REPUBLIC OF SEYCHELLES

BILL

DATA PROTECTION BILL, 2023

(Bill No…….of 2023)

OBJECTS AND REASONS

The object of this Bill is to provide for the protection of individuals with regards to the processing of personal data and to recognise the right to privacy envisaged in Article 20 of the Constitution.

The Bill seeks to strengthen the control and personal autonomy of data subjects over their personal data in line with current relevant international standards and best practice.

The Bill also seeks to promote and facilitate responsible and transparent flow of information by private and public entities while ensuring respect to individual's privacy.

Dated this ……..... day of .....……., 2023

FRANK D. R. ALLY
ATTORNEY GENERAL

REPUBLIC OF SEYCHELLES

BILL

DATA PROTECTION BILL, 2023

(Bill No. of 2023)

ARRANGEMENT OF SECTIONS

PART I - PRELIMINARY

Sections

PART II - INFORMATION COMMISSION

PART III - DATA PROTECTION

PART IV - PROCESSING SPECIAL CATEGORIES OF PERSONAL DATA

PART V - DATA SUBJECTS RIGHTS

PART VI - OBLIGATIONS OF DATA CONTROLLERS AND DATA PROCESSORS

PART VII - TRANSFER OF DATA TO THIRD PARTIES

PART - VIII OFFENCES AND PENALTIES

PART IX – MISCELLANEOUS

REPUBLIC OF SEYCHELLES

BILL

DATA PROTECTION BILL, 2023

(Bill No. of 2023)

A BILL

FOR

AN ACT for the protection of individuals with regards to the processing of personal data, to recognise the right to privacy envisaged in Article 20 of the Constitution, to promote and facilitate responsible and transparent flow of information by private and public entities and to provide for other related matters

ENACTED by the President and the National Assembly**.**

PART I - PRELIMINARY

Short title

1. This Act may be cited as the Data Protection Act, 2023.

Interpretation

2. In this Act unless context otherwise requires —

"biometric data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allows or confirms the unique identification of that natural person;

"Chief Executive Officer" means the Chief Executive Officer appointed under section 41 of the Access to Information Act;

"Commission" means the Information Commission established under section 36 of the Access to Information Act;

"consent" means an informed, freely given and unambiguous agreement to the processing of personal information by the data subject;

"data controller" means an individual or legal entity which alone, or jointly with others, determines the purposes and means of the processing of personal data and has decision making power with respect to the processing;

"data processor" means any natural or legal person who processes personal data for or on behalf of the data controller;

"data protection impact assessment" means a tool to identify and assess privacy risks arising from the development life cycle of a program or system;

"data subject" means any natural person whose personal data is being collected, processed, stored or further distributed;

"designated officers" means officers or individuals tasked by the Commission to conduct an investigation or audit;

"Minister" means the Minister responsible for information;

"personal data" means any information relating to an identified or identifiable natural person;

"processing" means an operation involving collection, recording, structuring or storage, adaptation or alteration, retrieval, consultation or use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, or restriction, erasure or destruction;

"personal data breach" means an unauthorized access and retrieval of personal information by an individual, group of persons, or software system or a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed;

"profiling" means automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, and in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, preferences, interests, reliability, location or movements;

"sensitive personal data" means personal data related to the most private areas of the data subject's life, or whose misuse might lead to discrimination or involve a serious risk for the data subject;

"third party" means a natural or legal person, public authority, agency or body that is authorised to process personal data; and

"traffic data" means any computer data relating to a communication by means of a computer system generated by a computer system that formed a part in the chain of communication, indicating communication's origin, destination, route, time, date, size, duration,or type of underlying service.

Application

3. This Act applies to the processing of data through automatic or semi-automatic means, and to the processing of data through non-automatic means within Seychelles, which data forms part of the filing system whether managed by a private or public data controller.

Exemptions

4. This Act does not apply to —

(a) the processing of personal data by relevant authorities in the course of a criminal investigation;

(b) matters that pertain to national security; or

(c) processing of personal data by a natural person for a personal activity.

PART II - INFORMATION COMMISSION

Information Commission

5.(1) The Information Commission is the competent authority to enforce and implement this Act.

(2) Any function of the Commission under this Act and under any regulations made under this Act may, to the extent authorised by the Commission be performed by any officer of the Commission.

(3) In order to implement this Act, the Commission shall appoint its own officers and staff who may be public servants, consultants or such other persons as the Commission may consider necessary.

Powers and duties of the Commission:

6.(1) The Powers and duties of the Commission under this Act include, among others —

(a) enforcement of this Act and any related regulations;

(b) promoting public awareness;

(c) handling complaints from data subjects;

(d) conducting investigations;

(e) imposing fines; and

(f) perform such other functions as may be conferred upon it under any other written law.

(2) Notwithstanding the generality of subsection (1), the Commission shall in consultation with the relevant public and private sector stakeholders issue guidelines to further facilitate the implementation of this Act.

Investigations and audits

7.(1) The Commission has the powers of investigation and audit for complaints received by a data subject in relation to offences under this Act.

(2) The power of the Commission under subsection (1) includes the power to investigate complaints or information that an offence may have been, is being or is about to be, committed under this Act.

(3) In the performance of the duties under this section, the designated officers, shall have the authority of a law enforcement agent.

(4) For the purposes of an investigation under this section, the designated officers shall have the right to obtain the information needed to carry out their duties, and notify the data controller or data processor of the alleged infringement under this Act.

(5) The right to obtain information under subsection (4) includes the right of the designated officers to issue an order to —

(a) request the receipt or inspection of any required documentation or information, and examine those documents or information where they are located or where the data is processed;

(b) obtain a copy of any documents or information in a form that can be taken away and is visible and legible;

(c) inspect equipment, systems or place used to process the data, documents or information, and request the running, processing or managing of any such systems or equipment to inspect how they are de facto used;

(d) whenever needed for the investigation, access the private residence of an investigated party, either by having obtained prior consent by such party, or having obtained a court order;

(e) order a person to attend, at a specified time and place, for the purpose of being examined orally in relation to an investigation;

(f) order a person to furnish a statement in writing made under oath, with all the information which may be required under the order;

(6) A person whom an order has been served under this section shall comply with the order.

