A Q&A guide to data protection in Seychelles. This Q&A guide gives a high-level overview of data protection rules and principles, including obligations on the data controller and the consent of data subjects; rights to access personal data or object to its collection; and security requirements. It also covers cookies and spam; data processing by third parties; and the international transfer of data. This article also details the national regulator; its enforcement powers; and sanctions and remedies.

To compare answers across multiple jurisdictions, visit the Data protection Country Q&A tool.

**SECTORAL LAWS**

There are various sectoral laws in the Seychelles, which include the following:

- The Civil Code of Seychelles (1976), which provides for a general protection of the court with regards to an individual’s rights to privacy and confidential information.
- The Electronic Transactions Act (2001), which regulates access to computers and data and provides for the offence of breach of confidentiality and privacy.
- The Financial Institutions Act (2004), which relates to the disclosure of restricted and confidential information.
- The Central Bank of Seychelles Act (2004), which provides that a member of the board of directors or an employee of the Central Bank of Seychelles (CBS) must not disclose to any person any confidential information relating to the affairs of the CBS that was acquired during the performance of his duties under the Central Bank of Seychelles Act or any other law, except if required for the performance of his duties or by law or a court order.
- The Anti-Money Laundering Act (2006), which provides for the protection of the identity of persons and information.
- The Financial Services Authority Act (2013), which provides for the protection of disclosure of protected information and for the restrictions on disclosure of financial information.
- The Anti-Corruption Act (2016), which provides for the confidentiality of certain documents, communications, and information.
- The International Business Companies Act (2016), which provides for the non-disclosure to a third party of any information or documents obtained by employees and agents of the Financial Services Authority.

It is important to note that the Seychelles is in the process of signing a Model 1B inter-governmental agreement for the implementation of the US Foreign Account Tax Compliance Act. This agreement most likely will override the existing data protection provisions put in place by the regulators.

**REGULATION LEGISLATION**

1. What national laws regulate the collection and use of personal data?

**GENERAL LAWS**

The right to privacy is guaranteed by the Constitution of the Seychelles.

The Seychelles do not have a single comprehensive law that addresses the collection and use of personal data. The key piece of legislation is the Data Protection Act (DPA), which was enacted in 2003 to provide individuals with privacy rights regarding the processing of their personal data. However, as of December 2017, the DPA has not yet been given the force of law. The act will come into operation when the Minister notifies in the official Gazette. There is no deadline for the Minister to provide this notification.
When the Data Protection Act (DPA) is given the force of law, it will apply to data users and persons carrying on a computer bureau.

For the purposes of the DPA:
- A data user is a person who holds data. A person is deemed to be holding data if:
  - the data forms a part of a collection of data processed or intended to be processed by or on behalf of that person;
  - that person (either alone or jointly or in common with other persons) controls the contents and use of the data comprised in the collection; and
  - the data is in the form in which it has been or is intended to be processed or (though not for the time being in that form) in a form into which it has been converted after being so processed and with a view to being further so processed on a subsequent occasion.
- A person carries on a computer bureau if he provides services respecting data. A person provides these services if:
  - as an agent for other persons he causes data held by them to be processed; or
  - he allows other persons to use equipment in his possession for processing.

The DPA defines data subject as an individual who is the subject of personal data. The DPA does not refer to data processors or data controllers.

### 3. What data is regulated?

When the Data Protection Act (DPA) comes into force, it will apply to personal data held by data users.

The DPA defines data as information recorded in a form in which it can be processed by equipment operating automatically in response to instructions given for that purpose.

Personal data is defined 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 to that individual.

However, the DPA does allow the Minister to amend or enhance data protection principles to provide additional safeguards in relation to personal data comprising information regarding a data subject's:
- Racial origin.
- Political opinions or religious or other beliefs.
- Physical or mental health or sexual life.
- Criminal convictions.

### 4. What acts are regulated?

When the Data Protection Act (DPA) comes into force, the DPA will apply to the collection and processing of data. Processing in relation to data is defined as amending, augmenting, deleting, or re-arranging the data or extracting the information constituting the data and, in the case of personal data, means performing any of those operations by reference to the data subject.

However, this definition will not apply to any operation performed only for the purpose of preparing the text of documents.

