PLANETARY RESOURCES®

THE ASTEROID MINING COMPANY

Planetary Resources, Inc. Human Resources Data Privacy Policy

May 12, 2017

6742 185th Ave NE
Redmond, WA 98052-1111
425-336-2448
425-336-2439
planetaryreosurces.com

Table of Contents

INTRODUCTION: 3

PREAMBLE: 4

SCOPE: 4

NOTICE: 5

CHOICE: 5

DISCLOSURE: 6

SECURITY: 7

DATA INTEGRITY, ACCURACY, AND COMPLETENESS: 7

ACCESS AND CORRECTION: 7

COMPLAINT RESOLUTION: 8

COMPLIANCE: 8

TRANSPARENCY: 8

SUPPLEMENTAL PRINCIPLES: 9

INTRODUCTION:

Planetary Resources, Inc., Planetary Resources Development Corp., and Planetary Resources Luxembourg, S.á r.l. (collectively "the Company") complies with the EU-U.S. Privacy Shield and the Swiss-U.S. Privacy Shield Frameworks as set forth by the U.S. Department of Commerce ("the Department") regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland, to the United States.

The Company has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit: https://www.privacyshield.gov/.

To provide an adequate level of protection for Personal Data received from the European Union and Switzerland, the Company adheres to the EU-U.S. Privacy Shield and the Swiss-U.S. Privacy Shield Frameworks, which includes 16 Supplemental Principles, developed by the United States Department of Commerce, and the European Commission, as well as the accompanying letters from the International Trade Administration, the U.S. Federal Trade Commission (FTC) and the U.S. Department of Transportation (DOT). The Company is subject to the investigatory and enforcement powers of the FTC. This Privacy Policy (the "Policy") sets forth the privacy principles that the Company follows when processing Personal Data received from the EU and Switzerland.

The privacy principles in this Policy are based on the seven Privacy Shield Principles and the 16 Supplemental Principles of the EU-U.S. Privacy Shield. The full text of the agreement can be found here: https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/eu_us_privacy_shield_full_text.pdf.pdf

PREAMBLE:

The Company recognizes and supports the need for reasonable protections regarding the privacy of personal "human resources" data collected by the Company through the employment relationship. For this reason, the Company has developed and adopted these general guiding Principles. Individual locations should consider adopting regional implementation policies to put these Principles into practice.

All Company employees should help to ensure that the personal information the Company holds about them is accurate and up to date. In addition, all Company employees whose responsibilities include the collection, processing or storage of personal data are expected to assist in the protection of that data by adherence to these Principles.

In following these Principles, the Company complies with the applicable laws and regulations protecting the privacy of personal data in the employment relationship in the jurisdictions in which the Company operates.

SCOPE:

These Principles apply to all personal data about employees and applicants residing in the EU or Switzerland that is collected, maintained or used by the Company as part of an actual or prospective employment relationship.

Nothing in these Principles is intended to form a contract of employment or otherwise. The Company may amend these Principles from time to time, should it become necessary to do so.

Personal data collected, maintained or used outside of the employment relationship, such as personal data arising from consumer marketing, is not covered by these Principles.

COLLECTION AND USE:

The Company collects and uses personal data in a reasonable and lawful manner. The Company collects and uses personal data for relevant and appropriate purposes.

The Company receives Personal Data from the U.S., EU, and Switzerland pertaining to job applicants, employees, potential customers and customers (collectively "data subjects") to assist its foreign subsidiaries and affiliates in administering the recruitment process, their employment relationship with employees located in the Member States, and their obligations, if any, to former employees, and to facilitate customer relationship management. The Personal Data is stored in the Company's human resources management system database.

NOTICE:

The Company informs individuals about whom the Company collects personal data of (1) the type of data the Company collects, (2) the purposes for which the Company collects and discloses personal data, (3) the circumstances under which the Company discloses personal data, including the types of potential recipients (4) that the Company employs privacy and information safeguards; and (5) the circumstances under which individuals may access and correct their personal data.

