



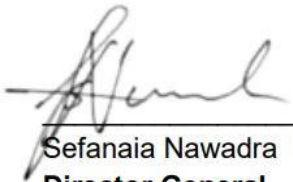
**SECRETARIAT OF THE PACIFIC
REGIONAL ENVIRONMENT
PROGRAMME
(SPREP)**

PERSONAL DATA POLICY

December 2024

Distribution List and Document Version Control

I hereby approve the Personal Data Policy for SPREP to come into effect on 1 January 2025.


Sefanaia Nawadra
Director General

Date: December 2024



This table tracks all revisions and updates to this policy from time to time. It attempts to capture the date of when the policy has been reviewed and updated together with the official designation and signature of the Director General or proxy for approval. A summary of the changes that are made to this policy should be provided in a separate form and attached as an “Addendum”.

| Policy Reviewed and Updated | | | |
|-----------------------------|-------------|-----------|-----------------|
| Date | Designation | Signature | Addendum Number |
| | | | |
| | | | |
| | | | |

SPREP PERSONAL DATA POLICY**Contents**

| | | |
|------------|--|----------|
| 1) | Introduction..... | 4 |
| 2) | Definitions..... | 4 |
| 3) | Subjects | 4 |
| 4) | Purpose..... | 5 |
| 5) | Scope..... | 5 |
| 6) | Principles and application | 5 |
| 7) | Disclosure of Personal Data | 6 |
| 8) | Rights of the Subject..... | 6 |
| 9) | Data breach..... | 7 |
| 10) | Complaints..... | 7 |
| 11) | Links..... | 7 |
| 12) | Cookies | 7 |
| 13) | Data Protection..... | 7 |
| 14) | Related Polices..... | 8 |
| 15) | Review of the Policy..... | 8 |

1) Introduction

SPREP is committed to and will take all reasonable steps to protect your Personal Data

2) Definitions

- i) **Event** means any meeting, workshop, conference, and the like.
- ii) **Non-SPREP Staff** means secondments and placements; volunteers; young professionals; consultants; interns and work attachments; temps; and University of Newcastle Researchers under a Scholarship Agreement.
- iii) **Personal Data** (also known as Personal Information or Personally Identifiable Information) is any information relating to an identified or identifiable natural person.

Personal Data may include your:

designation, name(s), gender, physical address, email address, telephone number, mobile number, date and place of birth, nationality, details of family members, health status, ethnicity, country of residence, personal description, CV or biography, religion, photograph and images, ID or passport information, signature, fingerprint, language preference, job title, position, employer, remuneration and benefits; areas of expertise, emergency contact information, bank account details, CCTV footage, etc.

The following information is collected from your visits to the SPREP website:

- technical information, including the Internet protocol (IP) address used to connect your computer or mobile device to the Internet, online identifiers, your login information, browser type and version, time zone setting, browser plug-in types and versions, operating system and platform.
- information about your visit such as the full Uniform Resource Locators (URL) as well as date and time.

iv) **Sensitive Personal Data** includes the following types of information:

- racial or ethnic origin.
- political opinions.
- religious or philosophical beliefs.
- trade union membership.
- genetic data.
- health and medical data.
- information relating to an investigation.
- data related to a person's sex life or sexual orientation.
- biometric data for ID purposes.

v) **SPREP Staff** means an employee of SPREP under a Contract of Employment.

vi) **Subject** means a physical person from whom SPREP collects Personal Data.

3) Subjects

Personal Data is collected from Subjects, including:

- i) SPREP staff and SPREP non-staff.
- ii) country and institutional Focal Points.
- iii) applicants for jobs or tenders.

- iv) consultants.
- v) experts.
- vi) Event participants.
- vii) visitors.
- viii) staff of national environmental and related agencies.
- ix) project stakeholders.
- x) personnel of service providers, partners and donors.

4) Purpose

The purpose of this Policy is to outline the rules and principles followed by SPREP when collecting, using and disclosing Personal Data of Subjects.

5) Scope

This Policy applies to all Personal Data of Subjects held by SPREP. Collection of Personal Data from Subjects below the age of 18 will not be collected without prior consent from a parent or legal guardian.

6) Principles and application

a) Legitimate Purpose

Personal Data will be collected for a purpose related to SPREP's functions and activities such as:

- Organising travel and logistical arrangements for participation at an Event.
- Conducting Events or other activities with Member States, partners, etc.
- Recruitment and management of SPREP Staff and SPREP non-Staff.
- Providing policy or advice to Member States, partners, etc.
- Disseminating correspondence to Member States, partners, etc.
- Providing information about SPREP's work.
- Enhancing users' website browsing experience.
- To meet **contractual obligations** entered into by the Subject.
- To comply with SPREP's **legal obligations**.
- For tasks carried out in the **public interest** or exercise of authority vested in SPREP.
- For the purposes of **legitimate interests** pursued by SPREP except where such interests are overridden by the interests of fundamental rights and freedoms of the Subject which require protection of personal data.
- If the Subject gives their explicit **consent** or if the processing is necessary.
- To protect the Subject's **vital interests**.

b) Transparency

Personal Data will be collected in a transparent manner that allows the Subject to clearly understand what information is needed, the purpose it is needed for and the process for collecting, using and disclosing it.

c) Relevance and adequacy

Personal Data collected by SPREP must be relevant and limited to only what is necessary for the purpose for which it is required.

d) Accuracy

Personal Data will be recorded accurately and will be updated, amended, or deleted as required.

e) **Confidentiality**

- i) Personal Data will be safeguarded and is accessible only to authorised personnel.
- ii) All who handle personal data on behalf of SPREP will be subject to SPREP's confidentiality agreement.
- iii) SPREP will observe confidentiality when holding or collecting Personal Data on behalf of a third party.

f) **Security**

SPREP will ensure that Personal Data is safeguarded, securely stored and managed in accordance with applicable SPREP policies to prevent unauthorised use or disclosure.