#### 5. What is the jurisdictional scope of the rules?

When the Data Protection Act (DPA) comes into force, the DPA will not apply to a data user in respect to data held, or to a person carrying on a computer bureau in respect of services provided, outside the Seychelles.

The DPA will also not apply to data processed wholly outside the Seychelles unless the data is used or intended to be used in the Seychelles.

#### 6. What are the main exemptions (if any)?

When the Data Protection Act (DPA) comes into force, personal data will be exempted from the DPA's provisions regarding the regulation of data users and computer bureaux where necessary to safeguard national security.

- Additionally, personal data will be exempted from the DPA's access provisions if:
  - The information is held for:
    - the prevention or detection of crime;
    - the apprehension or prosecution of offenders; or
    - the assessment or collection of any tax or duty.
  - The information is necessary for the physical or mental health of a data subject.
  - The information modified by order from the minister, where the information is held by government departments or voluntary organisations or other bodies as specified, and deemed to be maintained for or acquired while undertaking social work. The exemption or modification is granted only if the provisions to the data are likely to prejudice the undertaking of social work.
  - The information is held for the purpose of discharging statutory functions and the application of those provisions to the data is likely to prejudice the fulfilment of these functions. These functions encompass the protection of members of the public against financial loss due to dishonesty, incompetence, or malpractice by persons providing services in the banking, insurance, investment, or other financial services sector or in the management of companies or to the conduct of discharged or undischarged bankruptcies.
  - The data consists of information maintained by a government department for the purposes of making appointments and has been received from a third party.
  - The data consists of information in respect to which a claim to legal professional privilege could be maintained in legal proceedings.
  - The personal data is held by a data user only for payrolls and accounts, or for domestic or other limited purposes.

### NOTIFICATION

#### 7. Is notification or registration required before processing data?
When the Data Protection Act (DPA) comes into force, the DPA will provide for the appointment of a Data Protection Commissioner (Commissioner) who will maintain a register of:

■ Data users who hold personal data.
■ Persons running computer bureaux who provide services respecting personal data.

A data user, or a data user who also carries on a computer bureau must be registered with the Office of the Data Protection Commissioner. The Commissioner, on review of the application and receipt of all the requisite information, will make an entry in the register for each accepted application for registration.

The following details must be entered in the register:

■ The name and address of the data user.
■ A description of the personal data to be held by him and of the purpose or purposes for which the data is to be held or used.
■ A description of every source from which he intends or may wish to obtain the data or the information to be contained in the data.
■ A description of every person to whom he intends or may wish to disclose the data (otherwise than in cases exempted from non-disclosure as provided by the DPA).
■ The name of every country outside Seychelles to which he intends or may wish directly or indirectly to transfer the data.
■ One or more addresses for the receipt of requests from data subjects for access to the data.

A registered person may at any time apply to the 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 to the additional purpose.

The Commissioner must, as soon as practicable and in any case within the period of six 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. If 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 will be retained in the register after the initial period of registration has been expired except in accordance with a renewal application made to the Commissioner.

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.

**Main Data Protection Rules and Principles**

**Main Obligations and Processing Requirements**

**8. What are the main obligations imposed on data controllers to ensure data is processed properly?**

When the Data Protection Act (DPA) comes into force, data controllers can be equated to data users (see Question 2) under the DPA. The main obligations of data users are enshrined in the eight principles set out in the DPA as follows:

■ The information to be contained in personal data must be obtained, and personal data must be processed, fairly and lawfully.
■ Personal data must be held only for one or more specified and lawful purposes.
■ Personal data held for any purpose or purposes must not be used or disclosed in any manner incompatible with that purpose or those purposes.
■ Personal data held for any purpose or purposes must be adequate, relevant, and not excessive in relation to that purpose or those purposes.
■ Personal data must be accurate and, where necessary, kept up to date.
■ Personal data held for any purpose or purposes must not be kept for longer than is necessary for that purpose or those purposes.
■ An individual must be entitled, at reasonable intervals and without undue delay or expense, the following:
  - 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.

Appropriate security measures must be taken against the unauthorised access to, or alteration, disclosure, or destruction of, personal data and against the accidental loss or destruction of personal data for any personal data:

■ Held by data users.
■ For which services are provided by persons carrying on computer bureau.