(7) Any person who, without lawful excuse, fails to comply with an order under this section, commits an offence and shall be liable to an administrative fine not exceeding SCR200,000.

(8) Subject to this section, the Commission shall further regulate the handling of complaints, investigations and conduct of hearings in such manner as the Commission may determine.

(9) Where the Commission is unable to arrange, within a reasonable time, for the amicable resolution by the parties concerned of the complaint, the Commission shall notify in writing the individual who made the complaint of its decision in relation to the complaint so that the individual may, where he or she considers that he or she is aggrieved by the decision, appeal against it under section 13.

(10) The Commission shall plan pre-emptive audits to address data processing in any given sector, to assess compliance with this Act and implementing regulations.

(11) If the investigation or audit is performed pursuant to a complaint, the Commission shall keep the complainant informed of the results of the investigation or audit.

Enforcement notice and corrective powers

8.(1) If the Commission has information or receives a complaint that a data processor or data controller is contravening this Act, the Commission may serve that person with a written enforcement notice requiring him or her to take, within such time as is specified in the notice, such steps as are specified for securing compliance with this Act.

(2) An enforcement notice under subsection (1) shall —

(a) contain a statement of the provision of this Act that has been, is being, or is likely to have been contravened;

(b) specify the measures that shall be taken to remedy or eliminate the situation that may cause the contravention to arise;

(c) specify a period which shall not be less than 21 days within which those measures shall be implemented; and

(d) state that a right of appeal is available under section 13, and if such appeal is brought, such steps need not be taken pending the determination or withdrawal of the appeal.

(3) If by reason of special circumstances the Commission considers that the steps required by an enforcement notice should be taken as a matter of urgency, the Commission may include a statement to that effect in the notice, and in that event, subsection (2) (c) shall not apply.

(4) On complying with an enforcement notice, the relevant data controller or data processor, shall, not later than 21 days after compliance, notify —

(a) the data subject concerned; and

(b) where such compliance materially modifies the data concerned, any person to whom the data was disclosed during the period beginning 12 months before the date of the service of the notice and ending immediately before compliance, of any amendment.

(5) Where the Commission considers that any provision of the enforcement notice may not be complied with to ensure compliance with this Act, the Commission may vary the notice and, where this is done, the Commission shall give written notice to the person on whom the notice was served.

(6) The Commission may cancel an enforcement notice by written notification to the person on whom it was served, providing the reasons for the cancellation of the enforcement notice.

(7) Any person who fails to comply with an enforcement notice commits an offence and shall be liable on conviction to a fine not exceeding level 5 on the Standard Scale.

(8) In addition, the Commission shall have the power to —

(a) issue reprimands to a data controller or data processor where processing operations have infringed provisions of this Act;

(b) order the data controller or data processor to comply with the data subject's requests to exercise his or her rights under this Act;

(c) order the data controller to communicate a personal data breach to the data subject;

(d) impose a temporary or definitive limitation including a ban on processing;

(e) order the rectification or erasure of personal data or restriction of processing and the notification of such actions to recipients to whom the personal data have been disclosed;

(f) impose an administrative fine in addition to, or instead of measures referred to in this section, depending on the circumstances of each individual case;

(g) order the suspension of data flows to a recipient in another country or to an international organization.

Preliminary injunction

9.(1) The Commission may apply to a court for a preliminary injunction to preserve data, including traffic data, where the Commission has reasonable ground to believe that the data is vulnerable to loss or modification.

(2) Where the court is satisfied that a preliminary injunction may be made under subsection (1), the court shall issue the injunction specifying a period for preservation which shall not be more than 90 days during which the order shall remain in force.

(3) The court may, on application by the Commission, extend the 90 day period for such period as the Commission thinks fit.

Disclosure

10.(1) The Commission and every person acting on behalf or under the direction of the Commission shall be bound by the duty of secrecy and shall not disclose any confidential information that comes to their knowledge in the performance of their duties and functions under this Act, neither during nor after their term in office.

(2) The Commission may disclose or may authorise any person acting on behalf or under the direction of the Commission to disclose information —

(a) that, in the opinion of the Commission, is necessary to—

(i) carry out an investigation under this Act;

(ii) establish the grounds for findings and recommendations contained in any report under this Act; or

(b) in the course of a prosecution for an offence under this Act, or an appeal from a review of a court.

Liability

11. No criminal or civil proceedings shall be pursued against the Commission, or against any person acting on behalf or under the direction of the Commission for anything done, reported or said in good faith in the course of the exercise or performance of any power, duty or function of the Commission under this Act.

Powers and duties of the Chief Executive Officer

12.(1) The Chief Executive Officer shall —

(a) issue and adopt the rules and procedures of the Commission, to allow it to exercise its functions under this Act, and amend such rules of procedures as appropriate;

(b) determine the nature, process and undertakings necessary to enable the Commission to discharge its

mandate under this Act, including all work necessary for the promotion, monitoring and protection of personal data and the rights conferred under this Act;

(c) promote awareness of data controllers and data processors of their obligations under this Act;

(d) promote self-regulation among data controllers and data processors including encouraging the establishment of data protection certification mechanisms and of data protection seals and marks, approve the criteria of certification, and where applicable, carry out a periodic review of certifications issued;

(e) exercise control on all data processing operations, either of his or her own concurrence or at the request of a data subject, and verify whether the processing of data is done in accordance with this Act;

(f) promote public awareness, including of children and the youth, on the risks, rules, safeguards and rights in relation to processing personal data, and in general to familiarize the general public with the provisions of this Act;

(g) provide information to data subjects on the exercise of their rights and remedies under this Act;

(h) advise other public institutions on measures and tools to protect personal data;

(i) issue, on the Commission's own initiative or on request, opinions to the National Assembly or the Government, other institutions and bodies on any issue related to the protection of personal data;

(j) undertake research and monitor relevant developments that can impact the protection of personal data, in particular the development of information and communication technologies and commercial practices;

(k) examine any proposal for automated decision making or data linkage that may involve an interference with, or

may otherwise have an adverse effect on the privacy of individuals, and ensure that any adverse effect of the proposal on the privacy of individuals is minimised;

(l) cooperate with supervisory authorities of other countries, to the extent necessary for the performance of his or her duties under this Act, in particular by exchanging relevant information in accordance with the laws and regulations of Seychelles;

(m) keep internal records and publicize infringements and measures taken under this Act;

(n) fulfil any other tasks related to the protection of personal data under this Act; and

(o) bring infringements of this Act to the attention of the judicial authorities and where appropriate, to commence or engage in legal proceedings in order to enforce the provisions of this Act.

