Pan-African Space Industry_ Data Protection Policy, Privacy, and Confidentiality

Data subjects:

- Users: suppliers, buyers, contractors, service providers, customers, investors
- Temporary Workers: freelancers, consultants, independent contractors, service providers
- Partners
- Employees: staff (full-time/ part-time), contractors, interns, volunteers
- Customers
- General Public

Law: The Pan-African Space Industry (PSI) Data Protection Policy, Privacy, and Confidentiality framework aligns with the Africa Union Data Policy Framework, emphasizing data as a strategic asset vital for innovation and economic growth while upholding human rights and legal compliance. It advocates for collaborative efforts among stakeholders to develop robust data governance mechanisms, including transparent accountability, stringent cybersecurity measures, and ethical data use. The policy promotes cross-border data flows within the continent, capacity-building initiatives, and legal harmonization to create a unified framework that fosters trust, innovation, and economic development while safeguarding privacy and confidentiality in the PSI ecosystem.

Regulator:

The Pan-African Space Industry (PSI) is dedicated to adhering to the highest data protection standards recommended by the Africa Union Commission. PSI will align with established frameworks to ensure robust data governance and regulatory compliance.

- PSI aims to facilitate seamless cross-border data flows within the region, leveraging international frameworks proposed by organizations like the OECD and ASEAN. This collaboration will promote data exchange while safeguarding privacy and data subject rights.
- PSI supports ratification of the AU Convention on Cybersecurity and Personal Data Protection to harmonize data processing practices. PSI encourages exploring additional protocols to address evolving technological advancements.
- PSI recognizes the African Continental Free Trade Agreement (AfCFTA) as vital for promoting regional integration and economic growth within the space industry. PSI commits to engaging with AfCFTA initiatives to advance data governance principles and foster innovation across the continent.

Summary: As PSI progresses towards a comprehensive data protection framework, we prioritize adherence to the highest standards recommended by the Africa Union (AU) and other relevant bodies. While awaiting the development of a dedicated data protection bill, PSI is guided by existing legal provisions that underscore privacy and confidentiality. For instance, the Constitution of Cameroon upholds the right to privacy and correspondence. Furthermore, Law No. 2010/012 of 21 December 2010 on Cybersecurity and Cybercrime in Cameroon addresses crucial aspects such as privacy protection, data retention, and electronic communications confidentiality. PSI is committed to incorporating these principles into our operations and engaging with regional initiatives, such as the African Continental Free Trade Agreement (AfCFTA), to advance data governance principles. As we continue to evolve, PSI remains dedicated to ensuring the security and privacy of all data within our ecosystem, thereby fostering trust and promoting responsible data management practices.

BP : 14 841 Yaoundé, Cameroon
Tel : +237 675 358 795 / +33 669 714 981
Headquater : Yaoundé-Omnisport (Avenue Marc Vivien FOE)
MB Tech & Services
Tax Number N° RC/YAE/2023/A/3644
NIU : P 069 315 998 003 B
Email : info@panafrican.space

1. Introduction

1.1. This Policy sets out the obligations of The Pan-African Space Industry (PSI), hosted by MB Tech & Services, a company legalised in Yaoundé-Cameroon whose registered office is at Yaoundé-Omnisport (Avenue Marc Vivien FOE) hereinafter referred to as "the Organisation'' regarding data protection and the rights of the users and freelancers of PSI's platforms and application(s) hereinafter referred to as "data subjects" in respect of their personal data under Law No. 2010/012 of 21 December 2010 on Cybersecurity and Cybercrime in Cameroon and the highest standards recommended by the Africa Union data protection framework.

1.2. Law No. 2010/012 of 21 December 2010 on Cybersecurity and Cybercrime in Cameroon defines "personal data" means any information relating to an identified or identifiable natural person (a "data subject"), directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural, or social identity (Article 2 of the Directive Harmonising Consumer Protection within CEMAC).

