1 Scope

This Privacy and Personal Data Protection Policy (this "Policy") applies to Allegis Group, Inc. and its subsidiaries (collectively referred to as the "Company"). This Policy applies to Company personnel, including employees, temporary workers, and any authorized representatives, contractors, or agents (collectively referred to as "Company Personnel," "You" or "you"). Capitalized terms have the definitions indicated in Section 17 of this Policy or as otherwise defined herein.

All of the Company's other personnel policies remain in full force and effect. Except to the extent in conflict with this Policy, the Company's Employee Handbook, Company Code of Conduct and Ethics, and other policies supplement this Policy.

This Policy applies whether or not the activities are conducted from the Company's premises.

This Policy and the practices established therein are mandatory and will be enforced worldwide.

This Policy establishes a minimum level of standards. Local facilities may adopt stricter policies upon the prior written approval of the Information Security Council. You are responsible for compliance with this Policy and any similar or supplementary policies that may be adopted by your local facility.

If as part of your relationship with the Company you provide services directly to a customer of the Company, either at the customer's facility or remotely, you will be subject to this Policy as well as any similar policy issued by the customer.

2 Purpose

The Company respects your right to privacy. This Policy outlines how we protect your Personal Data when it is in the custody and control of the Company.

The Company collects Personal Data from its employees and from people whom it may potentially employ, and at times, it may collect Personal Data from customers. Your Personal Data is only collected, used, and disclosed by the Company in accordance with this Policy. Personal Data may not be added to a Company Database unless it is collected and processed in accordance with this Policy.

This Policy, together with the policies listed in the Related Policies section of this Policy, provides the foundation for the Company's information security program ("Information Security Program"). The Information Security Program includes established safeguards as well as ongoing initiatives related to information security and data privacy. The goal of the Information Security Program is to ensure that all information assets identified with, owned by, or entrusted to the Company are protected in a manner consistent with the value attributed to them by the Company in accordance with business requirements, customer requirements, and relevant laws and regulations, as technically feasible. Appropriate controls, whether physical, technical, or administrative, are implemented and managed with the intent of protecting the confidentiality, integrity, and availability of these assets. The Information Security Program seeks to inform and ensure that all Company Personnel, partners, customers, and suppliers who work with the Company's information assets abide by these controls and protect these assets from loss and from unauthorized access, use, modification, destruction, or disclosure.

This Policy adheres to the United States Department of Commerce U.S.–EU Safe Harbor Framework, which has been approved by the European Commission as an adequate way for the Company to demonstrate that it is compliant with the privacy protections outlined in European Union ("EU") Directive 95/46/EC. In addition, this Policy adheres to the U.S.-Swiss Safe Harbor Framework, which has been approved by the Federal Data Protection and Information Commissioner of Switzerland as an adequate way for the Company to demonstrate that it is compliant with the privacy protections outlined in the Swiss Federal Act on Data Protection. In processing Personal Data, the Company complies with the following Safe Harbor principles: Notice, Choice, Onward Transfer (to third parties), Security, Data Integrity, Access, and Enforcement (including Verification, Self-Assessment, and Dispute Resolution).

3 Collection, Notice, and Disclosure

3.1 Collection of Personal Data and Notice

3.1.1 Definition of Personal Data: Personal Data means any information relating to an identified or identifiable natural person ("Data Subject"). 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/her physical, physiological, mental, economic, cultural, or social identity. Personal Data includes an individual's name, email address, work or home telephone number, home postal or other physical address, birth date, driver's license number or other municipality-issued identification card number, Social Security number or other national identification number, financial account, credit card or debit card number, geolocation data, or other information that may enable identification of a person or individual. What constitutes Personal Data varies by region and country. In the European Union and Canada, for example, an individual's Internet Protocol (IP) address can be considered personal information (depending on how it is used), and in Canada and India, passwords are considered personal information.