**9. Is the consent of data subjects required before processing personal data?**

When the Data Protection Act (DPA) comes into force, the DPA will not expressly provide for the concept of consent of data subjects. However, it is likely that the consent of the data subjects will be required before the processing of their personal data based on the First Principle of the DPA, which provides that the information to be contained in personal data must be obtained, and that personal data must be processed, fairly and lawfully.

In determining whether information was obtained fairly regard must be had to the method by which it was obtained, including in particular whether any person from whom it was obtained was deceived or misled as to the purpose or purposes for which it is to be held, used or disclosed.

**10. If consent is not given, on what other grounds (if any) can processing be justified?**

When the Data Protection Act comes into force, processing of personal data without prior consent of data subjects can be justified under the circumstances which are non-exhaustively listed below:
Where it is necessary to safeguard national security.
For the prevention or detection of crime.
For the apprehension or prosecution of offenders.
The assessment or collection of any tax or duty.

**SPECIAL RULES**

11. Do special rules apply for certain types of personal data, such as sensitive data?

The Data Protection Act does not include any provisions for sensitive data.

However, when the Data Protection Act comes into force, it will allow the Minister to amend or enhance data protection principles to provide additional safeguards in relation to personal data comprising information regarding a data subject’s:
- Racial origin.
- Political opinions or religious or other beliefs.
- Physical or mental health or sexual life.
- Criminal convictions.

**RIGHTS OF INDIVIDUALS**

12. What information should be provided to data subjects at the point of collection of the personal data?

When the Data Protection Act comes into force, an individual will be allowed to be informed by a data user whether the data held by the latter contains the personal data of which that individual is the data subject. Further, the individual is allowed to request a copy of the information constituting any such data held by the data user. The request must be in writing accompanied by payment of the prescribed fee (not exceeding the prescribed maximum) and the data user must comply with the request within 40 days of receipt.

13. What other specific rights are granted to data subjects?

When the Data Protection Act comes into force, the Seychelles will provide data subjects the following rights with respect to their personal information:

- **Right of access to personal data.** Data subjects will have the right to be provided with a copy of the data being held by a data user pertaining to the data subject, in a form as to be interpretable by the data subject or accompanied with the relevant explanatory notes where the information is not comprehensible.

- **Compensation for inaccuracy.** A data subject must be compensated by a data user for any damage resulting from the inaccuracy of data of which he is the subject and for any subsequent distress he suffers due to this inaccuracy.

- **Compensation for loss or unauthorised disclosure.** An individual must be compensated by a data user or a person carrying on a computer bureau holding data in respect to which he is the subject, if he suffers from any damage caused by:
  - loss of the data;
  - destruction of the data without the authorisation of the data user or of the person carrying on the bureau; or

- disclosure of the data or access granted to the data without prior requisite authority.

- **Rectification and erasure.** Where the personal data held by a data user is inaccurate, a data subject may apply to the Supreme Court for an order for the rectification or erasure of the data. The Supreme Court may order the erasure of personal data if it is satisfied that the data subject has suffered damages because of the disclosure of personal data or that there is substantial risk of further disclosure of or access to the data.

14. Do data subjects have a right to request the deletion of their data?

When the Data Protection Act comes into force in the Seychelles, data held by data users may be rectified or erased on an order granted by the Supreme Court following an application by the data subject, where the data is deemed to be inaccurate.

The Supreme Court may order the erasure of data on an application by a data subject where it is satisfied that:
- The data subject has suffered prejudice due to the disclosure of personal data or access granted to personal data which could entitle him to compensation.
- There is a significant risk of further disclosure of or access to the data without authorisation.

**SECURITY REQUIREMENTS**

15. What security requirements are imposed in relation to personal data?

The Data Protection Act does not specifically impose any security requirements in relation to personal data.

When the Data Protection Act comes into force, the eighth principle of the DPA will provide that appropriate security measures be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of personal data.

In connection with this principle, attention must be paid to:
- The nature of the personal data and the harm that would result from the access, alteration, disclosure, loss, or destruction as are mentioned in this principle.
- The place where the personal data is stored, to security measures programmed into the relevant equipment, and to measures taken for ensuring the reliability of staff having access to the data.

