Personal Information Protection Policy

P014
2021
VERSION: 1.1

APPLICATION
ALL Secretariat staff including those based at PTI Offices, whether full-time, temporary or casual

ALL non-staff personnel, including contractors, consultants, and implementing partners

RESPONSIBILITY
Director Operations through the relevant information custodians across the Secretariat.

PURPOSE

Provide the framework for how the Secretariat will process and protect any personal information that it collects in its day-to-day operations.

POLICY

1 Introduction

1.1 The Secretariat acknowledges the right to protection of personal information, in accordance with the Secretariat's values and international best practices.

1.2 This Policy describes the practices of the Secretariat to protect and safeguard the individual's privacy whose information is being collected and processed. It explains how the personal information is collected, for what purposes and how it is used.

1.3 Common examples of personal information that the Secretariat would collect include a person's name and address, photograph, employment history, passport details, pension and tax identification number, business and employment references, health information, contact details, or their geo-location.

2 Principles

2.1 This Policy is underpinned by the following principles:

(a) **Fair and legitimate processing** – personal information should be processed in a fair manner in accordance with the Secretariat's mandates and governing instruments and based on the following-

(i) the consent of the information subject;

(ii) the best interest of the information subject, consistent with the mandates of the Secretariat; or

(iii) any other legal basis specifically identified by the Secretariat.

(b) **Purpose specification** – personal information should be processed for specified purposes only, which are consistent with the mandates of the Secretariat and consider the balancing of relevant rights, freedoms and interests. Personal data should not be processed in ways that are incompatible with such purposes.

(c) **Proportionality and necessity** – the processing of personal information should be relevant, limited and adequate to what is necessary in relation to the specified purposes of personal information processing.

(d) **Retention** – personal information should only be retained for the time that is necessary and for the specified purpose.

PACIFIC ISLANDS FORUM SECRETARIAT

(e) **Accuracy** – personal information should be accurate and, where necessary, up to date to fulfill the specific purposes. Every reasonable step must be taken to ensure that personal information that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

(f) **Confidentiality** – personal information should be processed with due regard to confidentiality.

(g) **Security** – appropriate organisational, administrative, physical and technical safeguards and procedures should be implemented to protect the security of personal information, including against or from unauthorised or accidental access, damage, loss or other risks presented by information processing.

(h) **Transparency** – processing of personal information should be carried with transparency to the information subjects, as appropriate and wherever possible. This should include, for example, provision of information about the processing of their personal information as well as information on how to request access, verification, rectification, and/or deletion of that personal information, insofar as the specified purpose for which personal information is processed is not frustrated.

(i) **Transfers** – in carrying out the Secretariat's mandated activities, personal information may be transferred to a third party, provided that, under the circumstances, the Secretariat satisfies itself that the third party affords appropriate protection for the personal information.

(j) **Accountability** – adequate policies and mechanisms should be in place to adhere to these principles.

3 Collection of Personal Information

3.1 The privacy and security of personal information is of utmost importance to the Secretariat. Personal information will only be collected for purposes that are related to the Secretariat's official functions and activities. These purposes include the following but are not limited to-

(a) developing policy advice for Member states;

(b) disseminating correspondences and papers to Member states and Forum Dialogue Partners;

(c) conducting research, surveys and meetings with stakeholders of Member states;

(d) subscribing to updates on the Secretariat's website;

(e) seeking feedback on the Secretariat's website and activities to improve its service delivery;

(f) providing information about the Secretariat's projects, grants and activities;

(g) organising travel and other logistical arrangements for participation at Forum meetings and events; and

(h) selection, recruitment, engagement and management of staff, consultants and contactors.

3.2 The Secretariat may collect personal information directly from the individual, either in person, in correspondence, in an application form, through tender submissions, or over the phone or internet. The Secretariat may also collect personal information from another third party, for instance from other development partners or through a publicly available source.

3.3 The Secretariat also uses third-party analytics provider - Google Analytics - to collect information about the usage of its website to help improve service delivery to the targeted audience. Google Analytics uses cookies and various other technologies to collect information about the usage of the Secretariat's website and to report website trends, without storing any personal information.

4 Confidentiality

4.1 The Secretariat is committed to preserving the levels of confidentiality necessary to protect its reputation as an international intergovernmental organisation. All staff and non-staff personnel are required to sign an *Oath to Confidentiality* upon acceptance of employment with the Secretariat or when participating in a tender evaluation process. The Secretariat will also observe any additional confidentiality provisions in arrangements where it holds or collects personal information on behalf of other development partners.