3.1.2 Collection of Personal Data: The Company collects Personal Data to operate effectively and to comply with government regulations (e.g., regulations governing employment, tax, and insurance). The Company collects and maintains Personal Data from its current and former employees, temporary workers, and their respective dependants and beneficiaries, from individuals it may potentially employ or place for permanent or temporary employment with the Company's customers, from current and former contingent workers (including temps and other non-employees) of the Company, and at times it may collect or be exposed to Personal Data from its customers. Through certain of the Company's web sites, the Company collects Personal Data that is voluntarily provided by users who sign up for a job through Company's online job boards or other Company web sites that allow users to set up an account or otherwise submit information for the purpose of searching for temporary or permanent employment opportunities, submit a resume for inclusion in a Company database, or respond to a specific, listed employment position.

3.1.3 Personal Data – Where Included: Personal Data about a Data Subject may be collected and included in the following:

- Resumes
- Online submissions to Company job boards
- Company interview notes;
- Information obtained through reference and background checks;
- Educational or professional accreditation records;
- Information necessary to provide payroll services, including banking details, tax deductions, and vacation allowances;
- Information necessary to comply with laws or regulations (e.g., OFCCP, I-9s)
- Information about employees, temporary workers, and their respective dependants and beneficiaries, as required, to enroll in any benefits packages;
- Reference letters;
- Video surveillance tapes and other records related to the use of Company resources and property; and
- Test results, including without limitation medical and fitness testing, psychological testing and drug and alcohol testing.

3.1.4 Personal Data from Customers: In order to provide services to the Company's customers, we may collect Personal Data from our customers. The Company may collect this information solely for the purposes of managing the work that the Company is contracted to manage and to communicate among affiliated entities within the Company regarding the services the Company may provide to customers and for no other reason. The Company will abide by any contractual obligations contained in any customer agreement related to the collection of Personal Data that the Company receives from the customer.

3.1.5 Notice to Data Subjects Regarding Purpose: The Company notifies all Data Subjects about the purposes for which Personal Data is collected and used. In appropriate situations, however, Personal Data **may be "anonymized" so that the identity of individual Data Subjects cannot be known**. In these cases, the Company will not (and is not required to) notify the Data Subjects regarding the purpose for which Personal Data is collected and used by the Company, because anonymized data is not considered to be Personal Data.

3.1.6 Requests for Personal Data: When requesting Personal Data (online or offline), fields that are required to be completed by the Data Subject must be identified as such. For example, if the Data Subject is required to submit his/her name and email address in order to participate, but is also asked for his/her physical address, employer, and title, the "name" and "email address" fields should be identified as required/mandatory fields and the consequences of failure to complete these fields should be indicated.

3.1.7 Required Data Fields: The Company will require that any data fields be mandatory only where the Personal Data is necessary to achieve the stated purpose.

3.2 Collection of Sensitive Data

Unless permitted or required by applicable law, Sensitive Data will not be collected from anyone, including but not limited to employees, temporary workers, and their respective dependants and beneficiaries, prospective employees, customers, online visitors, business partners, and other third parties, and may not be stored in the Company's Databases or by vendors or other third parties acting on the Company's behalf. In some jurisdictions, an individual cannot validly consent to the processing of his/her Sensitive Data unless such processing is required by law.

3.3 Confidentiality of Personal Data

Personal Data is considered confidential and should not be disclosed within the Company except to those employees who "need to know" and third-party non-employees who "need to know" such information to satisfactorily perform their jobs and have expressly agreed to protect its confidentiality. Those who "need to know" are those who need the information to properly perform their jobs and could not be expected to do so without access to such information. Generally, employees should exercise reasonable diligence to avoid disclosure of Personal Data to third parties except when necessary and only after appropriate security precautions are taken and/or the proper consent has been obtained. In addition to using Personal Data internally, the Company may at times share this information with third parties. The Company only shares Personal Data about Data Subjects that is relevant to the Company's legitimate business purposes or as required to meet legal and regulatory requirements and at all times pursuant to a Permitted Use. All Personal Data transferred to a third party will be considered "confidential" unless otherwise specified.