The Personal Data that the Company receives from the EU and Switzerland consists largely of information provided by job applicants and employees such as resumes and complete job applications, personal contact information and date of birth. The Company also may receive personal information about an applicant or employee which is created by one of its corporate affiliates, such as interview notes, business contact information, job title, job category, job status, compensation and benefits information, and performance reviews. Personal Data received pertaining to potential customers and customers as provided by these data subjects is generally limited to information on a business card such as name, business title and business postal address, email address and telephone number.

Before processing Personal Data of any employee who resides in an EU Member State or Switzerland, the Company provides the employee with a notice concerning the processing of their Personal Data. The Company will not use or disclose Personal Data transferred from an EU Member State or Switzerland to the United States for any purpose that has not previously been disclosed to the employee unless: (a) the employee has received notice and an opportunity to exercise choice, as described below, with respect to such use or disclosure; or (b) applicable law permits the use or disclosure without requiring that the Company first comply with the Notice and Choice Principles.

CHOICE:

The Company collects personal data for employment-related business purposes. Where consent of the employee or a representative of employees for the collection, use, or disclosure of personal data is required by law or contract, the Company will comply with the law or contract.

In the event that an individual expresses a concern about the collection, use or disclosure of personal data, the Company will respond to the employee's concern consistent with applicable law.

The Company will offer employees or customers in the EU and Switzerland whose Personal Data has been transferred to the United States the opportunity to opt out from: (a) the disclosure of Personal Data to a non-agent Third Party; and (b) the use or disclosure of their Personal Data for a purpose other than the purposes for which the information originally was collected or subsequently authorized by the individual or a compatible purpose. If the Company were to receive "sensitive personal information" (which includes, for example, personal information specifying medical or health conditions, racial or ethnic origin, or trade union membership), the Company will request and obtain affirmative consent before disclosing such information to a non-agent Third Party and before using such information for a purpose other than the purpose originally disclosed or a compatible purpose. The Company will provide employees or customers with reasonable mechanisms to exercise their choices should such circumstances arise.

DISCLOSURE:

The Company places substantial importance on protecting the confidentiality of personal data and seeks the cooperation of all employees in furthering this goal.

Internal Disclosure: To the extent feasible, the Company restricts access to personal data to those employees, agents, or contractors of the Company, its corporate parent, affiliates divisions, or subsidiaries who have a legitimate need for such access.

Onward Transfer: The Company is liable for onward transfers to third parties and will comply with the Notice and Choice Principles before transferring Personal Data to a Third Party who is not an agent of the Company. Before transferring Personal Data to a third-party agent, the Company will obtain assurances from the agent that it will safeguard the data subjects' Personal Data in a manner consistent with this Policy. Where the Company learns that an agent is using or disclosing Personal Data in a manner contrary to this Policy, the Company will take reasonable steps to prevent such use or disclosure. Disclosures to Third Parties, whether an agent of the Company or not, will be only for the purposes described in this Policy under the section entitled, "Notice," for a compatible purpose, or for a purpose subsequently authorized by the data subject. The Company may disclose human resource-related information, as described above in section entitled, "Notice," to third parties who assist the Company in administering employee benefits programs, payroll programs, pension and other retirement programs, and information technology programs and security.

Disclosure of personal data beyond the employees, agents, or contractors of the Company, its corporate parent, affiliates, divisions or subsidiaries may be made pursuant to a labor agreement, for a sound business reason, as required by law or legal process, for another lawful purpose, *e.g.*, cooperation with local law enforcement authorities; to protect the interests of the Company's employees, or, in the absence of any of the above, only with the authorization of the individual involved.

The Company requires agents and contractors to whom the Company discloses personal data for servicing to commit to protecting the privacy and security of the data and to refrain from any uses or further disclosures or not authorized by the Company.

The Company will not disclose personal data to unaffiliated third parties for consumer marketing purposes without the employee's written consent.

Aggregation: Where appropriate under the circumstances, the Company will anonymize or aggregate data to eliminate individual identifiers.