(2) The Chief Executive Officer shall produce an annual general report on the Commission's activities regarding data protection, and shall present the report to the National Assembly and publish it in the Gazette.

(3) The Chief Executive Officer may produce other reports relating to the Commission's functions and present them to the National Assembly.

Right of appeal

13. Any person aggrieved by a decision of the Commission under this Act may, within 21 days from the date when the decision is made known to that person, appeal to the courts.

Cooperation

14. The Commission has the right to obtain, on request, assistance from any other public bodies as well as natural or legal persons for performing its tasks, including the right to obtain data, reports, and any other documentation needed to perform its duties under this Act.

PART III - DATA PROTECTION

Processing personal data

15.(1) Every data controller and data processor shall adhere to the principles under this Act for processing data quality, purpose limitation, use and further disclosure limitation, transparency, data subject's participation, proportionality and accountability.

(2) Personal data shall be processed if —

(a) the data subject has provided consent for the processing of such data;

(b) processing of personal information is necessary for the performance of contractual obligations between the data controller and the data subject;

(c) a specific law requires the processing of personal data by the data controller to comply with its provisions;

(d) processing of personal data is necessary to protect vital interests of the data subject or of another natural person;

(e) processing of personal data is conducted in the context of public interest and a legal framework supports such public interest;

(f) processing of personal data responds to the legitimate interests of the data controller or a third party;

(g) processing is necessary for the administration of justice, public function in a state of emergency when the processing is conducted for the benefit of the data subject.

(3) Where consent is required for the processing of personal data, consent shall be freely given, explicit and informed.

(4) Data controllers shall develop policies, procedures and processes that enable the data subject to provide consent in an intelligible and user-friendly manner, and systems developed by the data controllers shall be designed in such manner as to allow consent established under this section.

(5) When combining data from different sources data controllers shall develop a layered approach to consent, allowing data subjects to choose between categories of data to be processed and the data controllers based on the specific purposes for data processing.

(6) The layered approach referred to under subsection (5) shall not apply under the following circumstances —

(a) when limiting data items can affect the purpose of the processing impeding such processing; or

(b) when categories of information are complementary to each other and contribute to the quality of the data being processed.

(7) Data controllers shall provide data subjects all necessary information regarding the processing, to allow the data subjects to make an informed consent.

(8) Data subjects may withdraw their consent for data processing at any time.

(9) Data controllers shall be able to provide evidence of data subject consent to processing his or her data.

(10) For credit reporting systems, the credit information laws for the time in force shall regulate the specific circumstances for consent.

(11) Data controllers shall not as a condition of the supply of a product or service, require a data subject to consent to the processing of personal data beyond that required to fulfil the specified and legal purposes.

(12) Where consent is not required for processing personal data, a data controller shall still provide sufficient information to a data subject regarding the processing of data.

(13) When data is not obtained directly from the data subject, a data controller shall inform the data subject about the processing of data by a third party.

(14) In certain circumstances personal information may be collected, used, or disclosed without the knowledge and consent of the individual for protecting vital interests of the data subject or another individual.

(15) When data is not obtained from the data subject, such data shall remain confidential in compliance with the law.

Data retention

16.(1) Personal data shall be stored for the necessary period to meet the purpose of data processing and after such period the data shall be anonymized or archived and if necessary erased from the database.

(2) Data controllers shall adopt procedures, mechanisms and processes to ensure that data remains anonymous once the retention period has elapsed, using techniques such as data masking, pseudonymization, encryption or removal of personal identifiable information among others.

(3) Further retention of personal data shall be lawful where it is necessary for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller, or on the grounds of public interest in the area of public health, for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes or for the establishment or exercise or defence of legal claims.

(4) The Minister may issue additional regulations related to specific data retention periods for different types of purposes in compliance with other laws of Seychelles.

Data minimization

17.(1) Personal data processed shall be kept to the minimum necessary, to meet the purposes specified by the data controller.

(2) Every data controller shall disclose the specific purpose or purposes for data processing that shall be compatible with the purposes of disclosure to third parties, unless additional legal basis for such disclosure is established.

Data quality

18.(1) Personal data shall be processed free of error, complete and up to date.

(2) Personal data may be collected used and disclosed only for purposes—

(a) that are specific and appropriate in the circumstances;

(b) that the individual has been informed of under section 15.

(3) Data controllers processing personal data shall adequately inform data subjects of—

(a) the purposes for the collection of information;

(b) the name of the organisation and the procedures to follow to exercise any rights established under section 15.

Access, requests and correction of data

19. Data Subjects shall access, request correction of data, request deletion of data, block access to their data and oppose the usage of their data for specific purposes and request data controllers to enable usage of their data to a third party.

Data security and confidentiality

20.(1) Data controllers and data processors shall implement technical, organisational and physical measures to manage security risks arising from the processing of personal information.

(2) Personal data processed under this Act shall be confidential and shall not be disclosed in any manner that contravenes this Act.

(3) The Minister may issue additional regulations relating to setting specific security standards that need to be adhered to under this section.

Accountability for data processing activities

21.(1) Data controllers and data processors are responsible for the processing of personal data and shall be accountable for the data processing activities.

(2) For the purposes of subsection (1), data controllers and data processors shall implement measures that guarantee data protection and adoption of privacy by design and security measures.

