ALIGN | Frequently Asked Questions

CLOUD-BASED COMPUTING

Q: Is all of Align technology and data in the internet cloud?

A: Yes. Align is built into the Microsoft Azure computing cloud which provides the highest level of security, encryption and data access worldwide.

Q: Our Company has a policy that does not allow cloud computing because of concerns around privacy, security-related issues and because cloud-based systems are constantly vulnerable to attack. How have you addressed these concerns?

A: Any technology, including on premise enterprise technology, that can be accessed from outside a company can be attacked. We chose *not* to build Align for enterprise deployment because of security concerns. In order to guarantee security, confidentiality and privacy we would have had to require that companies build and enforce security, build data privacy, conduct quarterly penetration audits and *monitor and fix security threats all day, 365 days a year*. Building Align into the Azure cloud resolves these issues. John Schlesinger, the Chief Enterprise Architect of Temenos, a leading supplier of bank technology summarizes the security benefit of Microsoft Azure: "From a security point of view, I think Azure is a demonstrably more secure environment than most banks' datacenters."

Q: In which geographic location(s) is Azure hosted?

A: United States – West.

Q: How does Azure provide this level of security and data privacy protection?

A: The following answers are provided by Microsoft Azure's white paper:

Physical security. Azure runs in geographically distributed Microsoft facilities. Each facility is designed to run 24x7x365 and employs various measures to help protect operations from power failure, physical intrusion, and network outages. These datacenters comply with industry standards (such as ISO 27001) for physical security and availability. They are managed, monitored, and administered by Microsoft operations personnel.

Network isolation. Azure is a multitenant service, meaning that multiple customers' deployments are stored on the same physical hardware. Azure uses logical isolation to segregate each customer's data from that of others. This provides the scale and economic benefits of multitenant services while rigorously preventing customers from accessing one another's data.

Monitoring and logging. Centralized monitoring, correlation, and analysis systems manage the large amount of information generated by devices within the Azure environment, providing continuous visibility and timely alerts to the teams that manage the service. Additional monitoring, logging, and reporting capabilities provide visibility to customers.

Encrypting communications. Built-in cryptographic technology enables customers to encrypt communications within and between deployments, between Azure regions, and from Azure to on-premises data centers.

Update management. Security update management helps protect systems from known vulnerabilities. Azure uses integrated deployment systems to manage the distribution and installation of security updates for Microsoft software. Azure uses a combination of Microsoft and third-party scanning tools to run OS, web application, and database scans of the Azure environment.

Antivirus and antimalware. Azure software components must go through a virus scan prior to deployment. Code is not moved to production without a clean and successful virus scan.

Penetration testing. Microsoft conducts regular penetration testing to improve Azure security controls and processes. Microsoft understands that security assessment is also an important part of our customers' application development and deployment. Therefore, Microsoft has established a policy for customers to carry out authorized penetration testing on their own—and only their own—applications hosted in Azure.

DDoS Protection. Azure has a defense system against Distributed Denial-of-Service (DDoS) attacks on Azure platform services. It uses standard detection and mitigation techniques. Azure's DDoS defense system is designed to withstand attacks generated from outside and inside the platform.

Q: What additional layers of security and data protection does Align build into its technology?

A: Align has engineered multiple processes and technologies into the application:

Adheres to Azure's best practices. Align rigorously follows and enforces all of Azures best security practices.

Partitioned Clients: Each organization is securely sectioned with its own encryption and unique URL.

Partitioned Matters: Matter partitioning builds another secure layer ensuring that users cannot see other's data.

Penetration audit, security certification. The industry standard is an annual security audit. Align conducts security and penetration tests quarterly, obtaining security certifications at the completion of each test. The assessment methodology includes structured review processes based on recognized "best-in-class" practices as defined by methodologies such as the ISECOM's Open Source Security Testing methodology Manual (OSSTMM) [1], Open Web Application Security Project (OWASP) [2], U.S. National Security Agency (NSA) [3] and ISO 27001 [4] Information Security Standard.

User Access. User access is the most vulnerable component of security. Align rigorously manages and monitors user access:

- **User identification and password control:** Password control is multi-layered staging user through challenges ensuring that the right person gains access to the right matter.
- **Rights:** Users are assigned rights limiting access to matters, modules and data.
- **Lock out:** Users are locked out of matters when they depart their organizations.

Encryption: Align's multipronged encryption delivers the highest level of data privacy securing data flows and access between matters and customers:

- Each company's matters and data are uniquely encrypted. Every team works on a client's matter via the client's encryption key.
- Documents are encrypted at rest.

