Privacy Policy for International Strategic Planning Services (ISPS)

Table of Contents

Effective Date: April 30, 2025
Website: https://isps.space
Operated by: International Strategic Planning Services (ISPS), Suva, Fiji

1. Introduction

At the International Strategic Planning Services (ISPS), we are committed to protecting the privacy and security of our users' personal information. This Privacy Policy outlines how we collect, use, store, and protect your data when you visit our website, https://isps.space, engage with the Pacific Project and Funding Intelligence Hub, or interact with our services, including the secure intelligence oversight module and AI chatbot. As a Pacific-led organization serving all Pacific Island Countries and Territories (PICTs), with support from the Melanesian Spearhead Group (MSG), regional NGOs, and Island administrations, we prioritize transparency, cultural sensitivity, and compliance with international and regional data protection laws, including the General Data Protection Regulation (GDPR) and Fiji's Data Protection Act.

This policy applies to all users, including individuals, organizations, government entities, and stakeholders accessing our services. By using our website or services, you consent to the data practices described in this policy. If you have any questions, please contact us at privacy@isps.space.

2. Information We Collect

We collect information to provide, improve, and personalize our services, including the Pacific Project and Funding Intelligence Hub, which offers project and funding intelligence, capacity-building resources, and secure intelligence oversight for PICTs. The types of information we collect include:

2.1 Personal Information

- **Account Information**: When you register for the Hub, we may collect your name, email address, organization name, job title, country of residence, and contact details (e.g., phone number).
- **Subscription Information**: For premium users, we collect billing information (e.g., credit card details, billing address) processed securely via third-party payment processors.
- **Authorized User Data**: For access to the secure intelligence oversight module, we collect additional verification data (e.g., government ID numbers, institutional affiliations) to ensure authorized access.

- **Communication Data**: Information you provide when contacting us via email (privacy@isps.space), phone (+679 123 4567), or the AI chatbot, including inquiries, feedback, or support requests.

2.2 Non-Personal Information

- **Usage Data**: We collect data on how you interact with our website and services, such as pages visited, time spent, clicks, and search queries within the Hub.
- **Device Information**: We collect technical data, including IP address, browser type, operating system, and device identifiers, to optimize performance and security.
- **Cookies and Tracking Technologies**: We use cookies, web beacons, and similar technologies to enhance user experience, analyze traffic, and deliver personalized content. You can manage cookie preferences via your browser settings.
- **Aggregated Data**: We collect anonymized data for statistical analysis, such as the number of users from Melanesia, Polynesia, or Micronesia, to improve our services.

2.3 Sensitive Data

- **Intelligence Module Data**: For authorized users (e.g., Island administration officials), we process sensitive data related to donor reliability and geopolitical risk assessments, stored securely with blockchain encryption.
- **Cultural Data**: We may collect data on Pacific cultural practices (e.g., kastom, fa'a Samoa) to ensure project alignment, handled with utmost respect for community values.

3. How We Collect Information

We collect information through:

- **Direct Interactions**: When you register, subscribe, submit forms, use the AI chatbot, or contact us.
- **Automated Technologies**: Via cookies, server logs, and analytics tools (e.g., Google Analytics) when you visit our website or use the Hub.
- **Third Parties**: From partners like the Pacific Community (SPC), Pacific Islands Forum (PIF), or payment processors, with your consent or as permitted by law.

- **Public Sources**: From publicly available data (e.g., government websites) to populate the project and stakeholder databases.

4. How We Use Your Information

We use your information to deliver, improve, and secure our services while respecting Pacific cultural values and geopolitical neutrality. Specific purposes include:

Service Delivery:

- Provide access to the Pacific Project and Funding Intelligence Hub, including project databases, funding trackers, and capacity-building resources.
- Personalize recommendations using AI analytics, such as matching funding opportunities to your organization's needs.
- Facilitate access to the secure intelligence oversight module for authorized users, ensuring transparency in donor assessments.