1.3. This Policy sets the Organisation's obligations regarding collecting, processing, transferring, storing, and disposing of personal data. The procedures and principles set out herein must be followed at all times by the Organisation, its employees, agents, contractors, or other parties working on behalf of the Organisation.

1.4. The Organisation is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

2. The Data Protection Principles

2.1. This Policy aims to ensure compliance with the Protection of Personal Information Act in Law No. 2010/012 of 21 December 2010 on Cybersecurity and Cybercrime in Cameroon and the highest standards recommended by the Africa Union data protection framework. The Act sets out the following principles with which any party handling personal data must comply. All personal data must be:

2.1.1. Processed lawfully, fairly, and transparently in relation to the data subject.

2.1.2. Collected for specified, explicit, and legitimate purposes and not further processed in an incompatible manner. Further processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes will not be considered to be incompatible with the initial purposes.

2.1.3. Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

2.1.4. Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, regarding the purposes for which it is processed, is erased, or rectified without delay.

2.1.5. Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for more extended periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, the pursuit of access to justice or statistical purposes in relation thereto, subject to the implementation of the appropriate technical and organisational measures required by the Protection of Personal Information Act in

BP : 14 841 Yaoundé, Cameroon
Tel : +237 675 358 795 / +33 669 714 981
Headquater : Yaoundé-Omnisport (Avenue Marc Vivien FOE)
MB Tech & Services
Tax Number N° RC/YAE/2023/A/3644
NIU : P 069 315 998 003 B
Email : info@panafrican.space

order to safeguard the rights and freedoms of the data subject.

2.1.6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

2.2. Protection of Personal Information Act states that electronic communication network operators and service providers must take all the necessary technical and administrative measures to guarantee the security of the services provided. To that end, they shall be bound to inform users about:

- the risks of using their networks;
- the specific risks of security violation, notably the denial of services distributed, abnormal rerouting, traffic points, traffic and unusual ports, passive and active listening, intrusion, and any other risk;
- the existence of techniques to ensure the security of their communications

3. The Rights of Data Subjects

3.1. The following rights shall be applicable to data subjects ;

In accordance with data protection principles and regulations, PSI recognizes and respects the following rights of data subjects:

3.1.1. **The Right to be Informed**: Data subjects have the right to be informed about collecting, processing, and sharing their personal data. PSI will provide clear and transparent information regarding data processing purposes, the legal basis for processing, and any other relevant details.

3.1.2. **The Right of Access**: Data subjects have the right to request access to their personal data held by PSI. Upon request, PSI will provide data subjects with information about whether their personal data is being processed and for what purposes. PSI will also provide copies of the personal data, along with details about how it is being processed.

3.1.3. **The Right to Rectification**: Data subjects have the right to request the correction of inaccurate or incomplete personal data held by PSI. PSI will promptly rectify any inaccuracies or incompleteness upon receiving a valid request from the data subject.

3.1.4. **The Right to Erasure ('Right to be Forgotten')**: In certain circumstances, data subjects have the right to request the deletion or removal of their personal data. PSI will honor such requests, provided that there are no legitimate grounds for retaining the data, as outlined in applicable data protection laws and regulations.

3.1.5. **The Right to Restrict Processing**: Under certain conditions, data subjects have the right to request the restriction of the processing of their personal data. PSI will limit the processing of personal data upon receiving a valid request from the data subject in accordance with applicable legal requirements.

3.1.6. **The Right to Data Portability**: Data subjects have the right to receive their personal data in a structured, commonly used, and machine-readable format, and to transmit that data to another controller without hindrance from PSI. PSI will facilitate the exercise of this right upon request from the data subject, where technically feasible.

BP : 14 841 Yaoundé, Cameroon
Tel : +237 675 358 795 / +33 669 714 981
Headquater : Yaoundé-Omnisport (Avenue Marc Vivien FOE)
MB Tech & Services
Tax Number N° RC/YAE/2023/A/3644
NIU : P 069 315 998 003 B
Email : info@panafrican.space

3.1.7. **The Right to Object**: Data subjects have the right to object to the processing of their personal data in certain circumstances, including processing for direct marketing purposes or where the processing is based on legitimate interests. PSI will cease processing personal data upon receiving a valid objection from the data subject unless there are compelling legitimate grounds for the processing that override the interests, rights, and freedoms of the data subject.