(3) Data controllers shall maintain appropriate documentation and record keeping for all the data processing of related activities as well as formalising contractual arrangements with data processors and third parties providing outsourcing services that require access or processing personal data.

PART IV - PROCESSING SPECIAL CATEGORIES OF PERSONAL DATA

Sensitive data

23.(1) Processing of personal data relating to race, ethnic origin, biometrics, genetics, political opinions, religious or philosophical beliefs or for the purpose of identifying a person's health or sex life is prohibited.

(2) Subsection (1) shall not apply where —

(a) the data subject has given explicit consent to the processing of that personal data for one or more specified purposes, unless the law otherwise provides that the prohibition under that subsection may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment and social security and social protection law;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside that body without the consent of the data subject;

(e) processing relates to personal data which is manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defense of legal claims or whenever courts request for it, acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Seychelles law;

(h) processing is necessary for the purposes of medical diagnosis, preventive or occupational medicine, for the assessment of the working capacity of the employee, the provision of health or social care or treatment or the management of health or social care systems and services;

(i) processing is necessary for reasons of public interest in the area of public health, to protect against cross-border threats to health or to ensure high standards of quality and safety of health care and of medicinal products or medical devices;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; or

(k) processing is necessary to cover data relating to misconduct or inadequate behavior.

Data related to children

24.(1) No person shall process the personal data of a child below the age of 18 years unless consent is given by the child's parent or guardian.

(2) In accordance with subsection (1), the data controller shall obtain consent from the parents or legal guardians or verify that consent has been given in the case of data obtained from third parties taking into account available technology.

Processing of personal data relating to offences and criminal convictions

25. Processing of personal data relating to criminal convictions and offences or related security measures based on the principles for lawful processing under this Act shall be carried out only under the control of official authority or when the processing is authorised by law providing for appropriate safeguards for the rights and freedoms of a data subject.

PART V - DATA SUBJECT'S RIGHTS

Rights of data subject

26.(1) Rights of a data subject may be exercised personally or through a legal or voluntary representative.

(2) A holder of parental or custodian authority may exercise on behalf of a minor or a person with mental disabilities the rights of access, rectification, deletion, blocking, opposition, data portability or any other rights that may apply under this Act.

(3) The data controller shall ensure that any information that is required under this Part to be provided to the data subject is provided in intelligible and easily accessible form, using clear and plain language.

(4) As specified under subsection (3), the information may in addition be provided in any form, including electronic form.

(5) Where information is provided in response to a request by the data subject, the data controller shall provide the information in the same form as the request if it is practicable to do so.

(6) Where information is provided in response to a data portability request, the data controller shall enable their Application Programming Interface (API) to be accessed by a third party.

(7) Where the data controller has reasonable doubts about the identity of an individual making a request under subsection (3), (4) or (5), the data controller may —

(a) request the provision of additional information to enable the data controller confirm the identity; or

(b) delay dealing with the request until the identity is confirmed.

(8) Any information that is required under this Part to be provided to the data subject shall be provided free of charge, unless a request from a data subject is manifestly unfounded or excessive.

(9) Where a data subject request is considered unfounded or excessive, the data controller may charge a reasonable fee for dealing with the request, or refuse to act on the request.

(10) The data controller shall facilitate the data subject exercise his or her rights both in person and through remote access, and shall implement such safeguards as may be necessary to protect data from unauthorized access, use and disclosure as well as effectively identifying the legitimate data subject.

(11) The data subject shall have the right to lodge a complaint with the Commission if he or she considers that the processing of personal data relating to him or her is being or has been conducted in contravention of this Act.

(12) The data subject may in addition to subsection (11) lodge a complaint to the Commission in a case where the data subject considers that his or her rights have not been sufficiently responded to.

(13) The Commission shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy.

(14) The Minister may make regulations prescribing any matters regarding the data subject's rights under this Part, including limits to fees, timelines and such other matters as the Minister may consider necessary.

Right to be informed

27.(1) The data controller shall, for the purpose of enabling the exercise of a data subject's rights under this Part, give the data subject the following—

(a) information about the legal basis for the processing;

(b) information about the period for which the personal data will be stored or, where that is not possible, about the criteria used to determine that period;

(c) where applicable, information about the categories of recipients of the personal data including recipients in other countries or international organisations;

(d) such further information as may be necessary to enable the exercise of the data subject's rights under this Part.

Right to access data

28.(1) A data subject shall have the right to obtain from a data controller—

(a) confirmation whether the data controller is processing data subject's personal information;

(b) communication of the personal data undergoing processing and of any available information as to its origin;

(c) the recipients or categories of recipients to whom the personal data has been disclosed, including recipients or categories of recipients in third countries or international organisations;

(d) a list of data recipients that accessed the data in the past 6 months since the date of the request;

(e) the purposes for such data processing;

(f) the purposes of and legal basis for the processing;

(g) the categories of personal data concerned;

(h) the period for which it is envisaged that the personal data will be stored or, where that is not possible, the criteria used to determine that period.

(2) A data subject shall have the right to obtain the following from the data controller—

(a) rectification or correction of personal data, cancelation, deletion or erasure of personal data or the restriction of its processing;

(b) objection to further processing of data and circumstances under which such objection is legitimate;

(c) portability of data and mechanisms to request such access by a third party;

(d) the existence of the data subject's right to lodge a complaint with the Commission and the contact details of the Information Commission.

(3) The data controller may restrict, wholly or partly, the provision of information to the data subject under subsection (1) to the extent that and for so long as the restriction is in place, having regard to the rights and legitimate interests of the data subject, a necessary and proportionate measure to—

(a) avoid obstructing an official or legal inquiry, investigation or procedure;

(b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

(c) protect public security;

(d) protect national security;

(e) protect the rights and freedoms of others.

(4) Where the provision of information to a data subject under subsection (1) is restricted, wholly or partly, the data controller shall inform the data subject in writing without undue delay —

(a) that the provision of information has been restricted;

(b) of the reasons for the restriction;

(c) of the data subject's right to make a request to the Commission;

(d) of the data subject's right to lodge a complaint with the Commission; and

(e) of the data subject's right to apply to a court under section 13.