- People data is encrypted in XML fields.
- Backup data is encrypted in storage

No client caching. All Align data is actioned and stored in the cloud. No data or actions are cached on the client, removing the potential of malicious access from viruses on user's computers.

Confidentiality. Align provides customers granular control of matters to enforce confidentiality:

- **Restricted Matters:** Matters can be restricted on set up. Restricted matters are not visible to or searchable by others in the organization. Only the individuals on each approved team know about and can access the matters.
- **Restricted Views:** Companies control rights to see and manage data on each matter page (e.g., matter strategy, budget, scope change etc.)
- **Restricted access and security of documents in data rooms:** Searching, visibility and access to documents on matter data rooms are controlled matter-by-matter by the company.
- **Attorney-Client Privilege:** Rigidly enforced and managed by client organization, rights to privileged information and domain access.

Q: Is Align ISO standard certified?

A: Align's ISO standards are certified via Azure. ISO/IEC 27018 protects personal privacy and data stored in the cloud. Azure is also certified to ISO 27001, FedRAMP, SOC 1 and SOC 2.

Q: Why is Align Cloud based? What's the value of it to our company and legal department?

A: Align is a single platform for the planning and management of matters. Every team working on your matter uses Align – all users use the same application and the same data. The benefit to your legal department is that you have real time management and access to the work of all team members wherever they are. The automation built into Align delivers detailed data to you in real-time. All of your teams access Align and work on the matter in your own secure, private and encrypted Azure cloud. The alternative is for each of your outside teams and law firms to work on matters and supply reports which you manually key into on-premise technology. The complete inability to share data requires legal departments to require lawyers or to hire teams to manage these data. The source of law firm data is billing invoices. Legal departments receive invoices 45 – 90 days after events and then require additional time for their lawyers or support teams to key in data. The resulting information not only comes in too late, but it is subject to human error resulting in poor quality and unreliable data. Research by Thomson Reuters surfaced the fact that far the majority of these systems quickly become underutilized.

Q: Our Company has offices and sells our products to multiple countries around the world. We work with our own teams in those countries and we hire law firms and other vendors who work on our matters in those countries. Does Align support matters and users in other countries?

A: Yes. By design, Align is a multi-country and multi-lingual application and our Azure cloud provides worldwide access and support.

Q: Our Company is dependent on real time access to our information and data. We need 24X7 confirmation that new information instantly updates our data systems and is available to all of our users. What uptime guarantees does Align promise? How does Align manage and ensure business continuity?

A: Align delivers these assurances through Azure. Azure provides the highest level uptime SLA. Azure integrates business continuity by replicating data and immediately making it available through alternate Azure resources.

Q: Our technology department is responsible for all of our company's technology. They may not have the budget, time or personnel to take on another major system.

A: Unlike other legal technologies, you do not purchase a six-figure enterprise application that requires additional costs for supporting technology. You purchase Align for matters and grow it as you need it. You can start using Align for a single matter at $100 per month and because Align is in the Microsoft Azure cloud you will require minimal technical support.

Q: Our Company pays considerable annual costs for the storage and security of electronic Company data. What additional costs and resources are required to store and secure Align data?

A: Align data is managed and stored in Azure. Your technology department is not required to manage, store or pay for these data. Align incrementally charges for data flow and storage. Your first 16 GB of data flow and storage is free. As you increase data and storage requirements, Align charges $750 per year for each additional 16 GB.

Q: What technology do we need to support or interface with Align in the cloud?

A: The only technology your company needs is current version browsers. Align supports Chrome, Safari, Internet Explorer, Firefox and Opera. Align also supports Apple and Android tablets and smartphones. Your company **does not** require **any other** technology.

Q: What teams, skills and expertise do we need to hire to support and manage Align?

A: You need a *part-time* Align Administrator who will spend 2 – 4 hours a month managing users and your company's business requirements relative to Align. This individual **does not** require **any** technical skills. Likely candidates for this role are a mid-level manager in finance or HR.

Q: What data does Align use from our internal systems and/or what data does Align send to our internal systems?

A: This is your choice. Align can be a self-standing application that does not gather or send data to any of your technologies. Or you can choose to send limited data from internal systems to or accept limited data from Align. Align limits the data it will accept from your systems. For example your company may send information about employees to Align. However, Align will not accept any personal data that can be compromised or misused, such as social security numbers or personal information contrary to privacy laws across countries.