Allocadia

TRUST AT ALLOCADIA

Product Security Overview

Allocadia has a robust and comprehensive privacy and data protection program. We provide all the necessary resources and information to help our customers validate their privacy and compliance requirements, and to show how Allocadia meets these requirements.

Our Privacy and Compliance team governs the privacy and data protection program and ensures its effectiveness. This team is led by Allocadia's data protection officer and General Counsel, and operationalized by the CISO.

The team handles:

- Creating, updating and maintaining our data privacy policies and procedures, which protect the data handled by Allocadia employees and partners
- Making sure that Allocadia meets the data privacy commitments it has made to customers, partners, investors and employees
- Handling third-party audits of our privacy policies, and ensuring that we remain in compliance with those policies
- Providing data privacy and compliance training for employees

Data Privacy

When considering Allocadia's data privacy commitments, it is important to note that the Allocadia application is a business tool for marketing teams, and that:

- The Allocadia application is not a data source for financial reporting purposes.
- Although the Allocadia application can import financial data from finance systems, it only uses such data to help the marketing team become more efficient in their planning and decision making. There are no secondary uses for this data.
- This data import function of the Allocadia application is not a two-way sync, nor is it a direct API connection to finance systems. The Allocadia application merely imports data from a flat file, which itself is exported by finance systems under controls operated by the customer's systems administrator.
- The Allocadia application does not and cannot manipulate financial data stored in a customer's financial system of record.
- The Allocadia application only processes a limited and predefined set of data assets as defined in the applicable data processing agreement. Such processing does not and will not include any data assets of any other third parties.

EU Data Privacy Requirements

Allocadia fully complies with all relevant data privacy requirements under EU General Data Protection Regulation (GDPR) regulations.

Specifically, we:

- Meet all requirements under GDPR Chapter 3 (Rights of the Data Subject).
- Have a fully compliant data processing agreement, standard contractual clauses, and appendices A, B, and C to the clauses.
- Process privacy-impacted assets only in covered jurisdictions.
- Have appointed a data protection officer and data privacy operations director.
- Conduct employee training on compliant security and privacy procedures.
- Publish Privacy Policies and Notices to inform customers of Allocadia's compliance capacities and posture.
- Provide configurable privacy and compliance features to our customers.
- Carry out Privacy Impact Assessments.
- Assure adequate data asset transfer methods for our customers.
- Maintain records of data processing activities.
- Assure that data processing agreement requirements with sub-processors are met.

Data Transparency

Allocadia provides transparency into the geographical regions where our customers' data assets are stored and processed. The customer has its choice of processing jurisdictions to ensure compliance with relevant regulations. Allocadia, its customers, and its supply chain comply with applicable international data privacy regulations. Common privacy principles throughout jurisdictions include notice, choice, access, use, disclosure, and security. Our application is designed to only allow processing according to the customers privacy criteria, so organizations can meet the requirements of their country's specific privacy laws.

Data Jurisdiction

Customers retain control over which privacy jurisdiction their data assets are processed and stored in. Data processing jurisdictional requirements are detailed in the Data Processing Agreement.

Allocadia operates two separate data processing environments in two separate processing jurisdictions: Northern California (with a backup processing site in Virginia) and Ireland (with backup processing site in Frankfurt, Germany). When a customer organization is first set up in the Allocadia application, we assign them to the processing jurisdiction of their choice (either EU or US). Once selected, all processing for that organization will occur within that jurisdiction.

Allocadia minimizes both the collection and use of personally identifiable data assets. For each user, our application only requires a business email address, and a first name and last name for identification/authentication purposes. These data assets are only used to authenticate and communicate with the user. There are no secondary or downstream uses of these personally identifiable data assets.

The table below shows which data assets the Allocadia application requires, how the data is processed and stored, who has access to it, and whether it travels across jurisdictions:

Data Asset	Pupose	Security Comments
User's business email address (mandatory)	**Used by the application:** • as the 'username' for the User. • to communicate with the user for application. events (password change prompt, 'report is ready' email notification). **Used by Allocadia Customer Success & Support:** • to contact users for ongoing application support aligned to the written processing instructions provided by Users' organization. • no usage of this Data Asset by any other function.	This asset is encrypted in transport (TLS 1.2) and at-rest (AES 256). This data asset is only used to authenticate and support the user directly. There are no secondary uses for this data asset. This asset does not travel across processing jurisdictions.
User's first and last names (mandatory)	**Used by the application:** • to personalize the User experience. **Used by Allocadia Customer Success & Support:** • to personalize the Customer Success and Support experience. • no usage of this Data Asset by any other function.	These assets are encrypted in transport (TLS 1.2) and at-rest (AES 256). These data assets are used to personalize the user experience. Such assets are only processed in systems under Allocadia's administrative control according to the written processing instructions. There are no secondary uses for this data asset. This asset does not travel across processing jurisdictions.
User's job title / role (optional)	**Used by the application:** • to personalize the User experience. **Used by Allocadia Customer Success & Support:** • no usage of this Data Asset by the Success & Support teams. • no usage of this Data Asset by any other function.	This asset is encrypted in transport (TLS 1.2) and at-rest (AES 256). This data asset is used to personalize the user experience. Such assets are only processed in systems under Allocadia's administrative control according to the written processing instructions. There are no secondary uses for this data asset. This asset does not travel across processing jurisdictions.

Allocadia
Marketing Performance Management

EMAIL: hello@allocadia.com
TEL: 1-866-684-0935
WEB: www.allocadia.com