EU-US Privacy Shield
Privacy Policy

Blount International, Inc. ("Blount") has created this Information Protection and Privacy Statement ("Policy") in order to demonstrate our commitment to the EU-US Privacy Shield framework as set forth by the U.S. Department of Commerce ("Privacy Shield") regarding the collection, use, and retention of personal information from European Union member countries. The rules by which information is handled are determined by the framework, our business requirements, and company commitments relating to that type of information and the purposes for which it is collected and maintained. Blount is committed to compliance with the Privacy Shield Principles ("Principles") with regard to all personal data received from the European Union ("EU") in reliance on the Privacy Shield, and to further demonstrate that compliance, Blount is self-certified in the Privacy Shield program. This Policy applies to Blount's subsidiaries, affiliates, divisions and business units.

This Policy outlines our adherence and commitment to how we will handle the personal information of our Team Members and customers, including Notice, Choice, Accountability Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, and Recourse, Enforcement and Liability. Certain types of personal information can be deemed sensitive ("Sensitive Information") by its nature (*e.g.*, financial, health, religion or sexual orientation) and due to regulations and industry standards, (*e.g.*, geopolitical data protection standards, federal guidelines, or state-based frameworks, such as data breach notice laws or driver's license privacy acts) additional types of Sensitive Information can include:

- Client information, including, without limitation, business records and employee data;
- Government issued identification numbers, financial information, including, without limitation, credit cards, salaries, banking, and transactions;
- Medical or healthcare information of all types;
- Company patents, business plans, and other intellectual property;
- Company and client business records and planning materials, including, without limitation, customer list, marketing and sales efforts, and product line plans; and
- Intellectual property or other proprietary materials, both which our company creates and those which we obtain under license from others.

Most of this Sensitive Information resides within our computing infrastructure, including internal computer systems and paper files, as well as within the computing and storage infrastructure of our third-party services providers. Regardless of where the information is located, Sensitive Information must be properly protected against unauthorized access and disclosure at all times. Every Team Member, contractor, supplier or vendor, agent or representative of Blount must be aware of the significance of the information being handled, and ensure that proper controls are applied to prevent copying, unauthorized disclosure, or other misuse of Sensitive Information.

Blount relies upon its Team Members and business partners to properly develop, maintain, and operate our systems, networks, and processes which keeps our Sensitive Information safe and properly used. This means that every person and organization handling our Sensitive Information has the responsibility to keep the information safe, no matter where the information is located. This includes computing systems, networks, paper copies, business processes, and verbal transmission of information.

If there is any conflict between the principals 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 page, please visit https://www.privacyshield.gov/.

1. Notice and Personal Information Collection

Blount may collect personal information like the name, telephone number, email address, date of birth, home or business and mailing address when you access, for example: (1) certain areas of Blount's web sites that require registration for certain services; (2) when you become employed by Blount: (3) when you conduct business with Blount; or (4) if you require information about Blount's products or services.

The personal information that Blount collects is used for business purposes. Blount will provide you with the choice and means for limiting the use and disclosure of your personal information before Blount uses or discloses the information for a purpose other than for which it was originally collected. You have the right to access your personal data, which includes the choice to limit the use and disclosure of your personal data.

Blount participates in an independent third-party dispute resolution program, and will be liable for onward transfers of your personal information that violate our obligations under Privacy Shield. Blount's independent dispute resolution body is BBB an alternative dispute resolution provider based in the United States.

2. Choice.

Blount offers you the opportunity to choose (opt-out) whether personal information is: (1) to be disclosed to a third party, unless that third-party is under contract as an agent of Blount to perform an essential business process, and is bound by contract to treat your personal information in compliance with the Privacy Shield principles; or (2) to be used for a purpose that is materially different from the purposes for which it was originally collected or subsequently authorized by the individual. You will be notified before we use your personal information for such materially difference purposes.

To opt-out of such use, send an email to privacy@blount.com and include "Opt-Out" in the subject line.

For personal information that includes medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sexual preference of the individual ("Sensitive Personal Information"), Blount will

give individuals the opportunity to grant affirmative express consent (opt-in) prior to it being (i) disclosed to a third party or (ii) used for a purpose other than those for which it was originally collected or subsequently authorized by the individuals through the exercise of opt-in choice. Blount shall treat Sensitive Personal Information received from an individual the same as the individual would treat and identify it as Sensitive Personal Information. Conversely, Blount will treat as Sensitive Information, any personal information that Blount receives from a third party that the third party identifies and treats as sensitive.

3. Accountability For Onward Transfer.

Before Blount transfers personal information to a third party acting as a controller, Blount will enter into a contract with the third-party controller to ensure that personal information may only be processed for limited and specified purposes consistent with the consent provided by the individual, the recipient will provide the same level of protection as the Principles and the third-party controller will notify Blount if it makes a determination that it can no longer meet these obligations. The contract will also provide that when such a determination is made, that the third-party controller will cease to process the personal information or take other reasonable and appropriate steps to and remediate unauthorized processing.

Before Blount transfers personal data to a third party acting as an agent, Blount will: (i) ensure that the transfer of such data is only for limited and specified purposes; (ii) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with Blount's obligations under the Principles; (iv) require the agent to notify Blount if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles; (v) upon notice, including under (iv) above, take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vi) provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department of Commerce upon request.

Blount also may be required to disclose an individual's personal information in response to a lawful request by public authorities, including to meet national security or law enforcement requirements.

In cases of onward transfer to third parties of data of EU individuals received pursuant to the EU-US Privacy Shield, Blount is potentially liable.

4. Security.

Blount Information Security Policies regarding the creation, maintenance, use or dissemination of personal information reflect Blount's reasonable and appropriate measures to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.

