



CARICOM

CARICOM COMMUNITY (CARICOM)
SECRETARIAT

DATA PROTECTION AND PRIVACY RULES

Rules to provide for the protection of privacy and personal information to the satisfaction of the individual and or entity.

This page is left intentionally blank

FOREWORD

Privacy has been identified as a human right, as concretised in various provisions of the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, as well as the American and European Convention on Human Rights. This right to privacy which protects the individual's private life against arbitrary, unlawful or abusive interference, by extension provides for the protection of the personal information of the individual, and the protection of the transmission of such information.

Privacy and Data Protection laws are based on the premise that the individual must have some level of control over how the personal information collected from them, whether by the government, businesses, international and regional public service organisations is utilised, processed or disclosed. This control is primarily asserted at the point at which information is collected, at which time the collecting party must make a full disclosure of the intent for which the information is to be collected, and commit to be so constrained in the use of the personal information after it is collected. The other major facilitation of the individual's control is the obligation of the collecting party to provide the individual with the opportunity to review any information which is stored by the collecting party about the individual. Despite this, there are exemptions to the general rules associated with the restriction of the use and disclosure of personal information, with the application of specific, different guidelines in special circumstances, such as in the fields of medical services and national security where gaining the assent of the individual is not practical. Also, circumstances where disclosure is permitted by statute or is ordered by a court of law.

The implementation by the CARICOM Secretariat of a privacy and data protection framework supports the objectives of the organisation's respect for the individual's right to privacy and demonstrates the CARICOM Secretariat's preparedness to protect the individual. The framework is geared to treating with the management of personal information having regard to the relevant exemptions.

**PART 1
APPLICATION AND INTERPRETATION**

Rule 1.1	Citation and commencement	1
Rule 1.2	Application	1
Rule 1.3	Definitions	1

**PART 2
THE OVERRIDING OBJECTIVE**

Rule 2.1	The overriding objective.....	5
Rule 2.2	Application of overriding objective.....	6
Rule 2.3	Duty of Staff of the Secretariat.....	6

**PART 3
NON - APPLICABILITY**

Rule 3.1	Scope of this Part.....	9
Rule 3.2	Staff of the Secretariat	9
Rule 3.3	Contract for Services	9
Rule 3.4	Discretionary beneficiaries	9
Rule 3.5	Deceased persons	9

**PART 4
OBLIGATIONS OF THE DATA CONTROLLER**

Rule 4.1	Data controllers	11
Rule 4.2	Limitation on the collection and processing of personal data.....	11
Rule 4.3	Personal information to be collected directly	12
Rule 4.4	Individual to be informed of purpose	12
Rule 4.5	Retention of personal information used for an administrative purpose..	13
Rule 4.6	Accuracy of personal information	13
Rule 4.7	Protection of personal information	14

**PART 5
STORAGE, USE, ACCESS AND DISPOSAL OF PERSONAL INFORMATION**

Rule 5.1	Scope of this Part.....	15
Rule 5.2	Storage of personal information	15
Rule 5.3	Disposal of personal information	15
Rule 5.4	Use of personal information	15

**PART 6
DISCLOSURE OF PERSONAL INFORMATION**

Rule 6.1	Scope of this Part.....	18
----------	-------------------------	----

Rule 6.2	Disclosure of personal information	18
Rule 6.3	When personal information may be disclosed.....	18
Rule 6.4	Disclosure for research or statistical purposes.....	19
Rule 6.5	Disclosure for archival purposes	19
Rule 6.6	Disclosure of personal information to third-party funding agencies	20

**PART 7
RIGHTS OF THE DATA SUBJECT (INDIVIDUAL)**

Rule 7.1	Scope of this Part.....	21
Rule 7.2	Right of access to personal information	21
Rule 7.3	Refusal of access of personal information.....	21
Rule 7.4	Severance of exempt information.....	22
Rule 7.5	Delegation of rights of the individual.....	22

**PART 8
THIRD PARTY PROCESSING**

Rule 8.1	Scope of this Part.....	25
Rule 8.2	Compliance.....	25
Rule 8.3	Contract with Data Processor	25

PART 1

APPLICATION AND INTERPRETATION

Contents of this Part

Citation and commencement	Rule 1.1
Application	Rule 1.2
Definitions	Rule 1.3

Citation and commencement

- 1.1** (1) These Rules may be cited as the Privacy and Data Protection Rules (PDPR).
- (2) These Rules shall come into effect on the 28th day of October 2020.
- (3) A reference to a rule as PDPR xx or Rule xx is a reference to a rule so numbered in these Rules.

