

DATA PROTECTION LAWS OF THE WORLD

Seychelles



Downloaded: 29 April 2024

SEYCHELLES



Last modified 17 January 2024

LAW

The Data Protection Act 2023 (the Act) enacted in 2023 replaces the Data Protection Act 2003, which was never brought into force.

The Act itself has not been brought into force yet. Pending the its coming into force, data protection in Seychelles continues to be governed by general principles of privacy and confidentiality in the Civil Code of Seychelles and some provisions of various legislation, eg Financial Institutions Act and Revenue Administration Act.

The principal object of the Act is to provide for the protection of individuals with regards to the processing of personal data and to recognise the right to privacy. The Act seeks to strengthen the control and personal autonomy of data subjects over their personal data in compliance with current relevant international standards and best practice. The Act also seeks to promote and facilitate responsible and transparent flow of information by private and public entities while ensuring respect for individual's privacy.

DEFINITIONS

Definition of personal data

Personal data is defined under the Act as data consisting of information which relates to a living individual who can be identified from that information (or from that and other information in the possession of the data user), including any expression of opinion about the individual but not any indication of the intentions of the data user in respect of that individual.

Definition of sensitive personal data

The Act does not define sensitive personal data. However the Act makes provision for the Minister to modify or supplement the Data Protection Principles set out in the Act for the purpose of providing additional safeguards in relation to personal data consisting of information as to:

- the racial origin of the data subject
- his political opinions or religious or other beliefs
- his physical or mental health or his sexual life, or
- his criminal convictions.

NATIONAL DATA PROTECTION AUTHORITY

The creation of the Office of the Data Protection Commissioner is envisaged by the Act but has not yet taken place.

REGISTRATION

A person shall not hold personal data unless an entry in respect of that person as a data user, or as a data user who also carries on a computer bureau, is for the time being contained in the register of data users maintained by the Data Protection Commissioner.

The particulars to be entered into the data register are as follows:

- the name and address of the data user
- a description of the personal data to be held by it and of the purpose or purposes for which the data is to be held or used
- a description of every source from which it intends or may wish to obtain the data or the information to be contained in the data
- a description of every person to whom it intends or may wish to disclose the data (otherwise than in cases of exemptions from non-disclosure as set out in the Act)
- the name of every country outside Seychelles to which it intends or may wish directly or indirectly to transfer the data, and
- one or more addresses for the receipt of requests from data subjects for access to the data.

A person applying for registration shall state whether he wishes to be registered as a data user, as a person carrying on a computer bureau or as a data user who also carries on a computer bureau, and shall furnish the Data Protection Commissioner with the particulars required to be included in the entry to be made in pursuance of the application. Where a person intends to hold personal data for two or more purposes he may make separate applications for registration in respect of any of those purposes.

A registered person may at any time apply to the Data Protection Commissioner for the alteration of any entries relating to that person. Where the alteration would consist of the addition of a purpose for which personal data are to be held, the person may make a fresh application for registration in respect of the additional purpose.

The Data Protection Commissioner shall, as soon as practicable and in any case within the period of 6 months after receiving an application for registration or for the alteration of registered particulars, notify the applicant in writing whether his application has been accepted or refused. Where the Commissioner notifies an applicant that his application has been accepted, the notification must state the particulars which are to be entered in the register, or the alteration which is to be made, as well as the date on which the particulars were entered or the alteration was made.

No entry shall be retained in the register after the expiration of the initial period of registration except in pursuance of a renewal application made to the Data Protection Commissioner. The initial period of registration and the period for which an entry is to be retained in pursuance of a renewal application ('the renewal period') shall be a period 5 years beginning with the date on which the entry in question was made or, as the case may be, the date on which that entry would fall to be removed if the application had not been made.

The person making an application for registration or a renewal application may in his application specify as the initial period of registration or, as the case may be, as the renewal period, a period shorter than five years, being a period consisting of one or more complete years.

DATA PROTECTION OFFICERS

The Act does not contain any legal requirement to appoint a data protection officer.

COLLECTION & PROCESSING

The data protection principles set out in the Act apply to personal data held by data users. Those data protection principles are as follows:

- the information to be contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully
- personal data shall be held only for one or more specified and lawful purposes
- personal data held for any purpose or purposes shall not be used or disclosed in any manner incompatible with that purpose or those purposes
- personal data held for any purpose or purposes shall be adequate, relevant and not excessive in relation to that purpose or those purposes
- personal data shall be accurate and, where necessary, kept up to date
- personal data held for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes
- an individual shall be entitled:
 - at reasonable intervals, and without undue delay or expenses to be informed by any data user whether he holds personal data of which that individual is the subject
 - to access to any such data held by a data user, and
 - where appropriate, to have such data corrected or erased.

