

## Alcoa, Inc.

### Safe Harbor Privacy Principles

Alcoa, Inc. (“Alcoa”) recognizes and respects the privacy rights of individuals with regards to Personal Information the company obtains about them. As part of its compliance with European privacy laws, Alcoa participates in the International Safe Harbor Program established by the United States, the European Union, and Switzerland (see [www.export.gov/safeharbor](http://www.export.gov/safeharbor)) for the purpose of regulating the transfer of Personal Information from Europe to the United States.

**BACKGROUND:** These privacy principles consolidate earlier principles issued under previous certifications by Alcoa and expand the scope.

**SCOPE:** These principles apply to all Personal Information received by Alcoa from Europe under its consolidated Safe Harbor certification.

### DEFINITIONS

**Personal Information:** Personal Information is any information about an identified or identifiable individual, regardless of the medium or format in which the information is stored.

**Sensitive Information:** Sensitive Information is Personal Information treated in European data protection laws as posing special risks to individuals, such as information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health, or sex life. Other categories of personal data subject to special protections in some European countries include information about criminal history, civil judgments, administrative sanctions, government security measures, government-issued ID numbers, biometric data, genetic data, geo-location data, personality profiling, and information in the context of “whistleblowing.”

**Data Controller:** A data controller is a party or entity that determines the purposes and means of the processing of Personal Information. A company functions as a data controller when it decides how such data is to be used, and then uses that data accordingly.

**Data Processor:** A data processor is a party or entity that processes Personal Information on behalf of a data controller. A company functions as a data processor when it acts as an agent of another company, following its instructions as to how that data should be handled and processed.

## ALCOA'S ROLES IN HANDING PERSONAL DATA

For some Personal Information covered by these principles, Alcoa acts as a data controller, making decisions about the purposes and means of processing of the information received from Europe, and then using the data for those purposes. For other Personal Information, Alcoa acts as a data processor, maintaining data in its North American Data Center in Pittsburgh, Pennsylvania solely on behalf of its European subsidiaries and affiliates.

### APPLICABLE PRINCIPLES

#### **A. Alcoa as a Data Controller**

With respect to Personal Information received from Europe where Alcoa operates as a data controller (i.e., makes decisions about the purposes and means of processing of the information), Alcoa handles such information in accordance with the seven Safe Harbor Privacy Principles (*Notice, Choice, Onward Transfer, Security, Data Integrity, Access, and Enforcement*). A full statement of these principles, summarized below, may be found on the Safe Harbor website of the U.S. Dept. of Commerce at [www.export.gov/safeharbor/eg\\_main\\_018247.asp](http://www.export.gov/safeharbor/eg_main_018247.asp).

##### **1. Notice**

Alcoa informs individuals about the purposes for which it collects and uses information about them, how to contact Alcoa with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means Alcoa offers individuals for limiting the use and disclosure of this information. This notice is provided in clear and conspicuous language when individuals are first asked to provide Personal Information to Alcoa or authorize Alcoa to collect the information from third parties (or as soon thereafter as practicable) and before Alcoa uses such information for a purpose other than that for which it was originally collected.

##### **2. Choice**

Alcoa collects and uses Personal Information required to operate its business. Such collection and use is subject to the Notice principle described above and in most circumstances does not require the explicit consent of the individual. However, Alcoa obtains the individual's consent before:

(a) disclosing Personal Information to a third party (other than disclosure to an agent or contractor processing the data solely on Alcoa's behalf, or disclosure required by law).

(b) using Personal Information for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual.

Where consent is required, Individuals are provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice. These mechanisms may normally be "opt-out" (Alcoa may proceed absent an objection from the individual within a reasonable

time), but if the data include Sensitive Information (as defined above), Alcoa will not proceed without the express (“opt-in”) consent of the individual.

### **3. Onward Transfer**

Alcoa discloses Personal Information externally only to third-party contractors or agents that process the data on Alcoa’s behalf; to satisfy government reporting requirements; to meet other legal obligations; to assert or defend legal claims or interests; or with the consent of the individual. Before making disclosure to a third party, Alcoa will first apply the Notice and Choice principles as described above. Unless the disclosure is legally required (such as tax reporting or responding to a judicial subpoena), Alcoa also ensures that the third party is obligated (by law, contract, or its own Safe Harbor certification) to provide at least the same level of privacy protection as is required by these principles. Where Alcoa contracts with third parties to process Personal Information on its behalf, Alcoa’s policy is to contractually obligate the third parties to maintain the confidentiality and security of Personal Information they receive; to act upon it only in accordance with the instructions they receive from Alcoa and/or the client; and to handle the information strictly in accordance with these principles.