3.4 Transfer of Personal Data to Other Countries

As the Company is headquartered in the United States but has operations worldwide, your Personal Data may be transferred to or accessed from countries outside your country of origin, including without limitation Canada, the EU, and India. Because these countries may not have similar data protection laws to your country of origin, the Company has taken numerous steps to protect your Personal Data, including joining the U.S.-EU Safe Harbor and the U.S.-Swiss Safe Harbor programs. The Company may transfer the Personal Data of its employees located in Canada, the EU, India, and other countries to the United States, to any Company subsidiary worldwide, or to third parties acting on our behalf for processing and storage. We safeguard your privacy interests around the world by ensuring that the Company adheres to the Safe Harbor principles and the data protection principles described in this Policy and by entering into binding data transfer agreements as appropriate. By providing the Company with your Personal Data, you consent to its transfer, storage, and/or processing outside your country of origin, including without limitation the processing of your Personal Data in the United States.

4 Choice / Consent

4.1 Use of Personal Data Limited to Purpose for Collection

Personal Data may not be collected or used for purposes other than the purpose for which the Data Subject supplied the Personal Data, unless the Data Subject has consented to such collection and/or use. This consent will generally be by Opt-in, except where Opt-out is permitted under this Policy and applicable law. Where it is allowed in accordance with this Policy, consent is only valid to the extent and for the purpose that the Data Subject has been informed of at the time, and if subsequently a different purpose is intended, it will be necessary to go back and inform the Data Subject providing a renewed opportunity to consent.

4.2 Opt-In Right

Where required by applicable law, Data Subjects must be given the option to Opt-in to use their Personal Data for purposes other than the purpose for which the Personal Data was supplied. This includes all methods of collection, whether on-line, business replay or other mail-back cards, or otherwise. Additionally, where required by applicable law, Data Subjects must be given the opportunity to Opt-in if the Personal Data is to be disclosed to a third party.

4.3 Opt-Out Right

Where required by applicable law, a Data Subject must be given the opportunity to Opt-out from allowing the Company to disclose Personal Data to a third party and the choice of whether or not to allow the Company to use the Personal Data for purposes incompatible with the purpose for which it was originally collected or authorized. The Company reserves the right to require sufficient information to confirm the identity of the individual requesting Opt-out.

4.4 Right to Withdraw Consent

Where required by applicable law, a Data Subject must be given the opportunity to withdraw his/her consent at any time. This right cannot be conditioned or restricted.

5 Use and Disclosure of Personal Data

5.1 Permitted Uses of Personal Data

Personal Data may not be used, collected, retained, distributed, or disclosed except in accordance with a Permitted Use. The following are Permitted Uses:

- To provide the ability to contact the Data Subject;
- To comply with contractual arrangements with our customers;
- To comply with human resources requirements, including conducting workplace investigations involving the Company or a customer of the Company;
- To comply with government regulations or requests from governmental authorities;
- To provide payroll and human resources functions, including employee benefits programs;
- To support recruitment inquiries;
- To facilitate the job search process and to help the Company find a suitable temporary or permanent job match for the Data Subject, including providing Personal Data to customers of the Company to facilitate the temporary or permanent placement process;
- To measure the number of users and usage of our web sites;
- To store information about the Data Subject's online preferences;
- To recognize when the Data Subject returns to our web sites;
- To provide the Data Subject with information on goods and services requested or which may interest the Data Subject, where the Data Subject has consented to be contacted for such purposes;
- For marketing, advertising and promotions, notification of events, surveys, workshops, and training sessions run by the Company;
- To notify the Data Subject about changes to our services;
- Pursuant to a consent from the Data Subject;

- To conduct a business transaction, such as a merger or sale involving all or part of the Company or as part of a corporate reorganization or other change in corporate control;
- To comply with a search warrant or other legally valid inquiry or order;
- To establish, exercise or defend legal claims; and
- Where the disclosure of Personal Data is permitted or required by applicable local or foreign law, including lawful access by foreign courts or governmental authorities (collectively and individually a "Permitted Use").