Application

1.2 (1) These Rules are intended to regulate privacy and data protection of the personal information of persons under the control of the Secretariat.

(2) These Rules shall apply to personal information supplied to the Secretariat by any person and under the control of the Secretariat in relation to -

- (a) procurement of goods, works, services and consultancies undertaken by the Secretariat, whether funded by the Secretariat or any international donor or loan agency;
- (b) selection and employment of consultants;
- (c) recruitment, selection, and employment of staff, including the dismissal and resignation of staff;
- (d) disposal of assets;
- (e) volunteer work and or internships; and
- (f) any other mechanism whereby personal information of individuals has come into possession of the Secretariat.

Definitions

1.3 In these Rules –

“**data**” includes any information, record, document, correspondence, memorandum, book, plan, drawing, pictorial or graphic work, photograph, film, microfilm, sound – recording, videotape, machine – readable record and any other documentary material, regardless of the physical form or characteristic, or any copy of those things.

“data controller” means any person whether by themselves, their servants, agents and or workers within the employ of the Secretariat, responsible for the collection of personal information of individuals.

“data processing” means collection, retrieval, recording, storage, organisation, disclosure, sharing, dissemination, blocking, alteration, adaption, use, analysis, erasure, destruction or transfer of personal information.

“data subject” means an individual who is the subject of personal information.

“dependent” has the same meaning as specified in clause 3(c) of the Revised Staff Regulations of the Secretariat.

“enterprise” means a partnership or body (corporate or unincorporated) engaged in the conduct of legal business;

“health care institution” refers to institutions registered as facilities for the provision of health care in any jurisdiction and includes hospitals, health centres, clinics and doctor’s offices.

“individual” means a natural person.

“personal information” means information about an identifiable individual that is recorded in any form including—

- (a) information relating to the nationality, address, age, contact details, country of residence, fax numbers, postal numbers or marital status of the individual;
- (b) information relating to social security status, national insurance contributions and judicial records of the individual;
- (c) any information supplied as information and evidence by an individual pursuant to the Secretariat’s Guidelines and Procedures Manual (the “GPM”);
- (d) information supplied pursuant to the disposal of assets procedure by the Secretariat;
- (e) information on the racial or ethnic origins of the individual¹;
- (f) information on the political opinions or affiliations of the individual; information on religious beliefs or other beliefs of a similar nature of the individual²;
- (g) information relating to physical or mental health or condition of the individual;
- (h) information related to fingerprints, deoxyribonucleic acid, blood type or biometrics of the individual;
- (i) information related to the sexual orientation or sexual life of the individual³
- (j) information related to the criminal or financial record of the individual;
- (k) information relating to the education, technical skills, expertise, languages, professional experience or employment history of the individual;
- (l) information supplied by an individual pursuant to employment opportunities, including the personal information of references, birth certificates, medical

¹ The Secretariat does not request the type of information described in (e), (f) and (i), but is not oblivious, that notwithstanding same, said information may come into its possession.

² Ibid

³ Ibid

- records, passport information, photographs, banking data, and information concerning a spouse, children or other dependants of the individual;
- (m) any identifying number, symbol or other particular designed to identify the individual;
 - (n) the views and opinions of any other person about the individual.
 - (o) The terms of any lease agreements entered into by employees of the Secretariat;
 - (p) correspondence sent to an establishment by the individual that is explicitly or implicitly of a private or confidential nature, and any replies to such correspondence which would reveal the contents of the original correspondence;

“Processing” or “processed” in relation to data means obtaining, recording or holding the data or carrying out any operation or set of operations on data, including –

- (a) organisation, adaptation or alteration of the data;
- (b) retrieval, consultation or use of the data; or
- (c) alignment, combination, blocking, erasure or destruction of the data.

“record” means recorded information collected, created or received in the initiation, conduct or completion of an activity and that comprises sufficient content, context and structure to provide evidence or proof of that activity or transaction;

“relevant filing system” means any structured set of personal data that can be searched or accessed by reference to relevant criteria (e.g., name, ID number, telephone number, etc.).

