1.12 Privacy Shield Privacy Policy

Effective Date: May 25, 2018

Applicability: This policy is applicable to all employees of Aleris International, Inc. and its subsidiaries and affiliates in the following geographic regions:

- North America: Yes
- Europe: Yes
- Asia Pacific: No
Aleris Corporation and Subsidiaries

PRIVACY SHIELD PRIVACY POLICY
(applicable to EU and Switzerland transfers)

May 25, 2018
PRIVACY SHIELD PRIVACY POLICY

It is the policy of Aleris Corporation and its US-subsidiaries Aleris International, Inc., Aleris Rolled Products Sales Corporation, Aleris Rolled Products, Inc., IMCO Recycling of Ohio, LLC, Nichols Aluminum LLC ("Aleris") to recognize and respect the privacy rights of individuals with respect to Personal Data (as defined herein) it receives. Aleris operates in many countries and recognizes its obligation to comply with applicable privacy and data protection requirements. As part of its compliance with European Union and Swiss privacy laws, Aleris complies with the U.S.-EU Privacy Shield Framework and the U.S.-Switzerland Privacy Shield Framework established by the United States with the European Union and with Switzerland regarding the collection, use, and retention of Personal Data transferred from the EU and Switzerland to the United States. Aleris certifies that it adheres to the Privacy Shield Privacy Principles of notice, choice, onward transfer, access, security, data integrity, and enforcement. Aleris' Privacy Shield certification can be found at www.privacyshield.gov/list. For more information about the Privacy Shield Principles, please visit www.privacyshield.gov.

1. SCOPE:

This Privacy Shield Privacy Policy (hereinafter referred to as the "Policy") applies to all Personal Data received by Aleris from individuals in the EU and Switzerland under the Privacy Shield Programs, as amended from time to time.

2. DEFINITIONS:

As used in this Policy, the following terms shall have the meanings set forth below:

Data Controller means the party or entity that, alone or jointly with others, determines the purposes and means of the processing of Personal Data. 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 means the party or entity that, alone or jointly with others, processes Personal Data 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.

Personal Data means information, including Sensitive Data, relating to an identified or identifiable natural person, which is received by Aleris in the US from the EU or Switzerland, regardless of the medium or format in which the information is recorded. 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 identity.

Sensitive Data means Personal Data that is regarded as posing special risks to individuals, such as information about ethnic or racial origin, health or sex life, political opinions, religious or philosophical beliefs or trade-union membership.

3. ALERIS’ ROLE AND TYPE OF PERSONAL DATA HANDLED:

Aleris receives a variety of Personal Data in order to conduct business. For some Personal Data, Aleris decides the purposes and means of the processing of the data received from The
EU and Switzerland and then uses the data for those purposes. As such, Aleris is acting as a Data Controller for such information. For other Personal Data, Aleris acts as a Data Processor, acting on instructions from a Data Controller, including maintaining data in data centers in the U.S. solely on behalf of its European and Swiss subsidiaries and affiliates.

Aleris collects and uses Personal Data from its affiliates in the EU and Switzerland concerning prospective, current and former employees (including temporary workers and other non-employee personnel), contractors and job applicants ("HR Data"). Aleris may collect, use and process EU/Swiss HR Data for purposes that include, but are not limited to:

(i) selecting, managing and administering its workforce (general personnel administration, recruitment, hiring and termination activities, administration of payroll, performance management, employee communication, management of employee participation in human resources trainings and talent development programs, facilitating employee relocations and international assignments;

(ii) internal business processes and management (reporting, managing information technology and communications systems, such as the corporate email system and company directory);

(iii) compliance with legal and regulatory requirements exercising legal rights or obligations (managing audit and compliance matters, complying with applicable legal obligations, including government reporting and specific local law requirements).

Aleris may disclose EU/Swiss HR Data to third party service providers that perform services on Aleris’ behalf, including, but not limited to, services in connection with finance or other administrative activities, IT support, and HR activities. Aleris will use and disclose such Personal Data in accordance with the notices provided by such entities and the choices made by the individuals to whom it relates.

