

# The Allied Group Privacy Shield Policy

The Allied Group, Inc. ("Allied") has adopted this Privacy Shield Policy ("Policy") with an effective date of June 6, 2017 to establish and maintain an adequate level of Personal Data privacy protection. This Policy applies to the processing of Personal Data that Allied obtains from Customers.

Allied complies with the EU-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries. Allied has certified that it adheres to the Privacy Shield Privacy Principles and is committed 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. If there is any conflict between the policies in this privacy policy and the Privacy Shield Privacy Principles, the Privacy Shield Privacy Principles shall govern. To learn more about the Privacy Shield program, and to view our certification page, please visit <https://www.privacyshield.gov>.

***All Allied employees who handle Personal Data from Europe are required to comply with the Principles stated in this Policy.***

Capitalized terms are defined in Section 14 of this Policy.

## I. SCOPE

This Policy applies to the processing of Customer Personal Data that Allied receives in the United States concerning Customers who reside in Europe. Allied provides various services, including the printing, kitting and distribution of products to individuals residing in Europe on behalf of its Customers.

This Policy does not cover data from which individual persons cannot be identified or situations in which pseudonyms are used. (The use of pseudonyms involves the replacement of names or other identifiers with substitutes so that identification of individual persons is not possible.)

## II. RESPONSIBILITIES AND MANAGEMENT

Allied has designated an internal team to oversee its information security program, including its compliance with the Privacy Shield program. The internal team shall review and approve any material changes to this program as necessary. Any questions, concerns, or comments regarding this Policy also may be directed to [privacyshield@thealliedgrp.com](mailto:privacyshield@thealliedgrp.com).

Allied will maintain, monitor, test, and upgrade information security policies, practices, and systems to assist in protecting the Personal Data that it collects. Allied personnel will receive training, as applicable, to effectively implement this Policy. Please refer to Section 7 for a discussion of the steps that Allied has undertaken to protect Personal Data.

Pursuant to the Privacy Shield, Allied remains liable for the transfer of personal data to third parties acting as our agents unless we can prove we were not a party to the events giving rise to the damages.

### III. RENEWAL / VERIFICATION

Allied will renew its Privacy Shield certification annually, unless it subsequently determines that it no longer needs such certification or if it employs a different adequacy mechanism.

Prior to the re-certification, Allied will conduct an in-house verification to ensure that its attestations and assertions with regard to its treatment of Customer Personal Data are accurate and that the company has appropriately implemented these practices. Specifically, as part of the verification process, Allied will undertake the following:

- Review this Privacy Shield policy and its publicly posted website privacy policy to ensure that these policies accurately describe the practices regarding the collection of Customer Personal Data
- Ensure that the publicly posted privacy policy informs Customers of Allied's participation in the Privacy Shield program and where to obtain a copy of additional information (e.g., a copy of this Policy)
- Ensure that this Policy continues to comply with the Privacy Shield principles
- Confirm that Customers are made aware of the process for addressing complaints and any independent dispute resolution process (Allied may do so through its publicly posted website, Customer contract, or both)
- Review its processes and procedures for training Employees about Allied's participation in the Privacy Shield program and the appropriate handling of Customer Personal Data

### IV. COLLECTION AND USE OF PERSONAL DATA

Allied provides various solutions to its Customers, which are predominantly business customers. Allied collects Personal Data directly from Customers when they purchase our products and services and indirectly when acting as a service provider to its Customers. The Personal Data that we collect may vary based on the Customer's interaction with our website and request for our services. As a general matter, Allied collects the following types of Personal Data directly from its Customers: contact information, including, a contact person's name, work email address, work mailing address, work telephone number, title, and company name.

For certain products, Allied serves as a service provider to its Customers. In our capacity as a service provider, we will receive, store, and/or process Personal Data owned and/or controlled by our Customers, including information about their employees, clients, customers, agents, or other individuals. In such cases, we will process the personal information on behalf of and under the direction of each particular Customer. The information that we collect from our Customers in this capacity is used for managing transactions, reporting, and other operations related to providing services to the Customer, and as otherwise requested by the Customer.

Allied uses Personal Data that it collects directly from its Customers and Customers' customers indirectly in its role as a service provider for the following business purposes, without limitation: (1) maintaining and supporting its products, delivering and providing the requested products/services, and complying with its contractual obligations related thereto (including

managing transactions, reporting, and other operations related to providing services to a Customer); (2) satisfying governmental reporting, tax, and other requirements (e.g., import/export); (3) storing and processing data, including Personal Data, in computer databases and servers located in the United States; (4) as requested by the Customer; (5) for other business-related purposes permitted or required under applicable local law and regulation; and (6) as otherwise required by law.

## V. DISCLOSURES / ONWARD TRANSFERS OF PERSONAL DATA

Except as otherwise provided herein, Allied discloses Personal Data only to Third Parties who reasonably need to know such data. Such recipients must agree to abide by confidentiality obligations. Examples of Third Parties that may receive personal information include suppliers that have been contracted on behalf of our Customer and are primarily providers of Recognition Awards. All Third Parties receiving personal information must have a written agreement in place between Allied and Third Party that obligates the Third Party to meet or exceed the Privacy Shield standards set forth in this policy.

Allied may be forced to disclose an individual's personal information when compelled by a request made by a recognized public authority or where required to meet national security and or law enforcement requirements.

Allied's accountability for personal data that it receives under the Privacy Shield and subsequently transfers to a third party is described in the Privacy Shield Principles. In particular, Allied remains responsible and liable under the Privacy Shield Principles if third-party agents that it engages to process the personal data on its behalf do so in a manner inconsistent with the Principles, unless Allied proves that it is not responsible for the event giving rise to the damage.