3.1.8. **Rights with Respect to Automated Decision-Making and Profiling**: Data subjects have the right not to be subject to decisions based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects them. PSI will ensure that appropriate safeguards are in place when engaging in automated decision-making processes. It will provide data subjects with the right to challenge such decisions, request human intervention, and express their point of view.

4. Lawful, Fair, and Transparent Data Processing

4.1. The Protection of Personal Information Act seeks to ensure that personal data is processed lawfully, fairly, and transparently without adversely affecting the data subject's rights. The Act states that processing of personal data will be lawful under the following considerations:

4.1.1. Operators of information systems shall take every technical and administrative measure to ensure the security of services offered. To this end, they shall have standardised systems enabling them to at all times identify, assess, process or manage any risk relating to the security of the information systems of the services provided directly or indirectly.

4.1.2. Operators of information systems shall set up technical mechanisms to avoid any hitches that may be prejudicial to the steady functioning of systems, their integrity, authentication, non-repudiation by third-party users, confidentiality of data, and physical security.

4.1.3. The mechanisms provided for in Subsection 2 above shall be subject to the approval and visa of the Agency.

4.1.4. Information systems platforms shall be protected against any radiation or intrusion that may impair the integrity of data transmitted and any other external attack, notably through intrusion detection systems.

4.2. If the personal data in question is “special category data” (also known as “sensitive personal data”) (for example, data concerning the data subject’s race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation), at least one of the following conditions must be met:

4.2.1. The data subject has given their explicit consent to the processing of such data for one or more specified purposes (Unless the law prohibits them from doing so);

4.2.2. The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject insofar as the laws of Cameroon authorise it;

4.2.3. The 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;

4.2.4. The processing relates to personal data, which is clearly made public by the data subject;

BP : 14 841 Yaoundé, Cameroon
Tel : +237 675 358 795 / +33 669 714 981
Headquater : Yaoundé-Omnisport (Avenue Marc Vivien FOE)
MB Tech & Services
Tax Number N° RC/YAE/2023/A/3644
NIU : P 069 315 998 003 B
Email : info@panafrican.space

4.2.5. The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;

4.2.6. The processing is necessary for substantial public interest reasons, on the basis of laws that will be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject.

4.2.7. The processing is necessary for archiving purposes in the public interest, legal, scientific, historical, or other important research purposes, or statistical purposes as guided by the principles of data collection in the Constitution of Cameroon and Africa Union Data Protection Framework.

5. Specified, Explicit, and Legitimate Purposes

5.1. The Organisation collects and processes the personal data. This includes:

5.1.1. Personal data collected directly from data subjects and;

5.1.2. Personal data obtained from third parties. The Organisation only collects, processes, and holds personal data for the specific purposes set out in Part 21 of the Data Protection and Privacy Act.

5.2. Data subjects are always kept informed as prescribed by the law of the purpose or purposes for which the Organisation uses their personal data. Please refer to Part 12 for more information on keeping data subjects informed.

6. Adequate, Relevant, and Limited Data Processing

The Organisation will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed)

7. Accuracy of Data and Keeping Data Up-to-Date

7.1. The Organisation will ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date at the time it comes into the possession of the Organisation as a data collector.

7.2. The accuracy of personal data will be checked (to the extent that it is reasonably possible to do so) when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

8. Data Retention

8.1. Protection of Personal Information Act states that electronic communication networks and information systems content providers shall be bound to conserve such content and stored data in their installations for a period of the 10 (ten) years.