Aleris also obtains Personal Data of its customers, prospects, partners, vendors, and suppliers from its affiliates in the EU and Switzerland and obtains Personal Data, when an individual visits Aleris’ websites and provides Personal Data to the company ("Non-HR Personal Data"). EU/Swiss Non-HR Personal Data are typically limited to name, business title, and contact information such as business postal address, email address, and telephone number.

Aleris may collect, use and process Personal Data of its EU and Swiss customers and suppliers and other third parties for purposes that include, but are not limited to, the provision of products and services, customer support and relationship management, general business administration, supply chain management, and legal compliance.

Aleris may disclose EU/ Swiss Non-HR Personal Data to third party service providers that perform services on Aleris’ behalf, including, but not limited to, services in connection with finance or other administrative activities and provision of Aleris’ products and services. Aleris will use and disclose such Personal Data in accordance with the notices provided by such entities and the choices made by the individuals to whom it relates.

4. APPLICABLE PRINCIPLES:

Aleris handles the Personal Data referred to above in accordance with the Privacy Shield Principles of Notice; Choice; Onward Transfer; Access; Security; Data Integrity; and Enforcement, as summarized below. A full statement of these principles, may be found on the Privacy Shield website of the U.S. Dept. of Commerce provided above.
4.1. Notice

Before processing Personal Data of any individual who resides in the EU and Switzerland and whose Personal Data is within the scope of the Privacy Shield, Aleris provides the employee with a notice concerning the processing of their Personal Data.

Aleris will not use or disclose Personal Data transferred from the EU and 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 Aleris first comply with the Notice and Choice Principles.

4.2. Choice

Aleris collects and uses Personal Data required to operate its business. Such collection and use of data in the ordinary course of business is subject to the Notice Principle described above but in most circumstances does not require the explicit consent of the individual. Aleris provides individuals in the EU and Switzerland whose Personal Data has been transferred to the United States the opportunity to choose (opt-out) whether their Personal Data will be disclosed to an external third party (other than disclosure to a contractor or agent processing the data solely on Aleris' behalf or disclosure required by law), or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual.

For Sensitive Data, Aleris provides the individual with an affirmative or explicit (opt-in) choice if the information is to be disclosed to an external non-agent third party or used for a purpose other than its original purpose or the purpose authorized subsequently by the individual or a compatible purpose where required by law. Aleris will provide employees or customers with reasonable mechanisms to exercise their choices should such circumstances arise.

4.3. Onward Transfer

Aleris may transfer EU/Swiss HR and Non-HR Personal Data to third parties, including service providers, who act as agents to perform tasks on behalf of and under the instructions of Aleris for purposes related to those set forth above.

With respect to transfers of EU/Swiss HR and Non-HR Personal Data to third-party processors, Aleris (i) enters into a contract with each relevant processor, (ii) transfers Personal Data to each such processor only for limited and specified purposes, (iii) ascertains that the processor is obligated to provide the Personal Data with at least the same level of privacy protection as is required by the Privacy Shield Principles, (iv) takes reasonable and appropriate steps to ensure that the processor effectively processes the Personal Data in a manner consistent with Aleris' obligations under the Privacy Shield Principles, (v) requires the processor to notify Aleris if the processor determines that it can no longer meet its obligation to provide the same level of protection as required by the Privacy Shield Principles, (vi) upon notice, including under (v) above, takes reasonable and appropriate steps to stop and remediate unauthorized processing of the Personal Data by the processor, and (vii) provides a summary or representative copy of
the relevant privacy provisions of the processor to the Department of Commerce, upon request.

Aleris remains liable under the Privacy Shield Principles if the company's third-party onward transfer recipients process relevant Personal Data in a manner inconsistent with the Privacy Shield Principles, unless Aleris proves that it is not responsible for the event giving rise to the damage.

To transfer EU/Swiss HR and Non-HR Personal Data to a third party acting as a controller, Aleris shall comply with the Privacy Shield Notice and Choice Principles. Aleris shall also enter into a contract with the third-party controller. The contract shall provide that such Personal Data may only be processed for limited and specified purposes consistent with the consent provided by the individual. It will provide the same level of protection as the Privacy Shield Principles. The contract will require the third-party controller to notify Aleris if the third-party controller determines it can no longer meet this obligation. The contract shall provide that when such a determination is made the third-party controller shall cease processing or take other reasonable and appropriate steps to remediate.