## VI. SENSITIVE DATA

Allied does not collect Sensitive Data from its Customers.

## VII. DATA INTEGRITY AND SECURITY

Allied uses reasonable efforts to maintain the accuracy and integrity of Personal Data and to update it as appropriate. Allied has implemented physical and technical safeguards to protect Personal Data from loss, misuse, and unauthorized access, disclosure, alternation, or destruction. For example, electronically stored Personal Data is stored on a secure network with firewall protection, and access to Allied's electronic information systems requires user authentication via password or similar means. Allied also employs access restrictions, limiting the scope of employees who have access to Customer Personal Data.

*Despite these precautions, no data security safeguards guarantee 100% security all of the time.*

## VIII. NOTIFICATION

Allied notifies Customers about its adherence to the Privacy Shield principles through its publicly posted website privacy policy, available at [www.thealliedgrp.com/privacysshield](http://www.thealliedgrp.com/privacysshield).

## IX. ACCESSING PERSONAL DATA

Allied personnel may access and use Personal Data only if they are authorized to do so and only for the purpose for which they are authorized.

## X. RIGHT TO ACCESS, CHANGE OR DELETE PERSONAL DATA

1. Right to Access. Data Subjects have the right to know what Personal Data about them is included in the databases and to ensure that such Personal Data is accurate and relevant for the purposes for which Allied collected the Personal Data. Data Subjects may review their own Personal Data stored in the databases and correct, erase, or block any data that is incorrect, as permitted by applicable law.
2. Requests for Changes to Personal Data. Allied allows Data Subjects that have directly supplied Allied with their Personal Data the ability to access their Personal Data upon reasonable request as required by the Privacy Shield principles in order to correct or amend such data where inaccurate. Data Subjects may edit or request erasure of their Personal Data by contacting Allied by email at [privacyshield@thealliedgrp.com](mailto:privacyshield@thealliedgrp.com). In making modifications to their Personal Data, Data Subjects must provide only truthful, complete, and accurate information. Data Subjects that have submitted their Personal Data to an Allied Customer should contact the Customer to access and update their data.
3. Tracking Requests for Personal Data . Allied will track each of the following and will provide notice to the appropriate parties under law and contract when either of the following circumstances arise: (a) legally binding request for disclosure of the Personal Data by a law enforcement authority unless prohibited by law or regulation; or (b) requests received from the Data Subject. If Allied receives a request for access to his/her Personal Data from a Customer's customer, then, unless otherwise required under law or by contract with such Customer, Allied will refer such Data Subject to Customer.
4. Satisfying Requests for Access, Modifications, and Corrections. Allied will endeavor to respond in a timely manner to all reasonable written requests to view, modify, or inactivate Personal Data.
5. Limiting Use of Personal Data. You may request limitations on the use and disclosure of your personal data specified in this agreement by contacting us at [privacyshield@thealliedgrp.com](mailto:privacyshield@thealliedgrp.com).

## XI. CHANGES TO THIS POLICY

This Policy may be amended from time to time, consistent with the Privacy Shield Principles and applicable data protection and privacy laws and principles. We will make employees aware of changes to this policy either by posting to our intranet, through email, or other means. We will notify Customers if we make changes that materially affect the way we handle Personal Data previously collected, and we will allow them to choose whether their Personal Data may be used in any materially different manner.

## XII. QUESTIONS OR COMPLAINTS

Customers may contact Allied with questions or complaints concerning this Policy at the following address; [privacyshield@thealliedgrp.com](mailto:privacyshield@thealliedgrp.com).

## XIII. ENFORCEMENT AND DISPUTE RESOLUTION

In compliance with the Privacy Shield Principles, Allied commits to resolve complaints about your privacy and our collection or use of your personal information. European Union individuals with inquiries or complaints regarding this privacy policy should first contact Allied at: [privacyshield@thealliedgrp.com](mailto:privacyshield@thealliedgrp.com).

Allied has further committed to refer unresolved privacy complaints under the Privacy Shield Principles to an independent dispute resolution mechanism, the BBB EU PRIVACY SHIELD, operated by BBB National Programs. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit <https://bbbprograms.org/privacy-shield-complaints/> for more information and to file a complaint. This service is provided free of charge to you.

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

As part of this agreement, Allied subjects itself to the investigatory and enforcement powers of the Federal Trade Commission (FTC).

## XIV. DEFINITIONS

Capitalized terms in this Privacy Policy have the following meanings:

**"Customer"** means a prospective, current, or former vendor, supplier, or client of Allied.

**"Data Subject"** means an identified or identifiable natural living person. An identifiable person is one who can be identified, directly or indirectly, by reference to a name, or to one or more factors unique to his or her personal physical, psychological, mental, economic, cultural or social characteristics.

**"Employee"** means an employee (whether temporary, permanent, part-time, or contract), former employee, independent contractor, or job applicant of Allied or any of its affiliates or subsidiaries, who is also a resident of a country within the European Economic Area.

**"Europe"** or **"European"** refers to a country in the European Economic Area.

**"Personal Data"** as defined under the European Union Directive 95/46/EC means data that personally identifies or may be used to personally identify a person, including an individual's name in combination with country of birth, marital status, emergency contact, salary information, terms of employment, job qualifications (such as educational degrees earned), address, phone

number, e-mail address, user ID, password, and identification numbers. Personal Data does not include data that is de-identified, anonymous, or publicly available.

**"Sensitive Data"** means Personal Data that discloses a Data Subject's medical or health condition, race or ethnicity, political, religious or philosophical affiliations or opinions, sexual orientation, or trade union membership.

**"Third Party"** means any individual or entity that is neither Allied nor an Allied employee, agent, or representative.