

We self-certify compliance with the EU-U.S. Privacy Shield.

## Privacy Shield Privacy Policy Statement

Freeport-McMoRan Inc. and its affiliates (hereinafter the “Company” or “FCX”) are committed to preserving personal privacy. As part of that commitment, the Company adheres to the EU-U.S. Privacy Shield Principles administered by the United States Department of Commerce in consultation with the European Commission (the “Privacy Shield Principles”) with respect to personal information within the scope of this statement. This Privacy Shield Privacy Policy (the “Policy”) sets forth the privacy principles that the Company follows with respect to personal information transferred from the European Union (EU) to the United States in reliance on the Privacy Shield.

### **Definitions**

“Agent” means any third party that processes personal information pursuant to the instructions of, and solely for the benefit of, the Company, or to which the Company discloses personal information for processing on the Company’s behalf.

“Data subject” means, as to personal information, the natural person as to whom such personal information relates. Under this Policy, a data subject may be an employee of the Company or may be an employee, customer or other associate of the Company’s client (provided that such customer or associate is a natural person), or may be any other natural person about which personal information is received by the Company (or its subsidiaries) in the United States from the European Union.

“Personal information” means any information relating to an identified or identifiable natural person that is within the scope of the EU Personal Data Directive, received by the Company from the European Union, and recorded in any form. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Personal information does not include information rendered anonymous or aggregate information (to the extent an individual’s identity cannot reasonably be derived from such information).

“Processing” of personal information means any operation or set of operations which is performed upon personal information, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure or dissemination, and erasure or destruction.

“Sensitive personal information” means personal information specifying medical or health conditions, race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual.

### **Privacy Shield Principles**

The following principles are based on the Privacy Shield Principles. Additional information about the Privacy Shield program is available at the U.S. Department of Commerce’s website at <https://www.privacyshield.gov>.

## **Notice**

FCX uses certain Internet-based human resource information management tools to conduct employment related activities to include recruitment and ongoing employee data maintenance, in addition to other methods of receiving information from individuals. The use of these HR systems requires individuals to provide personal information about themselves. FCX may also capture personal information about customers or suppliers in the course of conducting business with them, through its information systems and other avenues of communication, for the purposes of processing business transactions. The types of personal information collected by FCX includes email addresses, mailing addresses, phone numbers, tax IDs, gender, dates of birth, and employee information such as position, title, training records, and health information. Individuals, customers, and suppliers will be told the purpose for which the information is collected and used when asked to provide the information or soon thereafter. FCX may transfer personal information to third parties in the United States acting as agents for the Company to perform tasks on the Company's behalf and under its instructions in association with certain employment related activities including pre-employment background review and illegal substance screening.

## **Choice**

FCX gives you choices about the ways it uses and shares your personal information, and it respects the choices you make. Your personal information will not be used for a purpose that is materially different from the purpose for which it was originally collected or subsequently authorized by you. Any sensitive personal information you provide to FCX in accordance with applicable law in each country will be treated in the utmost confidence and used only for the purposes for which it was provided, unless you give your express consent.

EU data subjects may choose to opt out of the transfer, processing, or disclosure of their personal information by the Company by contacting the Chief Information Security Officer at the address provided below. For further information on your right of choice about the ways FCX uses and shares personal information, please contact the Office of the Chief Information Security Officer at the address provided below.

## **Onward Transfer**

The Company may transfer personal information to third parties in the United States acting as agents for the Company to perform tasks on the Company's behalf and under its instructions. The types of third parties to which the Company discloses personal information include consulting companies for the purposes of assisting the Company with data collection and processing tasks. The Company will transfer data to third party agents only for limited and specified purposes, ascertain that its agents are obligated to provide at least the same level of privacy protection as is required by the Privacy Shield Principles, and take reasonable and appropriate steps to ensure that its agents process personal information transferred in a manner that is consistent with the Company's obligations under the Privacy Shield Principles. The Company will require third party agents to notify the Company if the agent makes a determination that it can no longer meet its obligations to provide the same level of protection required by the Privacy Shield Principles. Where the Company becomes aware that an agent is

processing personal information in a manner contrary to this Policy, the Company will take reasonable steps to stop and remediate the unauthorized processing. If the Company shares information with certain third parties, the Company may be liable if those parties process that information in a manner that is inconsistent with the Privacy Shield Principles.

This provision does not apply to public record information or publicly available information except in certain situations as defined by the Privacy Shield Principles.

### **Access**

You have a right to access your personal information. Upon an individual's request, the Company will offer an individual reasonable access to his or her personal information and will afford such individual a reasonable opportunity to correct, amend, or delete inaccurate information, or information that has been processed in violation of the Privacy Shield Principles. If a Company employee would like to access personal information maintained by the Company, the employee should make a written request to his or her local human resources representative. If a non-Company data subject would like to access personal information maintained by the Company, the individual should contact the Company using the contact information set forth in the "Contact Information" section below. EU data subjects may also request confirmation of whether or not FCX has personal data relating to them by contacting the Chief Information Security Officer at the address provided below. For security purposes, the individual may need to provide the Company with various pieces of personal information to process the request. The Company may limit or deny access to personal information, or charge a reasonable fee, where providing such access would be unreasonably burdensome or expensive under the circumstances, would violate the rights of another person, or as otherwise permitted by the Privacy Shield Principles.

### **Security**

The Company will take reasonable and appropriate measures including technical, physical, and administrative measures and training to protect personal information from loss, misuse, and unauthorized disclosure, access, alteration, and destruction. The Company safeguards information according to established security standards and periodically assesses new technology for methods of protecting information.

### **Data Integrity**

The Company will take reasonable measures to ensure that personal information is relevant for its intended use, reliable for its intended use, accurate, complete, and current. The Company will only retain personal information for as long as it serves the purposes of processing that information, except as otherwise provided by the Privacy Shield Principles.

Any personal information provided to FCX in relation to a specific job application will be retained until the recruitment process for that role is complete, provided that in the case of successful applicants, their data will be retained by FCX for purposes of the person's continuing employment. For applicants who have indicated that they wish to be considered for future opportunities, personal information will be retained on file until the applicants indicate that they no longer wish to be considered.

Information gathered by FCX for the purposes of business transactions will be retained within the systems no longer than necessary, and in accordance with the FCX Records and Information Management guidelines and any other applicable retention periods, which may vary according to each country's laws.

### **Enforcement and Dispute Resolution**

Any questions, concerns, or complaints concerning the collection and use of personal information by the Company should be directed to the Chief Information Security Officer at the address given below.

The Company will conduct a reasonable investigation of and will attempt to resolve any complaints in accordance with the principles contained in this Policy.

The Company has designated the panel established by DPAs to address complaints and provide appropriate recourse free of charge to data subjects, including with respect to human resources personal information within the scope of this statement. The Company will cooperate with, and comply with any decisions by, the relevant European data protection authorities concerning unresolved complaints relating to personal information falling within the scope of this Policy. The Company is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission.

In certain circumstances, data subjects may be able to invoke binding arbitration with respect to adherence to the Privacy Shield.

### **Limitation On Application Of Principles**

Adherence by the Company to this Policy may be limited (a) to the extent required to respond to a legal or ethical obligations; and (b) to the extent permitted by an applicable law, rule or regulation. The Company may be required to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

### **Contact Information**

Questions or comments regarding this Policy should be submitted by mail as follows:

Freeport-McMoRan Inc.  
Attn: Chief Information Security Officer  
333 North Central Avenue  
Phoenix, AZ 85004

EU data subjects can also submit inquiries or complaints to the relevant European data protection authorities.

Last Modified: September 29, 2016