4.4. Access

Upon reasonable request, Aleris provides individuals an opportunity to access their Personal Data and permits individuals to correct, amend or delete that Personal Data where it is inaccurate or incomplete. Individuals who wish to review or update their Personal Data can do so by contacting Aleris' Global Data Privacy Officer at dataprivacy@aleris.com. Aleris may, in its discretion, charge a reasonable, cost-based fee for access or photocopying.

4.5. Security

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

Aleris utilizes a combination of online and offline technological and organizational measures to help safeguard Personal Data. Aleris also limits access to Personal Data to Aleris' 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.

4.6. Data Integrity

Aleris limits its collection of Personal Data to that which is relevant for the intended business and legal purposes for which it is to be used in accordance with this Policy. Aleris will not process the Personal 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, Aleris takes reasonable steps to ensure that the information it collects is accurate, complete, current, and reliable for its intended use.
Aleris 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.

4.7. Enforcement

Aleris (a) will conduct periodic self-assessments of its relevant practices to verify adherence to this Policy and the Privacy Shield Principles, (b) undertakes obligations to remedy problems arising out of a failure to comply with this Policy and the Privacy Shield Principles, and (c) provides independent recourse mechanisms so that each individual's complaints and concerns regarding Aleris' handling of Personal Data under this Policy can be investigated and resolved where the applicable law so provides.

Any individual who has a complaint concerning Aleris' processing of his or her Personal Data should contact Aleris' Global Data Privacy Officer at dataprivacy@aleris.com. Aleris will investigate and attempt to resolve such complaints in accordance with the Privacy Shield 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.

5. COMPLIANCE:

Aleris uses an internal self-assessment program to verify that this Policy is accurate, comprehensive, prominently displayed, implemented and accessible. The self-assessment program also is used to indicate that this Policy conforms to the Privacy Shield Principles and that Aleris has in place procedures for training employees in its implementation, disciplining employees for failure to follow it and periodically conducting objective reviews of compliance with the foregoing.

Additionally, Aleris is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC) that will effectively ensure compliance with the Privacy Shield Principles.

6. DISPUTE RESOLUTION:

Individuals who have any complaints or concerns regarding Aleris' handling of their Personal Data under the Privacy Shield should contact the Aleris Global Data Privacy Officer as set forth under "Contact Person" below. Aleris will address the complaint or concern and strive to reach a satisfactory resolution.

For those complaints or concerns regarding Personal Data that is human resources data that cannot be resolved through the internal dispute resolution process, in accordance with the Privacy Shield Program, Aleris will cooperate in investigations by and comply with the advice of competent European Union or Swiss data protection authorities, as the case may be.

For those complaints or concerns regarding Personal Data other than human resources data that cannot be resolved through the internal dispute resolution process, Aleris has selected the International Centre for Dispute Resolution division of the American Arbitration Association, an alternative dispute resolution provider located in the United States, as its independent dispute resolution mechanism (see www.icdr.org). If you do not receive timely acknowledgement for your complaint from Aleris, or if Aleris has not addressed your complaint to your satisfaction,
please contact or visit ICDR-AAA at [http://go adr org/privacyshield.htm](http://go adr org/privacyshield.htm) for more information or to file a complaint.

Additionally, you have the option to invoke binding arbitration for the resolution of claimed violations of the Privacy Shield Principles not resolved by any of the other Privacy Shield mechanisms, if any.

**7. CONTACT PERSON:**

Individuals who have questions, complaints or concerns, access requests or any other issues regarding the handling of their Personal Data by Aleris under the Privacy Shield Programs should contact Jill Cutwright, Global Data Privacy Officer, Beachwood, Ohio, by email to dataprivacy@aleris.com. Please put “Privacy Shield” in the subject line of the e-mail.

This Privacy Shield Privacy Policy is approved:
May 25, 2018

Sean M. Stack, Chairman and Chief Executive Officer