“Secretariat” means the CARICOM Secretariat:

“sensitive personal information” means information on a person’s–

- (a) racial or ethnic origins⁴;
- (b) political affiliations or trade union membership⁵;
- (c) religious beliefs or other beliefs of a similar nature⁶;
- (d) physical or mental health or condition;
- (e) sexual orientation or sexual life⁷;
- (f) criminal or financial record;
- (g) any personal identification numbers including social security numbers;
- (h) age; or
- (i) salary.

“service provider” means a person, whether natural or legal, retained under a contract to perform services required by the Secretariat.

“spouse” – includes a former spouse.

⁴ *Ibid*

⁵ *Ibid*

⁶ *Ibid*

⁷ *Ibid*

PART 2

THE OVERRIDING OBJECTIVE

Contents of this Part

The overriding objective	Rule 2.1
Application of overriding objective	Rule 2.2
Duty of Staff of the Secretariat	Rule 2.3

The overriding objective

2.1 (1) The objective of these Rules is to ensure that protection is afforded to an individual's right to privacy and the right to maintain sensitive personal information as private and personal in accordance with the general privacy principles prescribed in rule 2.1 (3).

(2) The Secretariat is to make available to individuals documents regarding its policies and practices related to the management of personal information.

(3) All persons that treat with personal data in the conduct of the Secretariat's business shall, when undertaking such business, be guided by the following basic privacy principles -

- (a) the Secretariat shall be responsible for the personal information under its control;
- (b) the purpose for which personal information is collected shall be identified by the Secretariat before or at the time of collection;
- (c) knowledge and consent of the individual are required for the collection, use or disclosure of personal information;
- (d) personal data shall be processed fairly and lawfully and, in particular shall not be processed unless particular conditions as stated herein have been met;
- (e) personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;
- (f) personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is required;
- (g) personal data shall be accurate and, where necessary, kept up to date;
- (h) personal information shall only be retained for as long as is necessary for the purpose collected and shall not be disclosed for purposes other than the purpose of collection without the prior consent of the individual;
- (i) personal data shall be processed in accordance with the rights of the individual under these Rules.
- (j) personal information is to be protected by such appropriate safeguards having regard to the sensitivity of the information;

- (k) appropriate technical and institutional measures shall be taken against unlawful processing of personal data and against accidental loss or destruction of, or damage to, such data;
- (l) comply with data transfer restrictions when transferring personal data internationally and to third-parties;
- (m) provide individuals with rights to access, correct, update, or delete their personal data, and object to the processing of their personal data under some circumstances;
- (n) the Secretariat shall, except where otherwise provided by written law, disclose at the request of the individual, all documents relating to the existence, use and disclosure of personal information, such that the individual can challenge the accuracy and completeness of the information.

Application of overriding objective

2.2 Data controllers must seek to give effect to the overriding objective when they —

- (a) exercise any discretion given to them by these Rules;
- (b) interpret the meaning of any Rule herein;
- (c) make any decision, which are not expressly provided for in these Rules.

Duty of Staff of the Secretariat

2.3 All staff of the Secretariat are required to assist the Secretariat, data controller or designated representative to *further the overriding objective*

PART 3

NON APPLICABILITY

Contents of this Part

Scope of this Part	Rule 3.1
Staff of the Secretariat	Rule 3.2
Contract for Services	Rule 3.3
Discretionary beneficiaries	Rule 3.4
Deceased persons	Rule 3.5

Scope of this Part

3.1 This Part defines personal information that does not fall under the provisions of these Rules.

Staff of the Secretariat

3.2 (1) The following information about an individual who is or has been a member of Staff of the Secretariat is not regarded as personal information for the purposes of these Rules:

- (a) The fact that the individual is or has been a Staff of the Secretariat ;
- (b) The title, business address and business telephone number of the individual;
- (c) The name of the individual on a document prepared by the individual in the course of employment; and
- (d) The professional opinion or views of the individual given in the course of employment.

Contract for Services

3.3 Information about an individual who is or was performing services under contract for the Secretariat that relates to the services performed, including the terms of performance, the name of the individual, and the opinion or views of the individual given in the course of performance of these services is not personal information for the purposes of these Rules.

Discretionary beneficiaries

3.4 Information relating to any discretionary benefit of a financial nature including the granting of any license or permit conferred to an individual, including the name of the individual and the exact nature of the benefit is not regarded as personal information for the purposes of these Rules.