(5) The data subject may request the Commission to verify and confirm that the restriction imposed by the data controller is lawful.

Right of rectification or correction

29.(1) The data subject shall have the right to request correction of data in cases where the data processed is inaccurate, incomplete or not up to date.

(2) The data controller shall evaluate the request and if there is disagreement with the request, the data controller shall justify the rejection for such correction and inform the data subject accordingly.

(3) If the data subject is not satisfied with the justification provided by the data controller in relation to the correction, the data subject may file a complaint to the Commission.

(4) When the data is corrected, the data controller shall inform the data subject about the correction and all other users that accessed such data in the previous 6 months since the correction request was received by the data controller.

Right to cancel or delete data

30.(1) The data controller shall immediately delete personal data where —

(a) the processing of the personal data would infringe sections 26, 27, or 28;

(b) the data controller has a legal obligation to delete the data;

(2) Where the data controller would otherwise be required to erase personal data under subsection (1) but the personal data must be maintained for evidence, the data controller shall restrict its processing.

(3) Where a data subject contests the accuracy of personal data but it is not possible to ascertain whether it is accurate or not, the data controller shall restrict its processing.

(4) The data controller shall delete personal data or restrict its processing based on the provisions of this Act whether or not the data subject makes a request.

Right to object the processing of data for a specific purpose

31.(1) The data subject shall have the right to restrict or prevent the processing of personal data by a data controller when processing-

(a) has served its purpose and data processing is no longer necessary;

(b) is conducted on the basis of a legal ground that is no longer in force; or

(c) is made contrary to the provisions of the law.

(2) The Minister may, in consultation with the Commission, make such regulations as the Minister considers appropriate to provide suitable measures to safeguard a data subject's rights, freedoms and legitimate interests in connection with the taking of qualifying significant decisions based solely on automated processing.

Right to data portability

32.(1) The data subject shall have the right to —

(a) request the data controller to allow the data subject access to personal data in a structured, machine-readable and interoperable format; or

(b) transfer personal data from one data controller to another data controller.

(2) When designing systems involving processing of personal data, the data controller shall do so in a manner that enables the data subject to exercise data portability rights.

(3) The Commission shall provide guidance related to the scope of personal data to be requested by the data subject, the security measures required to the infrastructure enabling the data portability and interoperability of formats.

(4) The Commission shall in addition approve the consent mechanism and features for data portability scenarios.

Right to compensation

33.(1) Any person who suffers material or non-material damage as a result of a contravention of this Act has a right to compensation from the data controller or data processor for the damage suffered.

(2) A data controller who is involved in processing shall be liable for the damage caused by processing which contravenes this Act, but a data processor shall be liable for the damage caused by processing where the data processor has not complied with the obligations of this Act specifically directed to data processors or where the data processor has acted outside or contrary to lawful instructions of the data controller.

(3) A data controller or data processor shall be exempt from liability under subsection (2) if it proves that it is not in any way responsible for the event giving rise to the damage.

(4) Where more than one data controller or data processor, or both a data controller and a data processor are involved in the same processing, and where they are under subsections (2) and (3) responsible for any damage caused by processing, each data controller or data processor shall be liable for the entire damage and compensation to the data subject.

(5) Where a data controller or data processor has, in accordance with subsection (4) paid compensation for a damage suffered by a data subject, that data controller or data processor shall be entitled to claim from the other data controllers or data processors involved in the same processing, that portion of the compensation which corresponds to thir part of responsibility for the damage in accordance with the conditions under subsection (2).

(6) Court proceedings for exercising the right to receive compensation under this section shall be brought the competent courts under the laws of Seychelles.

PART VI - OBLIGATIONS OF DATA CONTROLLERS AND DATA PROCESSORS

Safe custody

34.(1) A data controller is responsible for personal data in its possession or under its control.

(2) A data controller shall designate one or more individuals to be responsible for ensuring that the data controller complies with this Act.

(3) A person designated under subsection (2) shall not delegate to any other person the responsibility conferred by that designation.

(4) A data controller shall make available to the public the business contact information of at least one of the individuals designated under subsection (2).

Transparency

35.(1) The data controller and data processor shall make publicly and persistently available, in a clear and readily accessible manner all the information in their custody, and shall develop a privacy policy that provides a detailed and accurate representation of the entity's data processing and data transfer activities.

(2) The policy developed under subsection (1) shall include —

(a) the type of information being collected, processed and transferred;

(b) the identity and contact information of the data controller;

(c) categories of data and purposes of such data collection and further processing;

(d) security measures;

(e) manner to exercise rights; and

(f) data retention policies**.**

Privacy by design

36.(1) The data controller shall, at the time of the determination of the means of processing the data, and at the time of the processing itself, implement appropriate technical and organisational measures which are designed to —

(a) implement the data protection principles in an effective manner; and

(b) integrate into the processing itself the safeguards necessary for that purpose.

(2) In order to implement such measures, the data controller shall take into account the technology available, the cost of implementation and the nature, scope, context and purposes of processing, as well as the likelihood and severity of risks posed by the processing to rights and freedoms of natural persons and in particular, in taking such measures, the data controller shall take into account whether —

(a) the processing can lead to harm to the data subject;

(b) the processing can affect the rights and freedom of the data subject, or prevent them from exercising their rights on their personal data;

(c) the processing implies an evaluation of personal data with the goal to build a profile on the data subject;

(d) the processing involves the processing of data on vulnerable groups, such as minors or persons with

disabilities, or the processing of special categories of data;

(e) the processing involves a large number of personal data or a large number of data subjects.

(3) Each data controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which is necessary for each specific purpose of the processing is processed, and this obligation applies to —

(a) the amount of personal data collected;

(b) the extent of its processing;

(c) the period of its storage; and

(d) its accessibility.

(4) In particular, the measures implemented to comply with the duty under subsection (1) shall ensure that, by default, personal data is not made accessible to an indefinite number of people without an individual's intervention.