SECURITY:

The Company strives to protect the Personal Data that it receives from the EU and Switzerland. While the Company cannot guarantee the security of the Personal Data that it receives, the Company takes reasonable precautions to protect the Personal Data in the Company's possession from loss, misappropriation, unauthorized access, disclosure and destruction.

The Company utilizes a combination of online and offline security technologies, procedures and organizational measures to help safeguard Personal Data. For example, facility security is designed to prevent unauthorized access to company computers. Electronic security measures — including, for example, network access controls, passwords, and secure remote access — provide protection from hacking and other unauthorized access. The Company also protects information through the use of firewalls, role-based restrictions, and, where appropriate, encryption technology.

The Company limits access to Personal Data to the Company's employees and agents that have a specific business reason for accessing such Personal Data. Individuals who have been granted access to Personal Data will be made aware of their responsibilities to protect such information and are provided training and instruction on how to do so.

DATA INTEGRITY, ACCURACY, AND COMPLETENESS:

The Company employs reasonable means to keep personal data accurate, complete and up-to-date, and all employees have a responsibility to assist the Company in keeping the information the Company maintains about them accurate, complete and current.

The Company collects only Personal Data that is necessary for the purposes listed in this Policy under the section entitled, "Notice." The Company will process the Personal Data only in ways that are for, or compatible with, the purposes for which the data was collected or that are subsequently authorized by the data subject. The Company takes reasonable steps to ensure that the information it collects is accurate, complete, current, and reliable for its intended use. The Company will retain Personal Data only for as long as is necessary to accomplish its legitimate business purposes or for as long as may be permitted or required by applicable law.

ACCESS AND CORRECTION:

Upon reasonable request, the Company will grant data subjects reasonable access to their Personal Data and will permit them to correct, amend or delete Personal Data that is inaccurate or incomplete. Data subjects who wish to review or update their Personal Data can do so by contacting the Company's Human Resources Office. The Company may, in its discretion, charge a reasonable, cost-based fee for access or photocopying. For security purposes, the Company may require verification of identity before providing access to Personal Data.

COMPLAINT RESOLUTION:

The Company will conduct periodic self-assessments of its relevant practices to verify adherence to this Policy and the Privacy Shield Principles. Any employee who intentionally violates this Policy will be subject to disciplinary action up to and including termination of employment.

Any data subject who has a complaint concerning the Company's processing of his or her Personal Data should contact the Company's Human Resources Office. The Company will investigate and attempt to resolve such complaints in accordance with the principles contained in this Policy. Any data subject who is not satisfied with the internal resolution of the complaint may seek redress with the national data protection or labor authority in the country where the data subject resides.

RETENTION:

Personal data is kept in active files or systems only as long as needed to meet the purposes for which it was collected or as required by contractual agreement, by law or regulation, or, where applicable, for the appropriate statute of limitations period.

COMPLIANCE:

The Company maintains an active program to ensure compliance with these Principles, as well as with applicable law or contractual agreements on handling of personal data.

A senior official of the Company is responsible for implementing and overseeing the administration of these Principles.

All Company employees whose responsibilities include the collection, processing or storage of personal data are required to adhere to these Principles and implementing policy. Failure to do so may be grounds for discipline up to and including termination.

TRANSPARENCY:

The Company informs employees and others about our privacy principles, policies and procedures.

SUPPLEMENTAL PRINCIPLES:

1. Sensitive Data
The Company is not required to obtain affirmative express consent with respect to sensitive data where the processing is:

a. In the vital interests of the data subject or another person;
b. Necessary for the establishment of legal claims or defenses;
c. Required to provide medical care or diagnosis;
d. Carried out in the course of legitimate activities by a foundation, association, or any other non-profit body with a political, philosophical, religious, or trade-union aim and on condition that the processing relates solely to the members of the body or to the persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects;
e. Necessary to carry out the organization's obligations in the field of employment law; or
f. Related to data that are manifestly made public by the individual.