8.2. The Organisation will not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed (the data subjects' data will be deleted once the data subject deletes his or her account with the Organisation);

8.3. When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay;

9. Secure Processing

BP : 14 841 Yaoundé, Cameroon
Tel : +237 675 358 795 / +33 669 714 981
Headquater : Yaoundé-Omnisport (Avenue Marc Vivien FOE)
MB Tech & Services
Tax Number N° RC/YAE/2023/A/3644
NIU : P 069 315 998 003 B
Email : info@panafrican.space

9.1. The Organisation will take all reasonable steps to ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

9.2. The Organisation shall be under the authority of The National Agency for Information and Communication Technologies, which will ensure the regularity and efficiency of security audits of information systems in accordance with established standards, public bodies, and Certification Authorities as stated in Section 7, subsection 2 of the Protection of Personal Information Act.

10. Accountability and Record-Keeping

10.1. The Organisation will have a Data Protection Officer.

10.2. The Data Protection Officer will oversee the implementation of this Policy and monitor compliance with it, the Organisation's other data protection-related policies, the Protection of Personal Information Act, and other applicable data protection legislation.

10.3. The Organisation will keep written internal records of all personal data collection, holding, and processing, which will incorporate the following information:

- 10.3.1. The name and details of the Organisation, its Data Protection Officer, and any applicable third-party data processors;
- 10.3.2. The purposes for which the Organisation collects, holds, and processes personal data;
- 10.3.3. Details of the categories of personal data collected, held, and processed by the Organisation and the categories of data subject to which that personal data relates;
- 10.3.4. Details of any transfers of personal data internationally, including all mechanisms and security safeguards;
- 10.3.5. Details of how long the Organisation will retain personal data; and
- 10.3.6. Detailed descriptions of all technical and organisational measures taken by the Organisation to ensure the security of personal data.

11. Data Protection Impact Assessments

11.1. The Organisation will establish and maintain appropriate safeguards against internal and external risks to personal data under its control. The organisation will further regularly verify that the safeguards are efficiently implemented and continuously up to date in respect to new risks or developments. This will apply to any and all new projects and/or new uses of personal data that involve the use of the platform, and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects.

11.2. Data Protection Impact Assessments will be overseen by the Data Protection Officer and will address the following:

- 11.2.1. The type(s) of personal data that will be collected, held, and processed;
- 11.2.2. The purpose(s) for which personal data is to be used;
- 11.2.3. The Organisation's objectives;
- 11.2.4. How personal data is to be used;
- 11.2.5. The parties (internal and/or external) who are to be consulted;
- 11.2.6. The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
- 11.2.7. Risks posed to data subjects;
- 11.2.8. Risks posed both within and to the Organisation; and

BP : 14 841 Yaoundé, Cameroon
Tel : +237 675 358 795 / +33 669 714 981
Headquater : Yaoundé-Omnisport (Avenue Marc Vivien FOE)
MB Tech & Services
Tax Number N° RC/YAE/2023/A/3644
NIU : P 069 315 998 003 B
Email : info@panafrican.space

11.2.9. Proposed measures to minimise and handle identified risks.

12. Data Subject Access

12.1. Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data that the Organisation holds about them, what it is doing with that personal data, and why.

12.2. Employees wishing to make a SAR should do so using a Subject Access Request Form, sending the form to the Organisation's Data Protection Officer.

12.3. Responses to SARs will normally be made within one month of receipt. However, this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject will be informed.

12.4. All SARs received will be handled by the Organisation's Data Protection Officer.

12.5. The Organisation does not charge a fee for handling normal SARs. The Organisation reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive or where they require the input of significant resources from the Organisation, in order to be fulfilled.

13. Rectification of Personal Data

13.1. Data subjects have the right to require the Organisation to rectify any of their personal data that needs to be updated or completed.

13.2. The Organisation will rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Organisation of the issue.

13.3. In the event that any affected personal data has been disclosed to third parties, those parties will be informed of any rectification that must be made to that personal data.