5.2 Fair and Lawful Processing of Personal Data

Personal Data must be processed fairly and lawfully. Personal Data must be collected, used, and disclosed for a specified, explicit, and legitimate purpose and not further processed other than for that purpose.

5.3 Accuracy of Personal Data

Personal Data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that data which is inaccurate or incomplete, having regard to the purposes for which it was collected and for which it is further processed, are erased or rectified.

5.4 Retention of Personal Data

Personal Data must be kept in a form that permits identification of Data Subjects for no longer than is necessary for the purposes for which the data was collected or for which it is further processed. Once the Personal Data is no longer needed for legal or legitimate business purposes, the Company will destroy or anonymize the Personal Data in accordance with the Company's Records Retention Policy.

6 Data Security

6.1 Security Measures for Personal Data

The Company will strive to provide security that is proportional to the sensitivity of the Personal Data being protected. The following technical, administrative, and organizational measures must be implemented and observed to protect Personal Data from accidental or unlawful destruction or accidental loss, alteration, or unauthorized disclosure, use or access, and against all other unlawful forms of processing. At all times, Personal Data must be handled according to the Company's Information SecurityProgram.

6.1.1 Restricted and Secured Access: All Personal Data must be kept secure with restricted access. Access to Personal Data must be restricted via use of secure passwords and limited to those with a legitimate business purpose related to a Permitted Use.

6.1.2 Database Identification: Databases must identify the Permitted Uses of the Personal Data.

6.1.3 Disclosure of Personal Data to Third Parties: The Company may not always be able to control how Personal Data will be handled by a third party. Where required by applicable law, however, prior to the disclosure of Personal Data to a third party, the Company will obtain a written agreement from the third party obligating the third party to provide the same level of administrative, physical, and technical safeguards to protect Personal Data as used by the Company and requiring the third party to return to the Company or certify adequate destruction of the Personal Data when the third party ceases to be a data processor of the Personal Data. Where required by applicable law, this agreement must restrict the third party's use of the Personal Data to only the purposes for which it was obtained. Additionally, when appropriate or required by applicable law, the Company must be given the contractual right to periodically audit a third-party vendor's use, processing, storage, and destruction of Personal Data.

6.1.4 Third Party Obligations Regarding Personal Data Breaches: As part of the overall effort to adequately protect Personal Data, when appropriate or required by applicable law, third parties must be contractually obligated to notify the Company promptly following an actual or reasonably suspected privacy or security breach, including the unauthorized access, use, disclosure, modification, or transfer of Personal Data. When appropriate, third parties must also be contractually obligated to cooperate with the Company in the event of an actual or reasonably suspected privacy or security breach.

6.2 Training of Company Personnel Regarding Policies

Company Personnel who access Personal Data will be regularly trained regarding their obligations under this Policy, the Company's Online Privacy Policy, and the appropriate collection, use, disclosure and safeguarding of Personal Data.

6.3 Training of Company Personnel Regarding Security Procedures for Personal Data

Company Personnel must be trained to take reasonable precautions to physically secure Personal Data. The Company will establish and maintain physical and environmental controls for each particular facility that employees should be aware of and follow, including, but not limited to:

- Restricted access to areas of offices and buildings containing Personal Data;
- Keyed areas;
- ID badges;
- Terminated employee procedures;
- Tamper-proof window and door locks;
- Security guards; and
- Visitor ID procedures.

7 Data Access

7.1 Review of Personal Data by Data Subjects

Personal Data must be available to Data Subjects for review and update by one of the following methods.

7.1.1 Indirect Review of Personal Data: Indirect methods include an email alias to which Data Subjects can submit requests to update their Personal Data or their preferences or a phone number that the Data Subject can call.