### **4. Security**

Alcoa takes reasonable precautions, including administrative, technical, personnel, and physical measures, to safeguard Personal Information against loss, misuse, theft, and unauthorized access, disclosure, alteration, and destruction. Alcoa’s security policies, operating procedures, and technical controls, where applicable, generally adhere to commonly accepted standards for security of networks, infrastructure, applications, and data.

### **5. Data Integrity**

Alcoa limits its collection of Personal Information to that which is relevant for the intended business and legal purposes. Alcoa does not use the data in a way that is incompatible with the purposes for which it was collected or subsequently authorized by the individual. To the extent necessary for those purposes, Alcoa takes reasonable steps to ensure that Personal Information is reliable for its intended use, accurate, complete, and current.

### **6. Access**

Alcoa provides individuals an opportunity to access Personal Information about them and to correct, amend, or delete that information where it is inaccurate, out-of-date or irrelevant, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy, or where the rights of persons other than the individual would be violated.

### **7. Enforcement**

Alcoa will cooperate with European data protection authorities, the U.S. Dept. of Commerce, the U.S. Federal Trade Commission, relevant state or provincial agencies, and law enforcement and judicial authorities in investigating any privacy complaints or suspected violations of privacy laws or Alcoa’s International Safe Harbor commitments, as well as in rectifying any noncompliant practices. Employees or contractors who violate the terms of these principles

may be subject to disciplinary consequences up to and including termination of employment or termination or non-renewal of contract, in addition to any other legal measures that may be taken by Alcoa, its clients, or the affected individuals and their representatives.

## **B. Alcoa as a Data Processor**

With respect to Personal Information received from Europe where Alcoa operates as a data processor, all access to and use of such data is controlled by the Alcoa European subsidiaries and affiliates collecting the data. Staff in Alcoa's North American Data Center have no access to, and make no use of, such data. Their sole function is to provide the limited technical support needed to run the systems on Alcoa servers for the benefit of authorized users in Europe. In accordance with the provisions of Safe Harbor's *FAQ 10 – Article 17 contracts*, Alcoa has entered into a contract with each of its European subsidiaries and affiliates that control data in one of the supported systems. Under the terms of this contract, Alcoa is obligated to process the data only in accordance with instructions from the exporting European business entity and to provide an appropriate level of security for the data. The principles underlying these requirements can be summarized as follows:

### **1. Limits on Processing**

Alcoa acts strictly as an "arms-length" data processor with respect to data in the supported systems referenced above, with the sole responsibility of keeping the systems up and running. Alcoa does not have the authority to access or use the Personal Information in these systems. North American Data Center staff who attempt to bypass security protocols and policies in order to access Personal Information are subject to dismissal and prosecution.

### **2. Security**

Alcoa takes reasonable precautions, including administrative, technical, personnel, and physical measures, to safeguard Personal Information against loss, misuse, theft, and unauthorized access, disclosure, alteration, and destruction. Alcoa's security policies, operating procedures and technical controls, where applicable, generally adhere to commonly accepted standards for security of networks, infrastructure, applications and data.

As indicated in *FAQ 10*, Alcoa's European subsidiaries and affiliates, as data controllers with respect to the data, remain responsible for following other privacy principles or provisions required by local laws, such as those relating to notice, choice, data integrity, access, etc.

## **COMPLIANCE**

Alcoa uses an annual self-assessment program to verify that the attestations it makes under the Safe Harbor Program are true and that its privacy policies are being followed in practice. In addition, Alcoa will cooperate with its European subsidiaries and affiliates and with European data protection authorities to resolve any complaints that may arise in relation to Personal Information transferred under the Safe Harbor Program.

## **POINT OF CONTACT**

Individuals with questions or concerns about the handling of their personal information by Alcoa following its transfer from Europe may contact Alan Levine, Privacy Officer, Pittsburgh, Pennsylvania, USA, by email to [alan.levine@alcoa.com](mailto:alan.levine@alcoa.com). Please put "*Safe Harbor*" in the subject line of the email.

**Safe Harbor Privacy Principles**  
**Effective June 11, 2010**  
**Alcoa, Inc. and its controlled U.S. subsidiaries**