Communication:

- Respond to inquiries, provide support, and send updates about projects, funding opportunities, or workshops.
- Deliver multilingual support (English, French, Bislama, Tongan, Samoan) via the AI chatbot.

Analytics and Improvement:

- Analyze usage data to optimize website performance, enhance user experience, and tailor content for PICTs.
- Track Key Performance Indicators (KPIs), such as user engagement and funding facilitated, to measure impact.

Security and Compliance:

- Protect against unauthorized access, fraud, or data breaches using blockchain encryption and AES-256 standards.
- Verify authorized users for the intelligence module to prevent misuse.
- Ensure compliance with data protection laws and Pacific data sovereignty requirements.

Cultural and Regional Alignment:

- Use cultural data to ensure projects respect Pacific practices, avoiding external interference as seen in global aid controversies (e.g., USAID allegations).
- Support Pacific-led development, prioritizing inclusivity for women, youth, and marginalized groups.

We do not use your data to support or promote carbon credit schemes or taxes associated with contested global warming narratives, aligning with skepticism about such initiatives.

5. How We Share Your Information

We share your information only when necessary and with strict safeguards:

- **Service Providers**: We engage trusted third parties (e.g., AWS for hosting, payment processors like Stripe) to perform functions like data storage, analytics, or billing. These providers are bound by confidentiality agreements and comply with data protection laws.
- **Regional Partners**: We share aggregated or anonymized data with SPC, PIF, MSG, or Pacific NGOs to improve project coordination and validate data, with your consent where required.
- **Intelligence Oversight**: Authorized user data and intelligence reports are shared securely with Pacific security bodies (e.g., PIF's Joint Heads of Pacific Security, INTERPOL Pacific) to ensure aid transparency, using blockchain for auditability.
- **Legal Obligations**: We may disclose data to comply with legal requirements, such as court orders or Pacific data protection regulations, or to protect our rights and safety.
- **Business Transfers**: In the event of a merger, acquisition, or asset sale, your data may be transferred to a successor entity, with notice and continued protection.

We do not sell, rent, or trade your personal information to third parties for marketing purposes.

5. Data Storage and Security

We prioritize the security of your data, especially given the Pacific's geopolitical sensitivities and the sensitive nature of the intelligence oversight module:

- **Storage**: Data is stored on Pacific-based servers (e.g., in Fiji) to comply with regional data sovereignty laws, with backups on AWS GovCloud for redundancy.
- **Security Measures**:
  - AES-256 encryption for all data transmissions and storage.
  - Blockchain technology for transparent, tamper-proof tracking of aid flows and intelligence reports.
  - Multi-factor authentication for secure module access.
  - Regular penetration testing and DDoS protection to prevent cyber threats.
- **Retention**: We retain personal information only as long as necessary to fulfill the purposes outlined in this policy (e.g., active user accounts) or as required by law. Non-personal data may be retained indefinitely for analytics.
- **Data Deletion**: Upon account closure or request, we delete personal information within 30 days, except where retention is legally required.

6. Your Rights and Choices

You have the following rights regarding your personal information, subject to applicable laws:

- **Access**: Request a copy of the data we hold about you.
- **Correction**: Request updates to inaccurate or incomplete data.
- **Deletion**: Request deletion of your data, except where retention is required by law.
- **Restriction**: Request that we limit the processing of your data in certain circumstances.
- **Objection**: Object to processing based on legitimate interests (e.g., analytics).
- **Data Portability**: Request a transferable copy of your data in a structured format.
- **Withdraw Consent**: Withdraw consent for data processing at any time, where applicable.

To exercise these rights, contact us at privacy@isps.space or +679 123 4567. We will respond within 30 days, as required by GDPR and Pacific laws. You may also lodge a complaint with a data protection authority, such as Fiji's Office of the Information Commissioner.

Cookie Preferences: Manage cookies via our website's cookie banner or your browser settings. Disabling cookies may affect functionality.

Do Not Track: Our website respects "Do Not Track" signals, limiting tracking when enabled.