16. Is there a requirement to notify personal data security breaches to data subjects or the national regulator?

There is no mandatory requirement to notify personal data security breaches to data subjects or the national regulator in the Seychelles.

However, when the Data Protection Act comes into force, the Commissioner will have the duty to ensure that data protection principles are observed and may consider complaints regarding contraventions of any of these principles or provisions of the act. The Commissioner must consider the complaint if the complaint raises
a substantial matter and has been lodged without undue delay by a directly affected person. The Commissioner will notify a complainant of the outcome of his investigations and of any action he proposes to take.

**PROCESSING BY THIRD PARTIES**

17. What additional requirements (if any) apply where a third party processes the data on behalf of the data controller?

The same requirements that will be applicable to data users when the Data Protection Act comes into force (see Questions 12, 13, and 15) will apply to third parties who process data on behalf of data users.

**ELECTRONIC COMMUNICATIONS**

18. Under what conditions can data controllers store cookies or equivalent devices on the data subject’s terminal equipment?

There is currently no legislation regarding the storage of cookies or equivalent devices in the Seychelles.

19. What requirements are imposed on the sending of unsolicited electronic commercial communications (spam)?

There are no specific requirements imposed on the sending of unsolicited electronic commercial communications.

When the Data Protection Act comes into force, it will apply to most electronic commercial communications, as there is likely to be processing and use of personal data.

**INTERNATIONAL TRANSFER OF DATA**

**TRANSFER OF DATA OUTSIDE THE JURISDICTION**

20. What rules regulate the transfer of data outside your jurisdiction?

When the Data Protection Act comes into force, data users who hold personal data and persons running computer bureaux must register with the Commissioner.

The entry made in the register of data users by the Commissioner should contain the name of every country outside the Seychelles to which a data user intends or wishes directly or indirectly to transfer personal data. Data users must not transfer directly or indirectly any data held by him to any country outside Seychelles other than a country named in that entry.

The Commissioner will cause a transfer prohibition notice to be served on a person registered as a data user or a data user carrying on a computer bureau, if the person proposes to transfer data to a place outside the Seychelles that would be in contravention of any data protection principle. This prohibition notice will either prohibit the transfer of data absolutely or until the necessary steps as specified in the notice have been taken to protect the interests of the concerned data subjects. When determining whether to serve the notice, the Commissioner will consider whether the transfer prohibition notice is required to prevent any damage or distress to any person and the general desirability of facilitating the free transfer of data between the Seychelles and other states.

The above provisions will not apply to transfers of data which are already outside Seychelles but will apply when the data is held in the Seychelles.

21. Is there a requirement to store any type of personal data inside the jurisdiction?

There is currently no general mandatory requirement to store any type of personal data inside the Seychelles.

**DATA TRANSFER AGREEMENTS**

22. Are data transfer agreements contemplated or in use? Have any standard forms or precedents been approved by national authorities?

The Seychelles have a number of Tax Information Exchange Agreements with Georgia, Denmark, the Netherlands, Sweden, and Guernsey amongst others that provide for the transfer of personal data for tax purposes.

There is, however, no standard form or precedent having been approved by the relevant national authorities in the Seychelles.

23. Is a data transfer agreement sufficient to legitimise transfer, or must additional requirements (such as the need to obtain consent) be satisfied?

When the Data Protection Act (DPA) comes into force in the Seychelles, data transferred under any data transfer agreement would be legitimate as long as the provisions under the data transfer agreement do not contravene any provision of the DPA and are in line with the local laws and requirements.

24. Does the relevant national regulator need to approve the data transfer agreement?

There is no requirement to obtain prior approval of a data transfer agreement by the national regulator.

**ENFORCEMENT AND SANCTIONS**

25. What are the enforcement powers of the national regulator?

When the Data Protection Act comes into force, the Commissioner will be empowered to:

- Serve enforcement notices on registered persons who have breached data protection principles.
- Require that persons take measures, within a certain time as specified in the notice, to comply with breached principles.
- Cancel any enforcement notice by written notification to the person on whom it was served.
- Serve a deregistration notice on a person who has breached or is in breach of any data protection principles or propose to remove from the register at the expiration of a period as mentioned in
the notice, all or any of the particulars constituting the entry or any of the entries contained in the register with respect to that person. However, the Commissioner must consider the damage or distress suffered or likely to be suffered by any person due to a breach of any of the data protection principles before serving a deregistration notice, and that compliance with the principle or principles in question cannot be adequately secured by the service of an enforcement notice.