Example: The following language, appearing on a web page, is an example of an indirect method of access: "If you have submitted personal information to the Company via our web site and would now like to have that information updated, please send an email to [insert name of alias]@allegisgroup.com."

7.1.2 Direct Review of Personal Data: Direct methods include password-protected access to Databases for online updating by Data Subjects of their Personal Data.

Example: Registered applicants can review and update their personal data by accessing a self-service portal.

7.2 Requests for Access to Personal Data

Data Subjects may make a written request for access to their Personal Data that the Company holds for them in order to review its accuracy and completeness. Data Subjects have the right to have their Personal Data corrected, amended, or deleted as appropriate where it is inaccurate. The Company reserves the right to redact protected information in order to give Data Subjects access to their Personal Data. All access requests are subject to the relevant access and exceptions set forth in this Policy. Subject to applicable law, access may be denied or limited in certain circumstances, including the following:

- If the Data Subject does not supply sufficient information to allow the Company to confirm the identity of the individual making the request;
- When the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the situation in question;
- Where the legitimate rights of persons other than the Data Subject would be violated;
- When providing access would interfere with execution or enforcement of the law or private cause of action;
- When references to other Personal Data cannot be redacted;
- When a legal or other professional privilege or obligation would be breached;
- When the confidentiality of future or ongoing negotiations would be breached;
- When employee security investigations or proceedings would be prejudiced;

- When the confidentiality that may be necessary for limited periods in connection with employee succession planning and corporate reorganization would be prejudiced; and
- When the confidentiality that may be necessary in connection with monitoring, inspection, or regulatory functions connected with financial management would be prejudiced.

You should check with individual departments, for example, Human Resources, to determine if there is additional documentation that must be completed prior to releasing such Personal Data or providing the Data Subject with access.

8 Use of Cookies, Web Bugs, and Similar Technologies

8.1 Right to Refuse Cookies

Under the European Union's Directive on Privacy and Electronic Communications, users must be given the opportunity to refuse cookies. The Company's global policy is to conform to the principles of this Directive for all use of cookies and tracking technologies. The use of cookies to collect Personal Data must always be optional to an online visitor to the Company's web sites. Visitors must be able to enter and use the Company's web sites with their browsers set to refuse cookies. Those who refuse cookies, however, may not be able to take full advantage of the Company's web sites and, if this is the case, visitors should be made aware of that fact.

8.2 Use of Cookies or Web Bugs on Company Sites

When utilizing cookies or web bugs, also known as web beacons, on the Company's web sites, Company Personnel must ensure users are given clear and precise information (1) that cookies or web bugs are used to collect Personal Data; (2) in what instances cookies or web bugs will be used to collect Personal Data; (3) what information will be stored in a cookie or web bug, and, if applicable, (4) that cookies or web bugs are placed on the Company's web sites by third parties; and (5) a disclosure of any transfer of Personal Data collected by a Company cookie or web bug to third parties, including contractors and vendors. Any collection of Personal Data by third-party cookies or web bugs and any transfer to third parties of information collected by the Company's cookies and web bugs for purposes unrelated to the reason for which the Personal Data was initially collected require that Data Subjects Opt-in to such transfers. The Company will disclose all uses of tracking technology, whether cookies, web bugs, or similar technologies, in advance and explain to users how they may disable cookies, web bugs, or the similar technology being used via their browsers, including by implementing or otherwise accepting Do-Not-Track features of their browsers or other mechanisms.