Deceased persons

3.5 Information about an individual who has been deceased for more than twenty (20) years is not personal information for the purposes of these Rules.

PART 4

OBLIGATIONS OF DATA CONTROLLERS

Contents of this part

Data Controllers	Rule 4.1
Limitation on the collection and processing of data	Rule 4.2
Personal information to be collected directly	Rule 4.3
Individual to be informed of the purpose	Rule 4.4
Retention of personal data	Rule 4.5
Audits	Rule 4.6
Accuracy of personal information	Rule 4.7
Protection of personal information	Rule 4.8

Data controllers

4.1 (1) For the purposes of these Rules there shall, by operation of the nature of the activity, be a data controller with direct responsibility for the management of an individual's personal information.

(2) The Head of the Department or authorised representative, for which the personal information is sought and or received by the Secretariat, shall be deemed to be the data controller for the specific personal information sought in carrying out of the functions of that department.

(3) Any personal data transferred by the original data controller to any other person within the employ of the Secretariat shall remain the responsibility of the data controller and the data controller shall ensure that said person treats personal data in a manner consistent with these Rules.

(4) Notwithstanding, rule 4.1 (3), the person within the Secretariat to whom said personal data is transferred shall also be considered a data controller and deal with personal data in accordance with these Rules.

Limitation on the collection and processing of personal data

4.2 Personal information may not be collected for or by the data controller unless -

- (a) the collection of that information is expressly authorised by or under any written rules or regulations of the Secretariat;
- (b) the information is collected for the purposes of law enforcement; or
- (c) that information relates directly to and is necessary for an operating programme or activity of the Secretariat.

Personal information to be collected directly

4.3 (1) Where a data controller requires personal information from an individual he or she shall collect the personal information or cause the personal information to be collected directly from that individual.

(2) Notwithstanding rule 4.3 (1), personal information may be collected from a source other than the individual where –

- (a) another collection method is authorised by the individual;
- (b) the collection of information is necessary for medical treatment of an individual and it is not possible to collect the information directly from that individual or the collection necessary to obtain authority from that person for another method of collection;
- (c) the information is collected for the purpose of–
 - (i) determining the suitability for an honour or award including an honorary degree, scholarship, prize or bursary;
 - (ii) proceedings before a court or a judicial or quasi – judicial tribunal;
 - (iii) collecting a debt or fine or making a payment; or
 - (iv) law enforcement

Individual to be informed of purpose

4.4 (1) A data controller shall ensure that the individual from whom it collects personal information or causes personal information to be collected is informed of –

- (a) the purpose for collecting it;
- (b) the authority for collecting it;
- (c) the intended recipients;
- (d) the individual's rights, such as access, correction, and deletion;
- (e) whether providing answers to questions are voluntary or compulsory and the possible consequences of failure to reply;
- (f) identification of recipients or categories of recipients of personal data; and
- (g) the title, business address and business telephone number of an official or employee of the Secretariat who can answer the individual's questions about the collection and use of the data.

4.4 (2) An individual from whom information is collected shall have the right to obtain from the data controller without undue delay the correction of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the individual shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

4.4 (3) An individual shall have the right to obtain from the data controller the deletion of personal data concerning him or her without undue delay and the data controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- (b) the individual withdraws consent on which the processing is based and where there is no other legal ground for the processing;

- (c) the individual objects to the processing and there are no overriding legitimate grounds for the processing;
- (d) the personal data have been unlawfully processed;
- (e) the personal data have to be erased in compliance with a legal obligation in law to which the data controller is subject.

4.4 (4) Where the data controller has made the personal data public and is obliged pursuant to rule 4.4(3) to delete the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform data controllers which are processing the personal data that the individual has requested the erasure by such data controllers of any links to, or copy or replication of, those personal data.

4.4 (5) Rules 4.4(3) and 4.4(4) shall not apply to the extent that processing is necessary:

- (a) for compliance with a legal obligation which requires processing by law to which the data controller is subject or 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
- (b) for the establishment, exercise or defence of legal claims.