(5) Where two or more data controllers jointly determine the purposes and means of processing data under this Act, they shall be known as joint data controllers.

(6) The joint data controllers shall in a transparent manner determine their respective responsibilities for compliance with their obligations under this Act, in particular regarding the exercise of the rights of a data subject.

Data processors

37.(1) The data controller may use only a data processor who provides guarantees to implement appropriate technical and organisational measures that are sufficient to secure that the processing shall meet the requirements of this Part and ensure the protection of the rights of the data subject.

(2) The data processor used by the data controller shall not engage a another data processor without the prior written authorisation of the data controller.

(3) Where the data controller gives a general written authorisation to a data processor, the data processor shall inform the data controller if the data processor proposes to add to the number of another data processors engaged by it or to replace any of them, to afford the data controller an opportunity to object to the proposal if the data controller wishes to.

(4) The processing by the data processor shall be governed by a contract in writing between the data controller and the data processor setting out the following—

(a) the subject-matter and duration of the processing;

(b) the nature and purpose of the processing;

(c) the type of personal data and categories of data subjects involved; and

(d) the obligations and rights of the data controller and data processor.

(5) The contract shall, in particular, provide that the data processor shall—

(a) act only on instructions from the data controller;

(b) ensure that the persons authorised to process personal data are subject to an appropriate duty of confidentiality;

(c) assist the data controller ensure compliance with the rights of the data subject;

(d) at the end of the provision of services by the data processor to the data controller—

(i) delete or return to the data controller (at the choice of the data controller) the personal data to which the services relate, and

(ii) delete copies of the personal data unless subject to a legal obligation to store the copies;

(e) make available to the data controller all the information necessary to demonstrate compliance with this section; and

(f) comply with the requirements of this section for engaging another data processors.

(6) The terms included in the contract shall provide that the data processor may transfer personal data to a third country or international organisation only if instructed by the data controller to make the particular transfer.

(7) If a data processor determines, in breach of this Part, the purposes and means of processing, the data processor is to be treated for the purposes of this Part as a data controller in respect of that processing.

(8) A data processor shall be considered a data controller if the data processor interacts with the data subject in his or her own name, without disclosing that he or she is acting on behalf of a data controller, even if there is a contract complying with this Part, that designates him or her as a data processor.

(9) A data processor, and any person acting under the authority of a data controller or data processor, who has access to personal data may not process the data except on instructions from the data controller, or to comply with a legal obligation.

(10) A data processor may keep the personal data blocked, in a manner specified under section 39, during the period in which he or she may still be liable following his or her relationship with the data controller.

Records of processing activities

38.(1) Each data controller shall maintain a record of all processing activities for which the data controller is responsible.

(2) When the data controller or the data processor have designated a data protection officer, they shall inform the officer of any modification, addition or exclusion to these records.

(3) The data controller's record shall contain the following information —

(a) the name and contact details of the data controller;

(b) where applicable, the name and contact details of the joint data controller;

(c) where applicable, the name and contact details of the data protection officer;

(d) the purposes of the processing;

(e) the categories of recipients to whom personal data has been or will be disclosed, including recipients in third countries or international organizations;

(f) a description of the categories of the data subject, and personal data;

(g) where applicable, details of the use of profiling;

(h) where applicable, the categories of transfers of personal data to a third country or an international organisation;

(i) an indication of the legal basis for the processing operations, including transfers, for which the personal data is intended;

(j) where possible, the envisaged time limits for erasure of the different categories of personal data;

(k) where possible, a general description of the technical and organisational security measures referred to in section 35.

(4) Each data processor shall maintain a record of all processing activities carried out on behalf of a data controller.

(5) The data processor's record shall contain the following information—

(a) the name and contact details of the data processor and of any other another data processors engaged by the data processor in accordance with this section;

(b) the name and contact details of the data controller on behalf of which the data processor is acting;

(c) where applicable, the name and contact details of the data protection officer;

(d) the processing activities carried out on behalf of the data controller;

(e) where applicable, details of transfers of personal data to a third country or an international organisation where explicitly instructed to do so by the data controller, including the identification of that third country or international organisation;

(f) where possible, a general description of the technical and organizational security measures referred to in section 37.

(6) The data controller and the data processor shall make the records kept under this section available to the Commission upon request.

Logging

39.(1) A data controller or, where personal data is processed on behalf of the data controller by a data processor, the data processor shall keep logs for all processing operations.

(2) The logs of consultation shall make it possible to establish the justification for, and the date and time of, the consultation; and as far as possible, the identity of the person who consulted the data.

(3) The logs of disclosure shall make it possible to establish the justification for, and date and time of the disclosure; and, as far as possible the identity of the person who disclosed the data and the identity of the recipients of the data.

(4) The logs kept under subsection (1) may be used only for one or more of the following purposes—

(a) to verify the lawfulness of processing;

(b) to assist with self-monitoring by the data controller or the data processor, including the conduct of internal disciplinary proceedings;

(c) to ensure the integrity and security of personal data;

(d) for the purposes of criminal proceedings.

(5) The data controller or the data processor shall make the logs available to the Commission upon request.

Blocking data

40.(1) The data controller shall block access to data when the data becomes subject to rectification or erasure.

(2) The data controller shall block such data following the principles established in Part III, including by—

(a) adopting such technical and organisational measures that allow him or her to comply with the principles; and

(b) developing mechanisms to allow the data subjects to effectively exercise their rights under Part V.

Data protection impact assessment

41.(1) Where a type of processing is likely to result in a high risk to the rights and freedoms of any individual, the data controller shall, prior to the processing, carry out a data protection impact assessment and a single assessment may address a set of similar processing operations that present similar high risks.

(2) An assessment is particularly required when—

(a) a systematic and extensive evaluation of personal aspects relating to individuals which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the individual or significantly affect the individual;

(b) processing on a large scale of special categories of data referred to under section 23;

(c) there is a systematic monitoring of a publicly accessible area on a large scale;

(d) any other circumstances as specified by the Commission in the implementation of this Act.