5. Data Integrity And Purpose Limitation.

Consistent with the Principles, Blount will ensure that personal information must be limited to information that is relevant for the purposes of processing. Blount will not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, Blount will take reasonable steps to ensure that personal information is reliable for its intended use, accurate, complete and current.

Blount will retain information in a form identifying or making identifiable the individual only for as long as it serves a purpose of processing. This obligation does not prevent Blount from processing personal information for longer periods of time and to the extent such processing reasonably serves the purposes of archiving in the public interest, journalism, literature and art, scientific or historical research, and statistical analysis. In these cases, such processing shall be subject to the other Principles and provisions of the framework.

6. Access.

Blount acknowledges that individuals have the right to access, correct, amend or delete the personal information that we maintain about them, where it is inaccurate, or has been processed in violation of the Principles, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

An individual who seeks access, or who seeks to correct, amend, or delete inaccurate data, should direct his query to privacy@blount.com. If requested to remove data, we will respond within a reasonable timeframe.

7. Enforcement.

In compliance with the Principles, Blount commits to resolve complaints about your privacy and our collection or use of your personal information. If you have further questions or need to make in inquiry about our Privacy Shield program or have general questions about your personal information, or if you are a European Union citizen with inquiries or complaints regarding this privacy policy you should first contact Blount:

Blount International Inc.
4909 SE International Way
Attn: General Counsel
P.O. Box 22127 (97269-2127)
Portland, OR 97222-4679

Blount has further committed to refer unresolved privacy complaints under the Privacy Shield to an independent dispute resolution mechanism, the BBB Privacy Shield Program, operated by the Council of Better Business Bureaus. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed within 45 days, please visit the BBB EU Privacy Shield web site at www.bbb.org/EU-privacy-shield/for-eu-consumers/ for more information and to file a complaint.

Please note that if your complaint is not resolved through these channels, under certain conditions, a binding arbitration option may be available before a Privacy Shield Panel.

Blount commits to cooperate with EU data protection authorities (DPAs) and comply with the advice given by such authorities with regard to human resources data transferred from the EU in the context of the employment relationship. Blount is subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC).

8. Other information Collection.

At other times, Blount may collect information that cannot be used to identify you. For example, we may aggregate non-personal information about you and other customers who visit our Web sites. Aggregated information will not contain any information that can be linked directly back to you.

9. How Blount Collects Personal Information.

Consistent with the Principles, personal information that Blount collects will be limited to the information that is relevant for the purposes of processing. Examples of such processing include those that reasonably serve customer relations, compliance and legal considerations, auditing, security and fraud prevention, preserving or defending the organization's legal rights, or other purposes consistent with the expectations of a reasonable person given the context of the collection. Blount will not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, Blount will take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete, and current. Blount will adhere to the Principles for as long as it retains such information.

Our Internet Service Providers (defined below) may also use other standard web-based technologies to analyze your movements while accessing our Web Sites. The technologies include web "beacons," "pixel tags," and "clear gifs." These technologies help us ascertain the effectiveness of our product and service campaigns and marketing programs, allow us to customize the services offered on or through our Web sites, and help determine the best use for Web sites content, and product and service offerings. Some of this information, including the Internet Protocol ("IP") address, may be stored on our Internet Service Provider's server logs, and may be available for extended periods of time.

10. Our Use and Disclosure of Your Personal Information.

At times, Blount may use the services of independent companies to provide certain services to you, including, without limitation, web site hosting services, credit card processing, order processing and shipping services, and guest surveys ("Internet Service Providers"). Blount may share your personal information with the Internet Service Providers as appropriate. We do not share personally identifiable information with outside third parties without your consent, except to the extent necessary to complete your request for products and services offered through the Blount Web sites.

Blount may use your personal information to contact you via mail, e-mail, or telephone in order to give you updates about Blount's special events, new services, current information regarding our products, or other promotions that may be of interest to you. If you are a business or organization that has scheduled a conference, event, or meeting at one of our facilities, we may also share your personal information with our event organizers. We also use return e-mail addresses to answer the e-mail we receive from you. Your e-mail address will not be used for any other purpose or shared with outside third parties for their direct marketing purposes. We may also use your IP address to help protect Blount and our Internet Service Providers from fraud.

Additional uses of your non-personal and personal information will allow us to tailor products and services specific to your needs, to help organize and manage our relationship with you or your business, to conduct business, to provide you with customer and guest support, to perform functions that are described to you at the time of collection, and to enforce our Web site's Terms of Use.

We may also use non-personal aggregate information to improve our technical operations. For example, our Internet Service Providers may report to us that there were a particular number of visitors to a certain area of our Web sites, or that a certain number of businesses or a certain number of individuals completed our registration forms in particular areas of our Web site. Such information may also be used to analyze the effectiveness of our business and advertising models.

If you submit a resume or seek to fulfill other staffing requirements, we will use that information solely in connection with your application for current or future staffing requirements, and we may also share your resume or application information with our business partners or affiliates that have staffing requirements for which you may be qualified.

Blount may also disclose your personal information as is necessary to: (a) comply with a subpoena or court order; (b) cooperate with law enforcement or other government agencies; (c) establish or exercise our legal rights; (d) protect the property or safety of our company and employees, contractors, vendors, suppliers, and customers; (e) defend against legal claims; (f) help with internal and external investigations; or (g) as otherwise required by law or permitted by law. We may disclose your information in connection with the sale or merger of Blount or any transaction that involves the sale or assignment of some or all of our assets.

11. General Information and Privacy Support Contact.

Blount may update this privacy policy from time to time, and you should take the time to review it each time that you visit one of our Web sites. Blount is committed to protecting your personal privacy. If you have questions or comments about our efforts to protect your personal privacy, or if you require additional information about Blount's privacy commitment, please contact us at privacy@blount.com.

Adapted: September 27, 2016