Retention of personal information used for an administrative purpose

4.5 Personal information that has been used by the Secretariat for administrative purposes shall be retained by the Secretariat for such period of time after it has been used—

- (a) in the case of matters concerning recruitment of successful candidates, unsuccessful candidates, unsolicited applications, third-party recruitment, retention of applications. pension benefits, personnel files, sick leave, medical records etc. - as prescribed by the Secretariat's recruitment policy;
- (b) in the case of matters related to procurement proceedings –
 - (i) non successful tenderers – five (5) years after the procurement procedure; and
 - (ii) successful tenderers – seven (7) years after the last payment made under the contract.
- (c) in the case of any other personal information that came into possession of the Secretariat, a reasonable time as determined by the data controller.

Audits

4.6 Notwithstanding rule 4.5, where an audit has commenced before the end of the periods identified above, and continues for any time in excess of the retention period above, the files containing the personal information shall be retained for such period as is necessary to complete and finalise the audit.

Accuracy of personal information

4.7 Where the personal information of an individual is in the custody or control of the Secretariat and the personal information will be used by or on behalf of the Secretariat to make a decision that directly affects the individual, the Secretariat shall make every reasonable effort to ensure that the personal information is accurate, complete and up-to-date.

Protection of personal information

4.8 (1) The Secretariat shall protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorised access, collection, use, alteration, disclosure and disposal.

(2) Where any other person processes personal information on behalf of the Data Controller, the Data Controller shall ensure that the person:

- (a) has sufficient controls in place to implement the security measures that must be taken;
- (b) actually takes the measures so identified by the data controller.

PART 5

STORAGE, USE, ACCESS AND DISPOSAL OF PERSONAL INFORMATION

Contents of this Part

Scope of this Part	Rule 5.1
Storage of personal information	Rule 5.2
Confidentiality	Rule 5.3
Disposal of personal information	Rule 5.4
Use of personal information	Rule 5.5

Scope of this Part

5.1 This Part outlines how personal information is to be processed, stored and disposed of.

Storage of personal information

5.2 The Secretariat shall ensure or take steps to ensure that personal information in its custody or under its control is stored in premises, facilities, equipment or machinery under the exclusive control of the Secretariat.

Confidentiality

5.3 Personal data will be treated in a confidential manner and stored responsibly. Appropriate security such as password-protected computer files shall be provided. In addition, the physical files containing personal information shall be securely locked away and retrievable only by authorised personnel.

Disposal of personal information

5.4 The Secretariat shall dispose of, erase or make anonymous all personal information in its control or custody, which is no longer required to fulfil the identified purpose for which the information was collected for, within a reasonable period of time or in accordance with any other department policy of the Secretariat or as prescribed by these Rules.

Use of personal information

5.5 (1) Personal information under the custody or control of the Secretariat shall not, without the consent of the individual to whom it relates, be used by the Secretariat except for the purpose for which the information was obtained or compiled by the Secretariat, or for a use consistent with that purpose, or for a purpose for which the information may be disclosed by the Secretariat pursuant to rule 5.5

(2) For job applicants, personal data will be collected and used by the Secretariat for the following purposes and such personal data may be disclosed by the Secretariat to third-parties where necessary for the following purposes:

- (a) assessing and evaluating job applicants' suitability for employment in any current or prospective position within the Secretariat;
- (b) verifying job applicants' identity and the accuracy of the personal details and other information provided; or
- (c) for auditing purposes

(3) In the case of an employee, personal data will be collected and used by the Secretariat for the following purposes and such personal data may be disclosed by the Secretariat to third-parties where necessary for the following purposes:

- (a) performing obligations under or in connection with an employee's contract of employment with the Community, including payment of remuneration and tax;
- (b) all administrative and human resources related matters within the Secretariat, including administering payroll, granting access to premises and computer systems of the Secretariat, processing leave applications, administering insurance and other benefits, processing an employee's claims and expenses, investigating any acts or defaults (or suspected acts or defaults) and developing human resource policies;
- (c) managing and terminating the employment relationship with an employee, including monitoring an employee's internet access and use of the Secretariat's intranet or email to investigate potential contraventions of the Secretariat's internal or external compliance regulations, and resolving any employment related grievances;
- (d) assessing and evaluating an employee's suitability for employment/appointment or continued employment/appointment in any position within the Secretariat;
- (e) ensuring business continuity for the Secretariat in the event that an employee's employment with the Secretariat is or will be terminated;
- (f) facilitating any proposed or confirmed merger, acquisition or business asset transaction involving any part of the Secretariat, or corporate restructuring process; and
- (g) facilitating the Secretariat's compliance with any laws, customs and regulations which may be applicable to the Secretariat.