(3) A data protection impact assessment shall include the following—

(a) a general description of the envisaged processing operations, their purpose, and legitimate interest pursued by the data processor;

(b) an assessment of the risks to the rights and freedoms of the data subjects;

(c) the measures envisaged to address those risks; and

(d) safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this section, taking into account the rights and legitimate interests of the data subjects and other persons concerned.

(4) In deciding whether a type of processing is likely to result in a high risk to the rights and freedoms of any individual, the data controller shall take into account the nature, scope, context and purposes of the processing.

Prior consultation

42.(1) This section applies where a data controller intends to create a filing system and process personal data forming part of it.

(2) The data controller shall consult the Commission prior to the processing if a data protection impact assessment prepared under section 41 indicates that the processing of the data may result in a high risk to the rights and freedoms of individuals.

(3) Where the data controller is required to consult the Commission under subsection (2), the data controller shall give the Commission the data protection impact assessment prepared under section 41, and any other

information requested by the Commission to enable the Commission to make an assessment of the compliance of the processing with the requirements of this Part.

(4) Where the Commission is of the opinion that the intended processing referred to in subsection (1) would infringe upon a provision of this Part, the Commission shall leverage the powers conferred by this Act, and shall provide written advice to the data controller and, where the data controller is using a data processor, to the data processor.

(5) The written advice provided under subsection (4) shall be made before the end of a period of 6 weeks beginning with the receipt of the request for consultation by the data controller or the data processor.

(6) The Commission may extend the period of 6 weeks under subsection (5) by a further period of 1 month, taking into account the complexity of the intended processing.

(7) If the Commission extends the period under subsection (6), the Commission shall inform the data controller and, where applicable, the data processor of any such extension before the end of the period of 1 month beginning with the receipt of the request for consultation, and provide reasons for the delay.

Security of processing

43.(1) The data controller and data processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risks arising from the processing of personal data, including—

(a) the pseudonymization and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

(2) In order to implement the measures under subsection (1), the data controller and data processor shall take into account the state of the art, the costs of implementation and the nature, scope, context and purpose of processing as well as the risk of varying likelihood and severity for the rights of the data subject.

(3) In assessing the appropriate level of security, the data controller and data processor shall take into account the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data, transmitted, stored or otherwise processed.

(4) The data controller and data processor shall implement measures designed to —

(a) prevent unauthorised processing or unauthorised interference with the systems used in connection with it to ensure that it is possible to establish the precise details of any processing that takes place;

(b) ensure that any systems used in connection with the processing function properly and may, in the case of interruption, be restored at the minimum timeframe possible, and in any case not exceeding 72 hours; and

(c) prevent data corruption in case a system used in connection with the processing malfunctions or suffers a cyber vulnerability.

(5) The data controller and data processor shall take steps to ensure that any natural person who has authorised access to personal data under their control shall ensure that data is processed in a diligent manner for the purposes specified by the data controller.

Notification of a personal data breach to the Commission

44.(1) In the case of a personal data breach, the data controller shall not later than 72 hours after having become aware of it, notify the personal data

breach to the Commission, and where the notification to the Commission is not made within 72 hours, the notification shall be accompanied by reasons for the delay.

(2) A data breach notification shall include —

(a) a description of the nature of the personal data breach, including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) the name and contact details of the data protection officer or other contact point from whom more information may be obtained;

(c) a description of the likely consequences of the personal data breach; and

(d) a description of the measures taken or proposed to be taken by the data controller to address the personal data breach, including where appropriate, measures to mitigate its possible adverse effects.

(3) The data controller shall record the information on a personal data breach in such a way that enables the investigation process to be initiated, including the facts relating to the breach, its effects, and the remedial action taken.

(4) The data controller and data processor shall collaborate with the Commission and other relevant authorities to investigate any data breach.

Communication of a personal data breach to the data subject

45.(1) Where a data breach is likely to affect a significant number of individuals and their rights and freedoms, the data controller shall promptly inform the data subject of the breach.

(2) The information given to the data subject under subsection (1) shall include —

(a) a description of the nature of the breach;

(b) the name and contact details of the data protection officer or other contact point from whom more information may be obtained;

(c) a description of the likely consequences of the personal data breach;

(d) a description of the measures taken or proposed to be taken by the data controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

(3) The duty under subsection (1) does not apply where —

(a) the data controller has implemented appropriate technological and organisational protection measures which were applied to the personal data affected by the breach;

(b) the data controller has taken subsequent measures which ensure that the risk to the rights and freedoms of the data subject referred to in subsection (1) is no longer likely to materialise; or

(c) it would involve a disproportionate effort and the data controller has made a public communication or similar measure where the data subject is informed in an equally effective manner.

(4) Where the data controller has not already communicated the personal data breach to the data subject, the Commission may, after having considered the likelihood of the personal data breach resulting in a high risk, require it to do so.

Data protection officer

46.(1) The data controller shall designate a data protection officer when —

(a) the core activities of the data controller or the data processor consist of processing operations which, by virtue of their nature, their scope or their purposes, require regular and systematic monitoring of the data subjects on a large scale; or

(b) the core activities of the data controller or the data processor consist of processing on a large scale of special categories of data under section and personal data relating to criminal convictions and offences under section 50.

(2) For other activities not falling under subsection (1), the data controller may designate a data protection officer, who shall be subject to the same regime as those data protection officers designated under subsection (1).

(3) When designating a data protection officer, the data controller shall have regard to the professional qualities of the proposed officer, in particular the proposed officer's expert knowledge of data protection law and practice, and the ability of the proposed officer to perform the tasks under section 47.

(4) For the avoidance of any doubt the same person may be designated as a data protection officer by several data controllers, taking into account their organisational structure and size.

Tasks of the data protection officer

47.(1) The data protection officer shall monitor compliance with the data controller's policies on the protection of personal data and monitor compliance with this Act.

(2) The data protection officer shall in addition act as the contact point for the Commission on issues relating to processing, including consultation, investigations, audits or any other aspect that the Commission deems necessary in relation to the data protection laws.