The Commissioner must consider the damage or distress endured or likely to be endured by any person due to that breach while deciding whether to serve an enforcement notice.

An enforcement notice in relation to a breach of the data principle on data accuracy may direct a data user to rectify or erase the data and any other data held by him which contains an expression of opinion which appears to be based on inaccurate data, or to take any steps so as to comply with provisions of the act or as is so directed in the notice.

The Commissioner cannot serve an enforcement notice requiring a person to comply with the provisions of the act in respect of the rights of access to personal data of data subjects, unless he is satisfied that this person has breached these provisions by failing to supply information to which the data subject is entitled and which has been requested in accordance with these provisions.

Failure to comply with an enforcement notice constitutes an offence, but it is a defence for the person charged with that offence to prove that he exercised all due diligence to comply with the notice.

REGULATOR DETAILS

The Seychelles do not have a national data protection regulator.

When the Data Protection Act comes into force, it will provide for a Data Protection Commissioner. The primary duty of the Commissioner will be to ensure that data principles are being properly observed by data users and persons carrying on computer bureaux.

ONLINE RESOURCES

W www.fsaseychelles.sc/index.php/component/k2/item/49-possession-or-use-of-non-public-information

Description. This website has been created by the Seychelles Financial Services Authority (FSA) to provide information and guidelines on the regulatory framework of the non-bank financial services sector of the Seychelles. The FSA is the regulatory body responsible for the licensing, management, and development of the non-bank financial services sector of the Seychelles. The website is officially updated.


Description. This is the website of the Seychelles Legal Information Institute (SeyLII). The SeyLII was established under the patronage of the judiciary of Seychelles and backing of the African Legal Information Institute. It is an independent association and a member of the international Free Access to Law Movement and subscribes to the principles of the Declaration on Free Access to Law. The SeyLII provides free, reliable online access to essential Seychelles legal resources.
CONTRIBUTOR PROFILES

MALCOLM MOLLER
Partner
Appleby
T +230 203 4301
F +230 210 8792
E mmoller@applebyglobal.com
W www.applebyglobal.com

Professional qualifications. Legal practitioner, Supreme Court of New South Wales, 1998; solicitor and barrister, High Court of Australia, 1999; solicitor, England and Wales (non-practising), January 2003; solicitor and barrister, Supreme Court of Bermuda, 2004; registered as a foreign lawyer, Mauritius, 2009.

Areas of practice. Public and private M&A; Credit; Restructuring; Bankruptcy; Capital markets; Fund Formation and Winding-up; Strategic and Advisory Corporate Assignments.

Non-professional qualifications. Master of Laws Degree, Corporate and Commercial Law, University of New South Wales, 2000.

Representative matters
- Mauritius funding special-purpose vehicle Renascor Ltd, which is ultimately owned by the Republic of Mozambique, in relation to the refinancing of a term loan facility arranged to restructure Hidroeléctrica de Cahora Bassa S.A.R.L. by the acquisition of further shares in Hidroeléctrica de Cahora Bassa S.A.R.L. from the Government of Portugal
- Sodexo SA in relation to the purchase of Indian-based Radhakrishna Hospitality Services Group, which services a prestigious client base in 22 states and employs 20,000 people across more than a thousand sites.

Professional associations/memberships. Law Society of England and Wales (non-practising); Bermuda Bar Association; Law Society of Australia.

ABOUT PRACTICAL LAW

Practical Law provides legal know-how that gives lawyers a better starting point. Our expert team of attorney editors creates and maintains thousands of up-to-date, practical resources across all major practice areas. We go beyond primary law and traditional legal research to give you the resources needed to practice more efficiently, improve client service and add more value.

If you are not currently a subscriber, we invite you to take a trial of our online services at legalsolutions.com/practical-law. For more information or to schedule training, call 1-800-733-2889 or e-mail referenceattorneys@tr.com.