Criminal Liability The DPL provides that all of the following constitute criminal offences:

- a failure to notify or to obtain the authorization of the DPA prior to commencing data processing operations that require such authorization
- provision of false information in requests for authorization or notification
- misuse of personal data (ie processing personal data for different purposes than those for which the notification / authorization was granted)
- the interconnection of personal data without the authorization of the DPA
- unlawful access to personal data
- a failure to comply with a request to stop processing personal data.

These offences are punishable with a term of imprisonment of up to 2 years or a fine of up to 240 days.

Additional Sanctions

The DPL also lays down sanctions that can be imposed in addition to criminal and civil liability, namely:

- a temporary or permanent prohibition on processing data
- the advertisement of a sentence applied to a specific case
- a public warning or reproach of a data controller.

ELECTRONIC MARKETING

Law 132/V/2001 provides an opt-in right for direct marketing communications. Moreover, both Law 132/V/2001 and the Data Protection Law grant data subjects the right to object to unsolicited communications, at his/her request and free of any costs, to any data processing in relation to marketing activities.

ONLINE PRIVACY

Law 132/V/2001 lays down the legal framework for data protection in the telecommunications sector. Special rules include the following:

- any personal data obtained through phone calls performed by public operators or telecommunication public service providers must be erased or made anonymous after the phone call has ended
- traffic data can only be processed for billing, customer information or support, fraud prevention and the selling of telecommunication services.

KEY CONTACTS

Costa Cunha Gonçalves & Associados
www.mirandalawfirm.com/

António Gonçalves
Partner
Costa Cunha Gonçalves & Associados
antonio.goncalves@ccg.cv

DATA PRIVACY TOOL

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