(4) The use of personal information is consistent with the purposes for which it was obtained or compiled, if the use has a reasonable and direct connection to the purpose, and is necessary for performing the duties of, or for operating an authorised programme of the Secretariat that uses or discloses the information or causes the information to be used or disclosed.

(5) The Secretariat shall not process sensitive personal information unless-

- (a) it obtains the express consent of the person to whom that sensitive personal information relates; and

- (b) processing of the personal data is necessary for or directly related to the purpose it was collected.

(6) Notwithstanding rules 5.5 (1), (2), (3) and (4), the Secretariat may process personal information where–

- (a) the individual has unambiguously given his/her consent;
 - (b) where it has been made public by the individual;
 - (c) for research and statistical purposes;
 - (d) in the interest of law enforcement and national security;
 - (e) processing is necessary for the performance of a contract to which the individual is party or in order to take steps at the request of the individual prior to entering into a contract; or
 - (f) processing is necessary for compliance with a legal obligation to which the Data Controller is subject; or
 - (g) processing is necessary in order to protect the vital interests of the individual or another person's vital interest and the individual cannot consent, or the Secretariat cannot reasonably obtain the individual's consent.
-

PART 6

DISCLOSURE OF PERSONAL INFORMATION

Contents of this Part

Scope of this Part	Rule 6.1
Disclosure of personal information	Rule 6.2
When personal information may be disclosed	Rule 6.3
Disclosure for research or statistical purposes	Rule 6.4
Disclosure for archival purposes	Rule 6.5
Disclosure of medical information	Rule 6.6
Disclosure of information to third-party funding agencies	Rule 6.7

Scope of this Part

6.1 This Part addresses the circumstances in which personal information of an individual may be disclosed.

Disclosure of personal information

6.2 Personal information under the custody or control of the Secretariat shall not be disclosed by the Secretariat without the consent of the individual to whom it relates, except in accordance with rules 6.3, 6.4, 6.5 and 6.6

When personal information may be disclosed

6.3 Personal information under the control of the Secretariat may only be disclosed—

- (a) for the purposes for which the information was collected or compiled by the Secretariat or for a use consistent with that purpose;
- (b) to staff members of the Secretariat, including any external experts who work on behalf of the Secretariat and are directly or indirectly involved in the procurement of consultants and contractors and in project execution;
- (c) for the purpose of any audit, monitoring and inspection of the programme or tender procedure, for which the personal information was requested;
- (d) members of the public, in which case such information shall be limited to name and address, the amount awarded and the name of the project or programme for which the personal information was collected.
- (e) for the purpose of complying with a *subpoena* or warrant issued or order made by a court, person or body with jurisdiction to compel the production of information or for the purpose of complying with rules of court relating to the production of information;
- (f) to an investigative body, on the written request of the investigative body, for the purpose of investigating compliance with any written law or carrying out a lawful

- investigation, if the request specifies the purpose and describes the information to be provided;
- (g) if the Secretary-General or the designated representative agrees that a compelling circumstance exists that affect the health or safety of any person and if notice of the disclosure is mailed to the last known address of the individual to whom the information relates, unless Secretary-General or the designated representative has a reasonable belief that providing notification could harm the health or safety of any person
 - (h) so that the next of kin or friend of an injured, ill or deceased person may be contacted;
 - (i) for the purpose of collecting monies owing by an individual to the Secretariat;
 - (j) for statistical purposes where the disclosure meets the requirements of rule 6.4 or
 - (k) for archival purposes where the disclosure meets the requirements of rule 6.5.

Disclosure for research or statistical purposes

6.4 The Secretariat may disclose personal information or may cause personal information in its custody or control to be disclosed for a research purpose, including statistical research only if—

- (a) the research purpose cannot reasonably be accomplished unless that information is provided in individually identifiable form;
- (b) the information is disclosed on condition that it not be used for the purpose of contacting a person to participate in research;
- (c) any record linkage is not harmful to the individual to whom that information is about and the benefits to be derived from the record linkage are clearly in the public interest;
- (d) the Secretary-General or the designated representative concerned has approved conditions relating to the following:
 - (i) security and confidentiality;
 - (ii) the removal or destruction of the individual identifiers at the earliest reasonable time; and
 - (iii) the prohibition of any subsequent use or disclosure of that information in individually identifiable form without the express authorisation of the Secretariat; and
- (e) the person to whom that information is disclosed has signed an agreement to comply with the approved conditions, and any of the Secretariat's policies and procedures relating to the confidentiality of personal information.

