



Allegis Group's General Data Protection Regulation Readiness

Our Commitment to the General Data Protection Regulation

General Data Protection Regulation (GDPR) compliance and respect for the privacy rights of individuals who entrust personal data to us is a top priority for Allegis Group, Inc. and its affiliated entities (“Allegis Group”). We have a dedicated global privacy program and are underway in our efforts to prepare for the European Union’s (EU) GDPR.

What is the GDPR?

The GDPR (General Data Protection Regulation) is a new EU Regulation which will replace the 1995 EU Data Protection Directive when it goes into effect on the 25th of May 2018. The GDPR was passed in 2016, and companies have been working since its passage to be prepared for the significant enhancements to the protection of the personal data of EEA residents (EEA or European Economic Area means the EU plus Iceland, Lichtenstein and Norway and, for data purposes only, Switzerland. In due course it will apply to the UK post Brexit). GDPR increases the obligations on organizations who collect or process personal data. While much attention has been paid to the strict penalties that accompany its passage (4% of worldwide global turnover for certain violations), it’s clear that it is achieving its true intended goal since companies caught in its broad wake are appropriately scrutinizing their personal data handling practices.

The GDPR applies to all companies located in the EEA, but its broad scope also applies to companies, regardless of their location, who are selling goods and/or services to individuals in the EEA or monitoring their behavior.

[The full text of the GDPR can be found here.](#)

Allegis Group's GDPR Readiness Effort

At Allegis Group, we are committed to ensuring the responsible and secure collection, use and sharing of personal data. We are diligently working to develop systems and processes to achieve compliance with the GDPR with our Global Privacy Office at the helm.

About the Allegis Global Privacy Office

The Global Privacy Office’s mission is to support Allegis Group’s commitment to the appropriate collection, use and sharing of personal data. The Global Privacy Office has key leaders in the United States, EMEA and APAC that coordinate with our Global Privacy Officer. Additionally, each of our brands has a dedicated Privacy Analyst that assists with the implementation of the GDPR readiness strategy in partnership with the Global Privacy Office. Each member of the team brings their subject matter expertise, including numerous IAPP certifications, and deep knowledge of their respective businesses. Additionally, Allegis Group has a centralized Global Data Protection Oversight Committee comprised of the most senior leaders within Information Services (IS), Information Security and Privacy to oversee the company’s global privacy initiatives.

Allegis Group has also appointed an external Data Protection Officer (“DPO”) to act as our official DPO under GDPR and to provide additional expertise and support to the commitment of the Global Privacy Office. Our DPO is Lillian Pang.

Lillian Pang is an IAPP member and designated as a Fellow of Information Privacy (FIP). Lillian is also CIPP-E and CIPT certified. Lillian has worked in the data privacy field for over 10 years and most recently worked for a global technology company as Vice President and Group Chief Privacy Officer. Lillian also has in-house counsel experience with the staffing industry and therefore has a strong understanding of our industry and our services. Lillian is based in London.

Allegis Group is also proud to be an [IAPP Gold Sponsor](#).

Allegis Group’s GDPR Readiness Program

The Global Privacy Office is actively developing and implementing on its initiatives to make sure Allegis Group is compliant with the GDPR and other applicable privacy legislation around the world. Allegis Group’s Global Privacy Office is approaching GDPR Readiness through its commitment to its “Top 10 GDPR Initiatives,” which include:

1	Understanding Our Data – Data Mapping and Justifications for Processing	<ul style="list-style-type: none">• Completion of data mapping exercises• Completion of our Article 30 records of processing activities
2	Privacy Notices	<ul style="list-style-type: none">• Updating all privacy notices
3	Data Breach Reporting	<ul style="list-style-type: none">• Ensuring our security incident response process is prepared to respond under the GDPR deadlines
4	Contracts – Customers and Suppliers	<ul style="list-style-type: none">• Implementing GDPR compliant provisions in our contracts with our customers and suppliers• Conducting due diligence on our suppliers through questionnaires and where appropriate, onsite or other forms of audit
5	Data Subject Rights	<ul style="list-style-type: none">• Implementing a repeatable, scalable process and set of procedures for handling data subject rights requests