7. International Data Transfers

As a Pacific-focused organization, we prioritize local data storage. However, some service providers (e.g., AWS, Google Analytics) may process data outside the Pacific. We ensure:

- **Adequate Protection**: Data transfers comply with GDPR's standard contractual clauses or equivalent safeguards.
- **Pacific Sovereignty**: Sensitive data (e.g., intelligence reports) remains on Pacific servers, with blockchain ensuring transparency.
- **User Consent**: We obtain consent for international transfers where required, clearly disclosing the purpose and recipients.

8. Third-Party Links and Services

Our website and Hub may contain links to third-party sites (e.g., SPC, PIF, donor portals). We are not responsible for their privacy practices. We encourage you to review their policies before sharing information.

9. Children's Privacy

Our services are not intended for individuals under 16. We do not knowingly collect personal information from children. If we learn that a child's data has been collected, we will delete it immediately. Contact us at privacy@isps.space if you believe this has occurred.

10. Special Considerations for Pacific Context

Given the Pacific's unique cultural, geopolitical, and environmental context, we take additional steps to protect your data:

- **Cultural Sensitivity**: We handle cultural data (e.g., kastom practices) with respect, consulting community leaders to ensure alignment with Pacific values, avoiding external interference as seen in global aid controversies.
- **Geopolitical Neutrality**: We maintain a “friends to all, enemies to none” approach, using intelligence oversight to ensure aid transparency without bias, particularly amid U.S.-China tensions or West Papua issues.
- **Geoengineering Concerns**: We do not support or collect data for carbon credit schemes or taxes linked to contested global warming narratives. Our focus is on addressing tangible vulnerabilities, such as those caused by geoengineering (e.g., Stratospheric Aerosol Injection) and natural disasters, as outlined in our project database.

11. Changes to This Privacy Policy

We may update this Privacy Policy to reflect changes in our services, legal requirements, or user feedback. We will notify you of significant changes via email or a website notice at least 30 days before they take effect. The updated policy will be posted on https://isps.space/privacy with the new effective date.

12. Contact Us

If you have questions, concerns, or requests regarding this Privacy Policy or our data practices, please contact:

International Strategic Planning Services (ISPS)
Email: privacy@isps.space
Phone: +679 123 4567
Address: ISPS, Suva, Fiji

For data protection inquiries in the Pacific, you may also contact Fiji’s Office of the Information Commissioner or your local data protection authority.

Notes on the Privacy Policy

Compliance with Laws:

- The policy aligns with GDPR for international users, Fiji’s Data Protection Act for Pacific operations, and broader Pacific data sovereignty principles, ensuring applicability across PICTs.

- It addresses the Pacific's limited regulatory frameworks by adopting best practices from GDPR and APEC's Cross-Border Privacy Rules.

Pacific Context:

- The policy emphasizes cultural sensitivity (e.g., respecting kastom, fa'a Samoa) and geopolitical neutrality, reflecting ISPS's Pacific-led mission.
- It incorporates your edit on geoengineering (Stratospheric Aerosol Injection) and skepticism about carbon credits, ensuring the policy distances ISPS from contested climate schemes.

Intelligence Oversight:

- The secure module's data practices (e.g., blockchain, restricted access) are clearly outlined to build trust, addressing concerns from the USAID controversy.
- Sensitive data handling is emphasized to protect Pacific sovereignty.

Accessibility:

- The policy is written in clear language for diverse Pacific audiences, with contact details for easy access.
- Future translations into Bislama, Tongan, or Samoan can be added to enhance accessibility.

Integration with Website:

- The policy should be linked in the footer of the Pacific Project and Funding Intelligence Hub page (as included in the HTML code) and hosted at https://isps.space/privacy.
- Ensure HTTPS and secure hosting to protect user interactions with the policy page.

Customizations:

- The address (Suva, Fiji) and phone number (+679 123 4567) are placeholders based on prior inputs. Replace with ISPS's actual contact details.
- If ISPS has specific data practices (e.g., additional third-party tools, unique user categories), I can refine the policy further.