2. Journalistic Exceptions
First Amendment must govern in the event that privacy and constitutional principles conflict. The Company will carefully review any situation in which such a conflict may arise.

3. Secondary Liability
Internet Service Providers, telecommunications carriers, and other organizations are not liable under the Privacy Shield Principles when on behalf of another organization they merely transmit, route, switch, or cache information.

4. Performing Due Diligence and Conducting Audits
At times, the Company hires auditors and investment bankers which may require personal data to perform certain tasks. Consent or knowledge of the individual is not required in certain circumstances where such auditors or investment bankers perform these duties pursuant to statutory or regulatory requirements, or in performing due diligence relating to a potential merger or acquisition of another organization. Premature disclosure of such activities could impede such negotiations and agreements, and as a result, investment bankers and attorneys engaged in due diligence, or auditors conducting an audit, may process information without the knowledge of the individual only to the extent and for the period necessary to meet statutory or public interest requirements and in other circumstances in which the application of these Principles would prejudice the legitimate interests of the organization.

5. The Role of the Data Protection Authorities (DPAs)
The Company commits to employ effective mechanisms for assuring compliance with the Privacy Shield Principles. The Company provides the following as it relates to the recourse, enforcement and liability principle:

a. Recourse for individuals to whom the data relates,
b. Follow-up procedures for verifying that the attestations and assertions the individuals have made about their privacy practices are true, and
c. Obligations to remedy problems arising out of failure to comply with the Principles.

The Company will complete the following:

a. Elects to satisfy the Notice and Choice Principles above;

b. Cooperate with the DPAs in the investigation and resolution of complaints brought under the Privacy Shield; and

c. Comply with any advice given by the DPAs (in regards to customer data and in regards to human resource date transferred from the EU or Switzerland in the context of the employment relationship) where the DPAs take the view that the organization needs to take specific action to comply with the Privacy Shield Principles, including remedial or compensatory measures for the benefit of individuals affected by any non-compliance with the Principles, and will provide the DPAs with written confirmation that such action has been taken.

6. Self-Certification

The Company will comply with all of the Department's self-certification submission requirements. The Company will ensure compliance with the Privacy Principles and will work its existing commercial relationships with third parties to ensure conformity as soon as possible and within nine months from the date upon which The Company certified to the Privacy Shield.

7. Verification

The Company will complete a self- assessment approach of its privacy practices to verify compliance with the attestations and assertions made under the Privacy Shield privacy practices.

8. Access

The Company will adhere to the Access Principle in Practice, which allows individuals to verify the accuracy of information held about them. The Company will also make good faith efforts to provide access. It may deny or limit access to the extent that granting full access would reveal its own confidential commercial information.

9. Human Resources Data

When the Company will transfer personal information about its EU or Swiss employees collected in the context of the employment relationship to a parent, affiliate, or unaffiliated service provided in the United States participating in the Privacy Shield, the transfer enjoys the benefits of the Privacy Shield. The collection of the information and its processing prior to transfer will have been subject to the national laws of the EU Member State or Switzerland where it was collected, and any conditions for or restrictions on its transfer according to those laws will be respected. The Company will adhere to the Notice and Choice Principles as well as the Access Principle regarding human resources data.

10. Obligatory Contracts for Onward Transfers

The Company complies with requirements relating to onward transfers of protected data through the use of model or other contractual clauses that comply with European Union and Switzerland data transfer standards and requirements. These principles apply to transfers of data within controlled groups of corporations or entities as well as with third party controllers and processors.

11. Dispute Resolution and Enforcement

The Company will satisfy the requirement of this Principle through the following:

a. Compliance with private sector developed privacy programs that incorporate the Privacy Shield Principles;

b. Compliance with legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution; or

c. Commitment to cooperate with data protection authorities located in the EU and Switzerland, as applicable, or their authorized representatives.