14. Erasure of Personal Data

14.1. Data subjects have the right to request that the Organisation erase the personal data it holds about them in the following circumstances:

14.1.1. It is no longer necessary for the Organisation to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;

14.1.2. The data subject wishes to withdraw their consent to the Organisation holding and processing their personal data;

14.1.3. The data subject objects to the Organisation holding and processing their personal data (and there is no overriding legitimate interest to allow the Organisation to continue doing so) ;

14.1.4. The personal data needs to be erased in order for the Organisation to comply with a particular legal obligation OR

14.1.5. Personal data is being held and processed to provide information society services to a child.

14.1.6. Unless the Organisation has reasonable grounds to refuse to erase personal data, all requests for erasure will be complied with, and the data subject will be informed of the erasure within one month of receipt of the request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject will be informed.

BP : 14 841 Yaoundé, Cameroon
Tel : +237 675 358 795 / +33 669 714 981
Headquater : Yaoundé-Omnisport (Avenue Marc Vivien FOE)
MB Tech & Services
Tax Number N° RC/YAE/2023/A/3644
NIU : P 069 315 998 003 B
Email : info@panafrican.space

14.1.7. If any personal data to be erased in response to a data subject's request has been disclosed to third parties, those parties will be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

15. Data Portability

15.1. The Organisation processes personal data using automated means; that is, automation towards increasing efficiency in delivering access to justice and the law.

15.2. The Organisation stores its data in the cloud via platforms that may be disclosed at the request of the data subject.

15.3. Where data subjects have given their consent to the Organisation to process their personal data in such a manner, or the processing is otherwise required for the performance of a contract between the Organisation and the data subject, data subjects have the right to receive a copy of their personal data and to use it for other purposes.

15.4. To facilitate the right of data portability, the Organisation will make available all applicable personal data to data subjects in the following formats:

15.5. All requests for copies of personal data will be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject will be informed.

16. Objections to Personal Data Processing

16.1. Data subjects have the right to object to PSI processing their personal data based on legitimate interests, direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.

16.2. Where a data subject objects to the Organisation processing their personal data based on its legitimate interests, the Organisation will cease such processing immediately unless it can be demonstrated that the Organisation's legitimate grounds for such processing override the data subject's interests and rights.

16.3. Where a data subject objects to the Organisation processing their personal data for direct marketing purposes, the Organisation will cease such processing immediately.

16.4. Where a data subject refuses/objects to the Organisation processing their personal data for legal, scientific, and/or historical research and statistics purposes, the data subject may object to the collection and clearly indicate reasons for refusal. The Organisation is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

17. Automated Decision-Making

PSI may use personal data in automated decision-making processes.

17.1. Where such decisions have a legal (or similarly significant effect) on data subjects, those data subjects have the right to challenge such decisions under the Protection of Personal Information Act, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the Organisation.

17.2. The right described in Part 19.1 does not apply in the following circumstances:

17.2.1. The decision is necessary for the entry into, or performance of, a contract between the Organisation and the data subject;

17.2.2. The decision is authorised by law; or

17.2.3. The data subject has given their explicit consent.

BP : 14 841 Yaoundé, Cameroon
Tel : +237 675 358 795 / +33 669 714 981
Headquater : Yaoundé-Omnisport (Avenue Marc Vivien FOE)
MB Tech & Services
Tax Number N° RC/YAE/2023/A/3644
NIU : P 069 315 998 003 B
Email : info@panafrican.space

18. Profiling

18.1. The Organisation uses personal data for profiling purposes. This includes capturing one's name, address, phone number, email and social media profile where available. This data also contains personal information on one's legal case enquiry.

