SyncSign

sync-sign.com | +1 (626) 269-9019

Data Protection

SyncSign take your privacy very seriously and adopt appropriate security measures to protect against unauthorized access, disclosure, alteration, or destruction of data.

Data center

SyncSign Cloud runs on AWS, with high-level data center hosting. For more compliance information, please visit AWS Security and AWS Compliance.

Data residency

All application servers are located in the United States, but can be accessed internationally via the Internet. The communication between the SyncSign devices (Hub, Node), the SyncSign Applications and the online calendar is managed through Google/Microsoft's official standard calendar API and authentication, authorized access rights and storing certain credentials in encrypted form for certain calendars.

At the same time, no calendar or event information is stored on SycnSign servers. The servers only store emails of room resources, and all other information is obtained through API calls, parsed, and sent directly to the devices. This information is temporarily stored in our cache, just to ensure that the events will still be displayed even if the calendar service is down.

Decommissioning and data removal

All user data is stored on the AWS, which follows the strict deactivation policy outlined on page 8 of its security white paper:

"AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process."

Uptime and reliability

We constantly monitor our service performance and have automatic notifications to ensure rapid response for service interruptions. All code is audited and approved by engineers before deploying to production servers. We also monitor updates from the security community and immediately update our systems when vulnerabilities are discovered.