5 Disclosure

5.1 The Secretariat will generally only disclose personal information where-

(a) the disclosure was consented to either at the time of collection, or afterwards;

(b) it is necessary to fulfil the purposes of the original collection, for instance if the Secretariat collected the information on behalf of the Member states;

(c) if the Secretariat is working with a development partner or other agency assisting with delivering a project or grant; and

(d) it is necessary for the Secretariat to refer information to law enforcement entities (e.g. Immigration and tax offices).

6 Storage and Security of Personal Information

6.1 The Secretariat will take all necessary steps under its *Information Security Policy* to protect the security of the personal information it holds from internal and external threats. These steps include password protection for electronic files, securing paper files in locked cabinets, and physical access restrictions.

6.2 Personal information held by the Secretariat is managed securely through its recordkeeping system as per the *Records Management Policy and Procedures.* Such information will be retained for the time that is necessary to fulfill the Secretariat's purposes. This assessment needs to be made on case-by-case basis and will include factors such as the need to keep financial, procurement or employment records for audit purposes.

7 Access or Correction to Personal Information

7.1 Personal information will be kept as accurate and, where necessary, up to date to fulfill the Secretariat's official purposes. In the event an individual wishes to access their personal information held by the Secretariat, or to correct that personal information, they can email the Director Operations on info@forumsec.org with the subject "Subject Access Request". The Director Operations will direct the request to the relevant information custodian within the Secretariat to facilitate and respond to the individual.

8 Complaint

8.1 The Secretariat takes any personal information breach seriously and will make all efforts to protect individual's personal information from misuse, interference and loss; and from unauthorised access, modification or disclosure.

8.2 A person may complain to the Secretariat about how it has handled their personal information. In that case, the individual should write to the Director Operations on info@forumsec.org, providing the following information-

- what happened;
- when it happened (including dates);
- what personal information of the individual was affected;
- who did it (include individual names if known);
- how and when the individual found out about it;
- the individual's contact details; and
- other relevant information, including what, if any, outcome the individual is expecting from the complaint process.

8.3 The Secretariat will consider all the information and determine what action, if any, should be taken to resolve the complaint. An initial response to the complaint would be provided within 10 working days.

8.4 Should the individual be not satisfied with the response, they may submit a complaint to the Secretary General on info@forumsec.org.

9 SPECIFIC DIRECTIVES

9.1 Notwithstanding any clause in this Policy, the Secretary General at any time may at their discretion where the policy is silent or ambiguous make a judgment call, provided that the minimum requirements and standards in the PIF Regulations are met.

9.2 Notwithstanding any clause in this Policy, the Secretary General at any time may at his/her discretion deviate from this policy, provided that the minimum requirements and standards in the PIF Regulations are met. Any such action shall be treated as an exception to policy.

9.3 Decisions made under 9.1 and 9.2 must be fully documented, recorded and forwarded to the Risk and Compliance Officer and the Policy and Procedure Writer.

9.4 A staff member who is delegated authority under the *Delegations Policy 2021* will be able to exercise powers within the scope granted.

DEFINITIONS

This section is used to describe the meaning of a word, phrase, acronym or other set of symbols that is being used in the context of this policy and in conjunction with other related governance instruments.

Archives - are either physical or electronic recorded information that has been deemed of sufficient administrative, fiscal, legal, historical or informational value as to warrant retention by the Secretariat.

Personal information - any information relating to an identified or reasonably identifiable individual. An identifiable individual is one who can be identified, directly or indirectly, in particular by reference to (i) an identifier such as a name, an identification number, audiovisual materials, location information, an online identifier, (ii) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual or (iii) assessments of the status and/or specific needs, such as in the context of assistance programmes.

Personal information breach - a breach of security leading to the accidental or unauthorized destruction, loss, alteration, disclosure, access, or unplanned loss of availability of personal information that is unencrypted or can be decrypted.

REVIEW

This Policy will be reviewed from time to time, and any amendments will be notified by posting an updated version on the Secretariat's intranet and website.

HISTORY

Approved:	28 July 2023
Effective:	22 March 2023
Authorisation:	Acting Sectary General – Dr. Filimon Manoni
Revision #1:	Inclusion of principles into policy under Section 2.

RELATED DOCUMENTS

Secretariat's Code of Conduct and Values 2018