Personal Data that is deemed sensitive will be handled with extra security, for example, by use of pseudonymisation and encryption.

g) **Currency**

Personal Data will be retained for no longer than is necessary to fulfil the purpose for which it was collected unless a longer period is required under another SPREP policy or because of a legal requirement. Personal data that is no longer required will be destroyed in a secure manner.

7) **Disclosure of Personal Data**

SPREP will only disclose Personal Data:

- i) To fulfil the purpose for which the information was collected for example recruitment, tenders, arranging travel and logistical arrangements for meetings etc.
- ii) Where the disclosure was consented to either at the time of collection, or afterwards.
- iii) Where there is a legal requirement directing release of the information to a third party.
- iv) Emergency situations.

Before disclosing your Personal Data to a third party, SPREP will check that the third party has a personal data policy that safeguards the data and that the data is used solely for the purpose stipulated by SPREP.

8) **Rights of the Subject**

a) **Right to information**

When collecting Personal Data from a Subject, SPREP should inform them of the following:

- i) The purpose for which the Personal Data is being collected.
- ii) Whether the Personal Data will be transferred to external parties.
- iii) The importance of the Subject providing accurate and complete information.
- iv) The Subject's duty to keep SPREP informed of changes to their Personal Data.
- v) Consequences for refusing or failing to provide the requested Personal Data.

b) **Right to object**

- i) The Subject has the right to withhold consent, in full or in part, to the collection of their Personal Data. SPREP will inform the Subject of the consequences of withholding Personal Data.

c) **Right to access**

The Subject has the right to request from SPREP,

- i) a copy of their Personal Data.
- ii) information on how their Personal Data has been used.

d) **Right to restrict use or disclosure**

- i) The Subject may request restrictions regarding the use or disclosure of their Personal Data. SPREP will inform the Subject of the consequences, if any, of such restrictions.

e) **Right to correction and deletion**

- i) The Subject may request the correction or deletion of Personal Data that is inaccurate, incomplete, unnecessary, or excessive. SPREP may request proof relating to the inaccuracy incompleteness, etc.

9) **Data breach**

A data breach occurs when personal data has been accidentally or unlawfully lost, altered, disclosed, destroyed, or accessed. SPREP staff, upon discovering the breach must, where the breach is likely to lead to more than a minor risk or is likely to result in serious harm to the Subject:

- i) Report the breach to SPREP_IT@sprep.org and Legal@sprep.org.
- ii) Inform the Subject affected by the breach without undue delay and in the case of Sensitive Personal Data, within 48 hours.
- iii) Inform other relevant parties on advice from Legal.

Examples of data breaches:

- Lost or stolen laptops, removable storage devices, or paper records containing Personal Data.
- Computer hard disk drives being thrown away or recycled without the contents first being erased.
- Databases or systems with Personal Data being hacked or illegally accessed.
- SPREP staff accessing or disclosing Personal Data without authorisation.
- Paper documents taken from recycling bins, rubbish bins or shredding machines.
- Personal Data sent to the wrong physical or email address.
- Personal Data released because of deceit or fraud.

10) **Complaints**

SPREP takes any Personal Data complaint seriously. Complaints regarding SPREP's handling of a Subject's Personal Data must be in writing and lodged with Legal@sprep.org and all relevant details provided along with the outcome that is being sought. SPREP will provide an initial response to the complainant within 7 working days.

11) **Links**

SPREP systems and website may contain links to other websites. This should not be construed as constituting any endorsement or approval of that website's ability to protect your Personal Data. It is your responsibility to check if such websites secure your Personal Data from unauthorised collection, use or disclosure.

12) **Cookies**

SPREP uses cookies to allow for better browsing of its website. Some cookies may collect Personal Data from you. You will be asked for your consent before being sent a cookie.

13) **Data Protection**

SPREP Legal will oversee compliance with this policy by SPREP, including arranging of trainings and audits.

14) Related Policies

- i) Access Control Policy (security of SPREP's networks, systems and applications)
- ii) Email Policy (rules for proper use of email)
- iii) Information and Communications Technology (ICT) Strategy 2023-2028 (how data fits within SPREP's ICT ecosystem)
- iv) Information and Knowledge Management Strategy (IKM) 2022-2027 (how SPREP treats data, information and knowledge)
- v) Information Security Policy (protection of information and response to breaches)
- vi) Internet Policy (acceptable uses of the internet)
- vii) Organisational Data Policy (principles regarding data storage and handling and different levels of disclosure)
- viii) Records Management Policy (rules for access to records)
- ix) Staff Regulations 2012 (rules relating to staff conduct and staff contracts and related matters).

15) Review of the Policy

This Policy will be reviewed at least every 3 years and changes made without prior notification.