Disclosure for archival purposes

6.5 The archives of the Secretariat may disclose personal information or cause personal information in its custody or control to be disclosed for archival or historical purposes if—

- (a) the disclosure would not be an unreasonable invasion of professional or personal privacy;
- (b) the disclosure is for historical research and is in accordance with rule 6.3;
- (c) the information concerns someone who has been deceased for twenty or more years;
or
- (d) the information is in a record that has been in existence for one hundred or more years

Disclosure of medical information

6.6 Notwithstanding rules 6.3, 6.4 and 6.5, medical information of any person under the control of the Secretariat shall not be disclosed by the Secretariat except with the express consent of the person to whom such information relates.

Disclosure of personal information to third-party funding agencies

6.7 (1) Where any activity of the Secretariat is funded by any third-party, the submission of an application by the individual, subject to rule 6.6), serves as consent by the individual that his personal information may be disclosed to that agency for the purposes of any audits, approvals or non-objections by the third-party.

(2) Rule 6.7 (1) is conditional upon the Secretariat informing the individual at the relevant time, that the personal information required may be requested and made available to the third-party funding agency, for the programme for which funding was received.

(3) Without prejudice to the aforementioned, the transfer to a third-party of personal data that is to undergo processing may only take place subject to the provisions of these Rules and provided that the third-party to which the data is to be transferred ensures comparable levels of protection.

(4) Notwithstanding Rule 6.7 (1), in transferring such information to a third-party, the data controller under whose control the personal information resides, shall make an assessment of the third-party's data protection policy or where such policy is inadequate enter into the appropriate agreement with the third-party to ensure the protection of personal information.

6.8 The Secretariat shall, where information held by it is being transferred as electronic communications data, either internally or externally, ensure the privacy and security of all data transferred.

PART 7

RIGHTS OF THE DATA SUBJECT (INDIVIDUAL)

Contents of this Part

Scope of this Part	Rule 7.1
Right of access to personal information	Rule 7.2
Refusal of access of personal information	Rule 7.3
Severance of exempt information	Rule 7.4
Delegation of rights of individual	Rule 7.5
Application for personal information	Rule 7.6
Right of an individual to correction and data portability	Rule 7.7

Scope of this Part

7.1 This Part addresses the individual's right to access personal information from the Secretariat and the circumstances in which the Secretariat can refuse the individual's right of access.

Right of access to personal information

7.2 (1) Subject to rule 7.3, every individual has a right to and shall on request, be given access to—

- (a) personal information about that individual contained in a personal information bank in the custody and control of the Secretariat; and
- (b) any other personal information about the individual under the custody or control of the Secretariat with respect to which the individual is able to provide sufficiently specific information on the location of the information as to render it reasonably retrievable by the Secretariat.

(2) A request for access to personal information under the control of the Secretariat shall be made to the Secretariat in writing.

(3) The Secretary-General or designated representative may, where reasonable and in appropriate circumstances, provide personal information in accordance with the provisions of these Rules in response to an oral request.

Refusal of access of personal information

7.3 (1) The Secretariat may refuse to disclose personal information to the individual to whom the information relates where—

- (a) the disclosure would constitute an unjustified invasion of another individual's personal privacy;
- (b) the disclosure could reasonably be expected to reveal information supplied in confidence;

- (c) it is evaluative or opinion material compiled solely for the purpose of determining suitability, eligibility or qualifications for employment or for the awarding of contracts and other benefits where the disclosure would reveal the identity of a source who furnished information to the institution in circumstances where it may reasonably be assumed that the identity of the source would be held in confidence.
- (d) it is information that is subject to legal privilege or obtained in the course of an investigation or legal proceeding; or
- (e) it is health or medical information where the Data Controller has a reasonable belief that providing access to the information could harm the health or safety of any person.

(2) The Secretariat may disregard requests from an individual for access to that individual's personal information where it would unreasonably interfere with the operations of the public body because of the repetitious or systematic nature of the requests or the requests are frivolous or vexatious.