6	Training and Awareness and Appointment of Data Protection Officer	<ul style="list-style-type: none"> • Appointment of Lillian Pang as Data Protection Officer • Online and in-person trainings across the business to promote privacy awareness and teach key privacy principles
7	Data Transfers	<ul style="list-style-type: none"> • Ensuring we are maintaining viable means for transferring personal data, including maintaining Privacy Shield certification and a Global Intercompany Data Transfer Agreement and executing model clauses where needed
8	Privacy in Day-to-Day Operations/Privacy by Design and DPIA	<ul style="list-style-type: none"> • Undertaking Data Privacy Impact Assessments (DPIAs) where appropriate across the business • Partnering with IS for Privacy by Design • Educating areas of the business (e.g., HR, Marketing, Procurement) on the meaning for their function of privacy in day-to-day operations
9	Information Security	<ul style="list-style-type: none"> • Partnering closely with our Information Security team to implement appropriate technical and organizational measures to protect personal data, including looking for opportunities to enhance the use of pseudonymization and encryption
10	Data Minimization	<ul style="list-style-type: none"> • Ensuring that Allegis Group keeps only data that is necessary for its legitimate business interests

Our Services – When We Act as a Controller and/or Processor

Understanding the role that you play as either a Controller or Processor is an important component of the GDPR. Controllers and Processors have different responsibilities under the GDPR, but both are directly subject to liability from the regulators under GDPR.

Controller: Determines the means and purposes of the processing of Personal Data (the “how” and the “why”)

Processor: Processes Personal Data on behalf of the Controller

Allegis Group has conducted an analysis to identify the role it plays for each of our service offerings as explained in the chart below:

	Staffing	Search	Consulting	MSP	RPO
Processor?	Yes	Maybe	Yes	Yes	Yes
What is the Personal Data?	Customer Personal Data – varies (depends on what Customer provides to our Contract Workers)	Candidate Data – if Customer supplies it (e.g., an internal candidate at the Customer)	Customer Personal Data – varies (depends what Customer provides to our Consultants)	Customer Personal Data – Staffing Supplier Contract Workers (to provide short-listing/evaluations, consolidated invoicing, analytics)	Customer Personal Data – Candidate data Customer provides to Allegis Group or directs Allegis Group to source on its behalf

Controller?	Yes	Yes	No	No	Yes
What is the Personal Data?	Contract Worker Data	Candidate Data			Candidate Data – sourced by Allegis Group (not at direction of Customer)

For more information about the concepts of Controller and Processor, please see the Article 29 Working Party [Opinion 1/2010 on the concepts of “controller” and “processor.”](#) For each of our service offerings, we have developed Data Protection language that is compliant with GDPR that we have ready for use with any customer engagement.

Transferring EEA Personal Data

Allegis Group is committed to responsibly and lawfully transferring personal data of our clients while performing our services that involve data subjects from the EEA. In order to do this, Allegis Group has the following mechanisms in place:

- We are EU-US and Swiss-US Privacy Shield certified and have been since the inception of the Privacy Shield Framework. Please see our certification [here](#).
- We have an intragroup data transfer agreement using the EU Controller to Controller Model Clauses that also includes the appropriate provisions required under GDPR to cover personal data transfers between and among our businesses globally. While we generally rely on our Privacy Shield certification for transfers from the EEA to the US, the intragroup data transfer agreement provides a second method of transferring that same data while also providing us with a mechanism to allow us to transfer data from the EEA to our companies outside of the US (for instance to our entities located in APAC).
- We make use of the Model Contract Clauses as appropriate with our business partners.
- We ensure an adequate transfer mechanism is in place when our suppliers are processing personal data outside of the EEA.