(3) The data protection officer shall in addition act as the main focal point to the data subjects' complaints, and shall be responsible for establishing adequate mechanisms to adopt handling of disputes.

PART VII -TRANSFERS OF DATA TO THIRD PARTIES

Cross-border data flows

48.(1) Personal data of Seychellois citizens pertaining to the special categories as specified under section 23 shall only be processed subject to the following —

(a) there is a designated data controller accountable for cross-border data processing in Seychelles;

(b) the transfer is made between intra group schemes and the head quarters is located outside Seychelles;

(c) the data controller or data processor has informed the data subjects about the location of the data processing and all other relevant information as specified under section 27;

(d) the transfer is necessary to protect vital interests of the data subject.

(2) The Commission may, by regulations specify—

(a) the circumstances under which a transfer of personal data to another country or international organisation is to be considered necessary to meet public interest reasons; and

(b) restrictions to the transfer of a category of personal data to another country or international organisation.

(3) The Commission may authorise the processing or transfer of personal data to another country, provided that is part of the cross border privacy rules system that ensures-

(a) cross-border rules system standards are legally enforceable against the data controllers and data processors as part of the certification system;

(b) data controllers and data processors have implemented security measures using a risk- based approach proportional to the probability of the threat and severity of the harm, the confidential nature of the information processed and the number of data subjects affected.

(4) The Commission may prohibit the transfer of data under this section as may be necessary in public interest.

PART VIII - OFFENCES AND PENALTIES

Unlawful disclosure of personal data

49.(1) A data controller who, without a lawful justification discloses personal data in any manner that is incompatible with the purpose for which such data has been collected, commits an offence.

(2) A data processor who, without lawful justification discloses personal data processed by him or her without the prior authority of the data controller on whose behalf the data is being or has been processed commits an offence.

(3) Subject to subsection (4), any person who —

(a) obtains access to personal data, or obtains any information constituting such data without the prior authority of the data controller or data processor by whom the data is kept; or

(b) discloses the data or information to another person who is not entitled to access such data or information commits an offence.

(4) Subsection (3) shall not apply to a person who is an employee or agent of a data controller or data processor and is acting within his or her mandate.

(5) Any person who offers to sell personal data, where such personal data has been obtained in breach of subsection (1) commits an offence.

Obstruction

50.(1) No person shall obstruct the Commission or any person acting on behalf or under the direction of the Commission in the performance of the Commission's duties and functions under this Act.

(2) Any person who contravenes this section commits an offence and liable on summary conviction to a fine not exceeding SR200,000.

Offence for which no specific penalty provided

51.(1) Any person who commits an offence under this Act for which no specific penalty is provided or who otherwise contravenes this Act shall be liable on conviction to imprisonment not exceeding 2years or to a fine of level 5 on the Standard Scale.

(2) In addition to any penalty referred to under subsection (1), the court may —

(a) order the forfeiture of any equipment or any article used or connected in any way with the commission of the offence; or

(b) order or prohibit the doing of any act to stop a continuing contravention.

General conditions for imposing administrative fines

52.(1) The Commission shall ensure that the imposition of administrative fines for infringements of this Act shall, in each individual case be effective, proportionate and dissuasive.

(2) Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures under the corrective authority of the Commission.

(3) When deciding whether to impose an administrative fine and on the amount of the fine in each individual case, the Commission will take into account the following —

(a) the nature, gravity and duration of the infringement, taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

(b) the intentional or negligent character of the infringement;

(c) any action taken by the data controller or data processor to mitigate the damage suffered by the data subjects;

(d) the degree of responsibility of the data controller or data processor, taking into account the technical and organisational measures implemented by them;

(e) any relevant previous infringements by the data controller or data processor;

(f) the degree of cooperation with the Commission, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the Commission, in particular whether and if so to what extent the data controller or data processor notified the infringement;

(i) where measures taken under the corrective authority of the Commission have previously been ordered against the data controller or data processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct or certification mechanisms; and

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

(4) If a data controller or data processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Act, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

(5) Infringements of the obligations of the data controller and the data processor under this Act shall, in accordance with subsection (2), be subject to administrative fines up to SCR 200,000.

(6) Infringements of the following provisions shall be subject to administrative fines up to SCR 200,000 —

(a) the basic principles for processing, including conditions for consent;

(b) the data subjects' rights pursuant;

(c) the transfers of personal data to a recipient in a third country or an international organisation;

(d) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows; or

(e) failure to provide access to the Commission in violation of section 7.

(7) Non-compliance with an order by the Commission under its corrective authority shall, in accordance with subsection 2, be subject to administrative fines up to SCR 200,000.

(8) Without prejudice to the corrective powers of the Commission, the regulations implementing this Act may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies.

(9) The exercise by the Commission of its powers under this section shall be subject to appropriate procedural safeguards in accordance with the law, including effective judicial remedy and due process.

(10) The Commission shall lay down the rules on other penalties applicable to infringements of this Act, in particular for infringements which are not subject to administrative penalties, and shall take all measures necessary to ensure that they are implemented.

PART IX - MISCELLANEOUS

Cooperation with other authorities

53.(1) The Commission shall develop effective collaborative mechanisms with other authorities and government agencies to ensure the effective enforcement of this Act.

(2) The Commission shall adopt formal and informal mechanisms to cooperate with international organisations and the supervisory authorities of other countries to facilitate the effective enforcement of this Act, and to support knowledge sharing and best practices.

(3) The Commission shall provide international mutual assistance in the enforcement of legislation for the protection of personal data, including through notification, complaint referral, investigative assistance and information exchange, subject to appropriate safeguards for the protection of personal data and other rights and freedoms recognized under the Constitution of Seychelles.

(4) The Commission shall effectively cooperate with other authorities in solving jurisdictional conflicts with other countries.

Compliance audit

54. The Commission may carry out periodical audits of the systems of data controllers or data processors to ensure compliance with this Act.

Regulations

55. The Minister may, in consultation with the Commission make regulations generally for the better carrying into effect the provisions of this Act.

Repeal

56. The Data Protection Act (Cap 57) is repealed.