Severance of exempt information

7.4 (1) The Secretariat shall make every effort to sever information that is exempt from disclosure pursuant to rule 7.3 from information that may be made available to the individual requesting access to his personal information and make the non-exempt information available.

(2) Where acknowledgment of the existence of information that is exempt from disclosure would reveal critical information about the nature or contents of the information, the Secretariat may refuse to disclose the existence of the information.

Delegation of rights of the individual

7.5 Any right or power conferred on an individual by these Rules may be exercised—

- (a) where the individual is deceased, by the individual's personal representative if the exercise of the right or power relates to the administration of the individual's estate;
- (b) by the individual's attorney under a power of attorney;
- (c) by the individual's guardian; or
- (d) where the individual is less than eighteen years of age, by a person who has lawful custody of the individual.

Application for personal information

7.6 (1) Upon an application by an individual for access to his personal information the Secretariat shall within thirty (30) days of the request being received where access is –

- (a) granted in whole or in part, give the information to the individual who made the request; or
- (b) refused in whole or in part, give the individual who made the request a written response stating—
 - (i) that the information does not exist; or

- (ii) the specific provision of these Rules on which a refusal could reasonably be expected to be based if the information existed; or
- (c) refused in whole or in part, give the individual who made the request, information regarding the right of appeal to an independent review committee to be constituted accordingly by the Secretary-General or the designated representative of the Secretary General.

(2) Where access is granted in whole or in part, the Secretariat shall ensure that the information is available in a comprehensive form, including where reasonable, comprehensible to an individual with a sensorial disability.

Right of an individual to correction and data portability

7.7(1) In the case of an individual who wishes to: -

- (a) verify personal data stored on his behalf by the Secretariat;
- (b) have it modified, corrected or deleted;
- (c) restrict the processing,
- (d) object to it; or
- (e) exercise the right of data portability.

said individual shall provide at least fourteen (14) days' notice to the data controller under whose request the personal information was provided and the Secretariat shall, subject to rules 7.3 and 7.4, comply with said notice.

(2) Any correction of personal data shall be taken into consideration from a data protection point of view.

(3) Any request for deletion or amendment of personal information may lead to alteration of the terms of the application, invitation to treat, offer, acceptance or contract and may lead to rejection of the application, offer, acceptance or contract.

(4) For the purposes of rule 7.7(1)(e) an individual whose information is held by the Secretariat shall, upon request, receive the personal data concerning him or her, which he or she has provided to a data controller, in a structured, commonly used format and have the right to transmit that data to another data controller without hindrance from the data controller to which the personal data would have been provided, where the processing is -

- (a) based on consent; and
- (b) carried out by automated means.

(5) In exercising his or her right to data portability pursuant to rule 7.7(4), the individual shall have the right to have the personal data transmitted directly from one data controller to another, where technically feasible.

PART 8
THIRD-PARTY PROCESSING

Contents of this Part

Scope of this Part	Rule 8.1
Compliance	Rule 8.2
Contract with Data Processor	Rule 8.3

Scope of this Part

8.1 This Part deals with circumstances in which the Secretariat uses a third-party, to process the personal data of any individuals or a group of individuals.

Compliance

8.2 A data controller who uses a data processor must ensure that the data processor:

- (a) provides sufficient guarantees regarding the technical and organisational security measures in place; and
- (b) takes reasonable steps to ensure compliance with those measures.

Contract with Data Processor

8.3 (1) In pursuance of the aforementioned, the Secretariat shall, if not satisfied with the third-party processor's data protection policy enter into a contract with the third-party processor to ensure the protection of personal information of any person.

(2) Third-party data processor contracts should include requirements to:

- (a) only process personal data according to the data controller's instructions;
- (b) only use personal data for specified purposes;
- (c) implement appropriate technical, physical, and organisational security measures to protect against the unauthorised access, alteration, disclosure, accidental loss or destruction of the data;
- (d) comply with any security obligations imposed on the data controller;
- (e) comply with all applicable laws and regulations including data protection, information security, and security breach notification laws;
- (f) return or securely delete personal data when the data processor no longer needs it for the specified purposes of processing;
- (g) comply with certain restrictions on the third-party's use of subcontractors or prohibit all subcontractors; and
- (h) permit the data controller to audit the third-party's data handling practices.