8.3 Notice to Users Regarding Cookies or Web Bugs

Users should be directed to the Company's Online Privacy Policy or to wording similar to the following on web sites where cookies or web bugs are used to collect Personal Data:

> "A cookie is a small data file that certain web sites write to your hard drive when you visit them. A cookie file can contain information such as a user ID that the site uses to track the pages you have visited.
> A web bug is a graphic on a web page or email that gathers information about the computers that view the web page or email. A web bug can collect your IP address and the time you viewed the web site or email.
> Neither a cookie nor a web bug can read data from your hard disk or read cookie files created by other sites other than as described above. Some parts of the Company's web sites use cookies and web bugs to track user traffic patterns on the Company's site. The Company does this in order to determine the usefulness of our web site information to our users and to see how effective our navigational structure is in helping users reach that information.
>
> "If you prefer not to receive cookies or web bugs while browsing our web site, you can set your browser to warn you before accepting cookies or web bugs and refuse them when your browser alerts you to their presence.
>
> "You can also refuse all cookies and web bugs by turning them off in your browser, although you may not be able to take full advantage of the Company's web sites if you do so. You do not need to have cookies turned on to use/navigate through many parts of the Company's web site, except that access to certain of the Company's web pages require a login and password.

"You can find information on popular browsers and how to adjust your cookie preferences at the following web sites:

Microsoft Internet Explorer: http://www.microsoft.com/info/cookies.htm

Mozilla Firefox: http://www.mozilla.org/projects/security/pki/psm/help_21/using_priv_help.html

Google Chrome: https://support.google.com/accounts/answer/61416

Apple Safari: Blocks cookies by default and accepts cookies only from your current domain. To change, click Safari, Preferences, Security, and choose your preference."

9 Click-through Tracking

9.1 Collection of Non-Personal Data

Where possible, the Company will collect only non-Personal Data if click-through tracking is being used on a web site.

9.2 Collection of Personal Data

If Personal Data will be collected, click-through tracking or other forms of online tracking are not permitted unless:

9.2.1 Meaningful Disclosure: The Company provides Data Subjects with a meaningful disclosure about what tracking is being conducted, what information or Personal Data is being collected, how it is used, and how a Data Subject can Opt-out;

9.2.2 Method for Opt-Out: The Company provides Data Subjects with a clear and unambiguous method for Opt-out, including by implementing or otherwise accepting Do-Not-Track features of their web browsers or other mechanisms; and

9.2.3 Security and Storage of Personal Data: The information or Personal Data collected is secure and kept for no longer than necessary for the stated purpose.

9.3 Use of Personal Data for Different Purpose

Before the Company uses the information or Personal Data in a manner that is materially different from what was stated when the data was collected, where required by applicable law, it will obtain the affirmative express consent (Opt-in) from the Data Subject.

9.4 Collection of Sensitive Personal Data

Sensitive Personal Data must not be collected for use in marketing, unless the appropriate consent is obtained in jurisdictions where consent is allowed to be obtained.

10 Sale of Personal Data

It is against the Company's policy to sell or rent Personal Data that the Company maintains about Data Subjects, including but not limited to its employees, temporary workers, and their respective dependents and beneficiaries, prospective employees, customers, prospective customers, online visitors, and business partners.

11 Agreements with Vendors of Personal Data and Service Providers

11.1 Company Policy with Vendors

The Company's policy is to do business with companies that respect the privacy of Data Subjects. Vendors and business partners that handle or manage Personal Data for the Company or host web sites or applications for the Company must have appropriate Privacy Statements on their web sites and follow policies regarding the collection, use, disclosure, and management of Personal Data which are consistent with the Company's Policy.

The Company may transfer Personal Data to service providers located outside your country of residence, including the United States, Canada, the EU and India. For additional information about the manner in which service providers treat your Personal Data, contact us as set out below.

11.2 Procurement of Personal Data from Vendors

It is essential that vendors who are selling or passing on Personal Data have the right to do so for the purposes for which the Company needs it. To ensure this, appropriate agreements must be signed. No list may be purchased or rented for use by the Company unless the vendor represents and warrants in writing that the Personal Data was collected in a manner that conforms to applicable law and which permits the use for which the Personal Data is procured.

11.3 Recordkeeping Requirement for Procurement of Personal Data

Any Company Personnel receiving Personal Data from a third party must maintain adequate records of lists rented / purchased so as to be able to identify the source of the Personal Data.