TRANSFER

If it appears to the Data Protection Commissioner that a person registered as a data user (or as a data user who also carries on a computer bureau) intends to transfer personal data held by him to a place outside the Seychelles, the Data Protection Commissioner may, if satisfied that the transfer is likely to contravene or lead to a contravention of any data protection principle, serve that person with a transfer prohibition notice prohibiting him from transferring the data either absolutely or until he has taken such steps as are specified in the notice for protecting the interests of the data subjects in question.

In deciding whether to serve a transfer prohibition notice, the Data Protection Commissioner shall consider whether the notice is required for preventing damage or distress to any person and shall have regard to the general desirability of facilitating the free transfer of data between the Seychelles and other states.

A transfer prohibition notice shall specify the time when it is to take effect and contain a statement of the principle or principles which the Data Protection Commissioner is satisfied are contravened and his reasons for reaching that conclusion, as well as particulars of the right of appeal conferred by the Act.

The Data Protection Commissioner may cancel a transfer prohibition notice by written notification to the person on whom it was served.

No transfer prohibition notice shall prohibit the transfer of any data where the transfer of the information constituting the data is required or authorised by or under any enactment or is required by any convention or other instrument imposing an international obligation on the Seychelles.

Any person who contravenes a transfer prohibition notice shall be guilty of an offence but it shall be a defence for a person charged with an offence under this subsection to prove that he exercised all due diligence to avoid a contravention of the notice in question.

SECURITY

The Act provides that appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of personal data.

BREACH NOTIFICATION

Breach notification

There is no mandatory requirement in the Act to report data security breaches or losses to the Data Protection Commissioner. However, the Act provides that the Data Protection Commissioner may consider any complaint that any of the data protection principles or any provision of this Act has been or is being contravened and shall do so if the complaint appears to him to raise a matter of substance and to have been made without undue delay by a person directly affected.

Where the Data Protection Commissioner investigates any such complaint he shall notify the complainant of the result of his investigation and of any action which he proposes to take.

Mandatory breach notification

None contained in the Act.

ENFORCEMENT

If the Data Protection Commissioner is satisfied that a registered person has contravened or is contravening any of the data protection principles, the Data Protection Commissioner may serve that person with an enforcement notice requiring him to take such steps for complying with the principle or principles in question. In deciding whether to serve an enforcement notice the Data Protection Commissioner shall consider whether the contravention has caused or is likely to cause any person damage or distress.

An enforcement notice in respect of a contravention of the data protection principle concerning data accuracy may require the user to rectify or erase the data and any other data held by him containing an expression of opinion which appears to the Data Protection Commissioner to be based on the inaccurate data.

If by reason of special circumstances the Data Protection Commissioner considers that the steps required by an enforcement notice should be taken as a matter of urgency, he may include a statement to that effect in the notice.

The Data Protection Commissioner may cancel an enforcement notice by written notification to the person on whom it was served.

Any person who fails to comply with an enforcement notice shall be guilty of an offence; but it shall be a defence for the person charged with an offence under this subsection to prove that he exercised all due diligence to comply with the notice in question.

If the Data Protection Commissioner is satisfied that a registered person has contravened or is contravening any of the data protection principles, the Commissioner may serve the person with a de-registration notice stating that the Data Protection Commissioner proposes to remove from the register all or any of the particulars constituting the entry or any of the entries contained in the register in respect of that person. In deciding whether to serve a de-registration notice, the Data Protection Commissioner shall consider whether the contravention has caused or is likely to cause any person damage or distress, and the Data Protection Commissioner shall not serve such a notice unless he is satisfied that compliance with the principle or principles in question cannot be adequately secured by the service of an enforcement notice.

ELECTRONIC MARKETING

Although not specifically provided for in the Act, the latter will apply to most electronic marketing activities, as there is likely to be processing and use of personal data involved (for instance, an email is likely to be considered as personal data for the purposes of the Act).

ONLINE PRIVACY

The Act does not contain specific provisions in relation to online privacy.

KEY CONTACTS

Juristconsult Chambers

www.juristconsult.com



Shalinee Dreepaul Halkhoree

Partner-Barrister

Juristconsult Chambers

T +230 465 00 20 Extension 225

sdreepaul@juristconsult.com

DATA PRIVACY TOOL

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

Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2022 DLA Piper. All rights reserved.