GPS LLC
GOUCHER PARKER SPIVEY

Security & Compliance

About GPSVirtual

GPSVirtual is a platform designed to securely capture remote and same-room audio/video testimony while simultaneously streaming the encrypted video to the cloud. Our platform is designed to enable users to gather testimony and conduct matters remotely, capturing higher-quality video testimony and reducing direct costs. The GPSVirtual platform places security first, which is why we use top web service providers to ensure reliability, access, and secure storage of your client's data. In this data security and privacy document, our team has compiled the steps taken to provide high-level compliance and our use of security best practices.

Security

WEB APPLICATION

- GPSVirtual platform web traffic is encrypted to meet or exceed current security standards
  - GPSVirtual uses TLS 1.2 with 256-bit keys to provide secure access to your account
  - All account webpages are secured with HTTPS

FILE STORAGE

- All testimony files including exhibits, audio/video files, and transcripts are stored on secure Amazon AWS S3 servers
  - This data can only be downloaded by users who are authenticated through the GPSVirtual site and invited by the testimony organizer
  - Appropriate permissions to access the videos for individual depositions are in place for each account
  - Standalone storage options are available
- Client data and exhibit metadata are stored on a Postgre SQL database that resides on AWS
- For files at rest, encryption is available at additional cost

DATA RETENTION

- Retention period equals two years, following the completion of the deposition.
  - Custom retention periods matching client's data retention policies are available.
  - For file removal redaction and deletion, contact our support team at gpsvirtual@gps.llc

GPS LLC
GOUCHER PARKER SPIVEY

Security & Compliance

STREAMING VIDEO

- All media traffic is 128-bit AES encrypted end to end
  - Recording is only decoded internally for conversion to .mp4 file type
- Port 443 Traffic
  - Media traffic may not be TLS encrypted if forced to use TCP instead of UDP
    - All traffic has additional 128-bit AES encrypted even if TLS encryption is unavailable
    - Redundant encryption ensures no man-in-the-middle attacks can occur
- UDP Port 3478 Traffic
  - UDP Port 3478 only accepts inbound traffic after an outbound request is sent
  - Connection is bidirectional and is always initiated from the corporate network/client

Support Services

Support services available at gpsvirtual@gps.llc

From pre-testimony setup to post-testimony questions, our support staff can help you with:

- Remote testimony frequently asked questions
- Computer setup and requirements
- Conference room setup and testing
- Security and firewall questions
- First time user walkthroughs
- Post-testimony questions

Compliance

AWS servers are deployed, security features include:

- Blocking unauthorized users from accessing data
- Supports server-side and client-side encryption
- Enables cloud-related regulatory compliance
  - AWS services are HIPAA eligible
  - AWS is certified under the EU-US Privacy Shield
  - Complete SOC 1 and SOC 2 reporting and certification

AWS SOC REPORTING

SOC 1 and SOC 2 certified AWS S3 storage file security

- Most recent SOC report from Amazon AWS: https://d1.awsstatic.com/whitepapers/compliance/AWS_SOC3.pdf

Note: AWS requests that a Nondisclosure Agreement (NDA) must be in place with AWS directly before these reports will be sent to any client.