In compliance with the Privacy Shield Principles, the Company commits to resolve complaints about the collection or use of your personal information. Individuals from the European Union and Switzerland with inquiries or complaints regarding our Privacy Shield Policy should first contact the Company by letter, or email as follows:

Planetary Resources Human Resources Office
ATTN: Privacy Shield
6742 185th Avenue, NE
Redmond, Washington 98052, USA
Email: privacyshield@planetaryresources.com

The Company further commits to arbitrate unresolved Privacy Shield complaints in accordance with Privacy Shield Annex I. Privacy Shield Annex I sets forth paremeters for arbitration of unresolved Privacy Shield Complaints, available remedies, and procedural requirements that must be satisfied prior to arbitration. In particular, an individual who decides to invoke this arbitration option must take the following steps prior to initiating an arbitration claim:

a. raise the claimed violation directly with the Company and afford the Company an opportunity to resolve the issue within 45-days, per the timeframe set forth in Section III.11(d)(i) of the Principles;

b. make use of the independent recourse mechanism, which is at no cost to the individual; and

c. raise the issue through their Data Protection Authority to the Department of Commerce and afford the Department of Commerce an opportunity to use best efforts to resolve the issue within the timeframes set forth in the Letter from the International Trade Administration of the Department of Commerce, at no cost to the individual. This arbitration option may not be invoked if the individual's same claimed violation of the Principles:

(1) has previously been subject to binding arbitration;

(2) was the subject of a final judgment entered in a court action to which the individual was a party; or

(3) was previously settled by the parties.

In addition, this option may not be invoked if an EU Data Protection Authority:

a. has authority under Sections III.5 or III.9 of the Principles; or

b. has the authority to resolve the claimed violation directly with the Company.

A DPA's authority to resolve the same claim against an EU or a Swiss data controller does not alone preclude invocation of this arbitration option against a different legal entity not bound by the DPA authority.

12. Choice-Timing of Opt Out

The Company data that is subject to the Privacy Shield framework is primarily human resource data. Consumer data in the Company's possession, if any, is primarily related to business contacts as the Company and its affiliates do not generally sell to end consumers. As a result, opt out policies are generally not applicable to Company activities and data. To the extent that any opt out policies or requirements are or may become applicable, the Company agrees to comply with such requirements.

13. Travel Information

The Company understands there are certain circumstances where travel information such as frequent flyer or hotel reservation information and special handling needs may be transferred to organizations located outside the EU and Switzerland in several different circumstances.

14. Pharmaceutical and Medical Products

The Company does not possess data relating to pharmaceutical or medical products and data relating to this industry.

15. Public Record and Publicly Available Information
Information available through public records, or is otherwise generally publicly available, is not subject to the Notice, Choice, and Accountability for Onward Transfer Principles in some circumstances, provided that such information is not combined with non-public information. In addition, the Access Principle is not applicable to such information except where such information is combined with non-public information.

16. Access Requests by Public Authorities
The Company may be required to disclose your personal information in response to lawful requests from public authorities, including to meet national security or law enforcement requirements. Where permitted by law, the Company has the option to issue reports relating to data privacy inquiries.

ADDITIONAL INFORMATION
Additional Questions
In compliance with the Privacy Shield Principles, the Company commits to resolve complaints about the collection or use of your personal information. Individuals from the European Union and Switzerland with inquiries or complaints regarding our Privacy Shield Policy, should first contact the Company by letter, or email as follows:

Planetary Resources Human Resources Office
ATTN: Privacy Shield
6742 185th Avenue, NE
Redmond, Washington 98052, USA
Email: privacyshield@planetaryresources.com

Please include your name, address and e-mail address in all communications and state clearly the nature of your request.

Changes to this Privacy Policy
The Company may revise this Policy at any time. If we decide to materially change this Policy, we will post the revised policy at this location. If, at any point, we decide to make any material changes in the way we process your Personal Data, we will make that information available by posting a notice on this site, and we will provide data subjects with choice as to whether or not we process their information in this different manner if it is incompatible with the purposes described in the section entitled, “Notice,” above.

Effective Date: May 12, 2017.