12 Persons Under the Age of 18 and 13

12.1 Persons under the age of 18

The Company's policy is not to collect Personal Data from individuals under the age of 18 without the consent of their parents.

12.2 Persons under the age of 13

The Company's policy is not to collect Personal Data from children under the age of 13 (minor children). Any deviation from this Policy requires approval from the Legal Department.

13 Email Marketing

13.1 Email Marketing Guidelines

Subject to applicable law, the Company will only engage in email marketing that satisfies the following criteria:

13.1.1 Truthful Information: All information regarding the point of origin, the transmission path, and the return path must be truthful; i.e., the reply path of the email must return to the Company when the recipient sends a "reply to" email.

13.1.2 Consent by Recipient: No email may be sent to a recipient who has not consented to receive the email as required by applicable law or who has unsubscribed after an initial Opt-in to receive emails from the Company.

13.1.3 Adherence to Opt-Out: No email may be sent to an individual who has made an Opt-out by placing his/her name on a do-not-email list.

13.1.4 Unsubscribe Information: All email sent by the Company to recipients on a mailing list must contain instructions (in a type size at least as large as the text of the email) on how to unsubscribe to receiving future marketing email. Unsubscribe requests must be honored within ten (10) business days.

13.1.5 E-mail Addresses in Database: Email addresses cannot be entered into a Database unless the Data Subjects have made an Opt-in to receiving email from the Company.

13.1.6 Entity Information: Emails should include the Company entity's name, physical mailing address, and either a toll-free telephone number or an email address for use by individuals who wish to Opt-out of receiving future emails.

14 Data Retention and Cleaning

14.1 Compliance with Laws and Policy

The Company will retain Personal Data as long as required by law or regulation and in accordance with its Record Retention Policy. A customer of the Company may also require that the Company keep or destroy Personal Data in accordance with the customer's data retention policy. Personal Data will be retained and disposed of in a secure manner in accordance with the Company's Record Retention Policy.

14.2 Retention of Personal Data

Personal Data must be retained only for the amount of time necessary for the Permitted Uses and must be kept up to date. Inactive information should not be kept for longer than required by applicable law or business necessity and should be kept in accordance with the Company's Record Retention Policy.

14.3 Updates to Personal Data

It is up to each Database Owner to ensure the accuracy of Personal Data and Opt-in/Opt-out preferences.

15 Complaints / Dispute Resolution

15.1 Reporting of Issues and Breaches

The Company takes its obligations regarding privacy and data protection seriously. Issues raised by employees, temporary workers, and their respective dependants and beneficiaries, prospective employees, customers, prospective customers, business partners, and online visitors regarding the Company's online or offline use, collection, retention, and/or disclosure of Personal Data should be sent to privacyofficer@allegisgroup.com. Customers may also submit a complaint regarding non-compliance with this policy to privacyofficer@allegisgroup.com.

A Data Subject, including Company Personnel, may report any suspected breach of this Privacy Policy or that an individual is not adhering to the provisions of this Policy. The Data Subject may contact the company hotline at +1 866 377 7489. If you are an employee or temporary worker of the Company, you may also contact the Human Resources representative at your office location.

The Company will investigate any reports of issues or breaches it receives in a timely manner.

15.2 Independent Recourse Mechanism

If, in the opinion of an EU or Swiss Data Subject, the Company does not respond satisfactorily to a report or complaint relating to the transfer of Personal Data from the EU or Switzerland to the United States, the Company has established an independent recourse mechanism through the BBB EU Safe Harbor to investigate such a report or complaint. EU and Swiss Data Subjects may file a complaint with the BBB EU Safe Harbor at http://www.bbb.org/us/european-union-dispute-resolution/.