18.2. When personal data is used for profiling purposes, the following will apply:

18.2.1. Clear information explaining the profiling will be provided to data subjects, including the significance and likely consequences of the profiling;

18.2.2. Appropriate mathematical or statistical procedures will be used;

18.2.3. Technical and organisational measures will be implemented to minimise the risk of errors. If errors occur, such measures must enable them to be easily corrected; and

18.2.4. All personal data processed for profiling purposes will be secured in order to prevent discriminatory effects arising out of profiling

19. Data Security - Use of Personal Data

PSI will ensure that the following measures are taken with respect to the use of personal data:

19.1. No personal data may be shared informally, and if an employee, agent, sub-contractor, or other party working on behalf of the Organisation requires access to any personal data that they do not already have access to, such access should be formally requested from the Data Protection Officer;

19.2. No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Organisation or not, without the authorisation of the Data Protection Officer;

19.3. Personal data must be handled with care at all times and should be supervised and visible to unauthorised employees, agents, subcontractors, or other parties at any time; 19.4. Where personal data held by the Organisation is used for marketing purposes, it will be the responsibility of the Data Protection Officer to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service.

20. Data Security - IT Security

20.1. PSI will ensure that the following measures are taken with respect to IT and information security:

20.1.1. All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols. All software used by the Organisation is designed to require such passwords;

20.1.2. Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Organisation, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff will not have access to passwords;

20.1.3. All software (including, but not limited to, applications and operating systems) will be kept up-to-date. PSI's IT staff will be responsible for installing any and all security-related updates as soon as reasonably and practically possible after the updates are made available by the publisher or manufacturer, unless there are valid technical reasons not to do so; and

BP : 14 841 Yaoundé, Cameroon
Tel : +237 675 358 795 / +33 669 714 981
Headquater : Yaoundé-Omnisport (Avenue Marc Vivien FOE)
MB Tech & Services
Tax Number N° RC/YAE/2023/A/3644
NIU : P 069 315 998 003 B
Email : info@panafrican.space

21. The Pan-African Space Industry Measures

21.1. PSI will ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

21.1.1. All employees, agents, contractors, or other parties working on behalf of PSI will be made fully aware of both their individual responsibilities and the Organisation's responsibilities under this Policy and will be provided with a copy.

21.1.2. Only employees, freelancers, users, or stakeholder partners working on behalf of the Organisation that need access to, and use of, personal data in order to carry out their assigned duties correctly will have access to personal data held by PSI;

21.1.3. All employees, freelancers, users, or stakeholder partners working on behalf of the Organisation handling personal data will be appropriately trained to do so and will be appropriately supervised;

21.1.4. Methods of collecting, holding, and processing personal data will be regularly evaluated and reviewed;

21.1.5. All employees, freelancers, users, or stakeholder partners agents, working on behalf of the Organisation handling personal data will be bound to do so in accordance with the principles of this Policy by contract;

21.1.6. Where any employee, freelancer, user, or stakeholder partner handling personal data on behalf of the Organisation fails in their obligations under this Policy, that party will indemnify and hold harmless the Organisation against any costs, liability, damages, loss, claims, or proceedings that may arise out of that failure.

22. Data Breach Notification

22.1. All personal data breaches must be reported immediately to PSI Data Protection Officer.

22.2. If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g., financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the supervising Authorities Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

22.3. In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.

22.4. Data breach notifications will include the following information:

22.4.1. The categories and approximate number of data subjects concerned;

22.4.2. The categories and approximate number of personal data records concerned;

22.4.3. The name and contact details of the Organisation's data protection officer (or other contact point where more information can be obtained);

22.4.4. The likely consequences of the breach;

22.4.5. Details of the measures taken, or proposed to be taken, by the Organisation to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

The Data Protection Officer will be responsible for overseeing the implementation of this Data Protection, Privacy, and Confidentiality Policy and monitoring compliance with this Policy, PSI's other data protection-related policies, the Protection of Personal Information Act, and other applicable data protection legislation.

BP : 14 841 Yaoundé, Cameroon
Tel : +237 675 358 795 / +33 669 714 981
Headquater : Yaoundé-Omnisport (Avenue Marc Vivien FOE)
MB Tech & Services
Tax Number N° RC/YAE/2023/A/3644
NIU : P 069 315 998 003 B
Email : info@panafrican.space