16 Enforcement

Any Company Personnel found to have violated this Policy may be subject to disciplinary action, up to and including termination of employment or contract, with or without prior notice or warning. In addition, the Company reserves the right to pursue any remedies available, whether civil or criminal and whether at law or in equity, for violations of this Policy. Nothing in this Policy alters the at-will nature of employment relating to Company employees in jurisdictions where at-will employment applies. Company Personnel must immediately report violations of this Policy to their department heads and to the Information Security Officer. The Company does not consider conduct in violation of this Policy to be within the course and scope of employment or the direct consequence of the discharge of one's duties. Accordingly, to the extent permitted by law, the Company reserves the right not to provide a defense or pay damages assessed against a Company Personnel for conduct in violation of this Policy. Individuals who report violations of this Policy in good faith or are involved in the investigation of violations of this Policy will not be subject to reprisal or retaliation, solely as a consequence of such reporting or involvement. Retaliation is a very serious violation of this Policy and should be reported immediately.

To the extent any portion of this Policy is inconsistent with any federal, provincial, state, or local law or regulation, such portion will be modified to the extent necessary to comply with such federal, provincial, state or local law or regulation, and the remaining portions of the Policy will remain unaffected.

17 Definitions

Term	Definition
"Company"	Allegis Group, Inc. and its subsidiaries.
"Company Personnel," "You" or "you"	Any employee or temporary worker of the Company and any authorized representatives, contractors, or agents of the Company.
"Data Subject"	Any person in any part of the world about whom Personal Data is collected or retained.
"Database"	Any system (whether electronic or manual) that allows one to collect, record, organize, access, modify, and/or retrieve information. This includes exploitable formats such as paper files as well as electronic spreadsheets, email group listings, and other similar digital information as well as information contained in electronic devices such as personal digital assistants, personal computers, servers, and smart phones.
"Database Owner"	The person responsible for managing and administering a Database.
"Information Security Program"	This Policy, together with the policies listed in the Related Policies section of this Policy.
"Online Privacy Policy"	The web site Privacy Statement posted on the Company's web sites.
"Opt-in"	One of the two methods used to obtain consent from a Data Subject to collect, use and share or process Personal Data (see "Opt-out"). To obtain a valid Opt-in, the Data Subject must give his or her affirmative consent; for example, by checking the "Yes" checkbox on a data collection form. The consent is only valid to the extent and for the purpose given at the time. If subsequently a different use of the Personal Data is intended, it will be necessary to obtain a new consent. Further, Opt-in consent must be specific as to the proposed form of communication from the Company; for example, direct mail and telephone.
"Opt-out"	One of the two methods used to obtain consent from a Data Subject to collect, use and share or process Personal Data (see "Opt-in"). It is called "Opt-out" because the Data Subject's consent is implied unless the Data Subject does something affirmative to remove the consent; for example, by un-checking the "Yes" checkbox on a data collection form.
"Permitted Use"	The permitted uses set forth in Section 5 of this Policy.

Term	Definition
"Personal Data"	Any information relating to an identified or identifiable natural person ("Data Subject"). 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/her physical, physiological, mental, economic, cultural, or social identity. Personal Data includes an individual's name, email address, work or home telephone number, home postal or other physical address, birth date, driver's license number or other municipality-issued identification card number, Social Security number or other national identification number, financial account, credit card or debit card number, geolocation data, or other information that may enable identification of a person or individual. What constitutes Personal Data varies by region and country. In the European Union, for example, an individual's Internet Protocol (IP) address can be considered personal information (depending on how it is used), and in India, passwords are considered personal information.
"Policy"	Privacy and Personal Data Protection Policy
"Sensitive Data"	Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life or as otherwise defined by applicable law.

18 Related Policies

- Allegis Group's Online Privacy Policy located at http://www.allegisgroup.com/Privacy/.
- Allegis Group's Acceptable Encryption Policy
- Allegis Group's Information Security Policy
- Allegis Group's Information Classification Policy
- Allegis Group's Electronic Resources Policy
- Allegis Group's Social Media Policy
- Allegis Group's Records Retention Policy

19 Revision History

Date of Change	Summary of Change
November 1, 2011	Version 2
January 1, 2013	Version 3
January 1, 2014	Version 4
January 1, 2015	Version 5