Security Whitepaper

Common links from this page

Customers Terms of Service

Users Terms of Service

Privacy Policy

Data Protection

Cookie Notice

Types of Users

Access Control Policy

Security-related Policies

GDPR at Remo, Roadmap, DPA for US, European, & other international clients

What Security Standards does Remo Adhere to?

Gear Test with Firewall Compatibility

Data Remo Collects about Users

How Remo Processes Sensitive Information

Security & Accessibility

Security is oxygen to any modern business. As Remo humanizes the online social interactions and helps create meaningful connections, security is built into the very core of our company. Even as a startup, we breathe security starting with utmost privacy of critical human information amidst the modern technology - without spoiling the human experience and collaboration. We take pride as we go all-out in protecting sensitive business and critical personal information of all our clients and partners who entrust to us their online conferences, web gatherings, and virtual human events experience.

This document intends to answer the usual questions on how Remo ensures data privacy, security awareness, how we collect and handle data, IT and Security compliance, and the high-level information and related resources overarching security within Remo.

Privacy and Security

As organizations and clients streamline their businesses, protecting everyone’s privacy is always at the core of Remo’s security. Our web application uses secure video, audio, and chat to allow people to interact naturally in real-time, from anywhere in the world. We have different types of users for those who securely create an account with Remo and enjoy distinct access to secured levels of features and perks in return. We can also implement SAML SSO as an add-on and other related options for your organization, just kindly email your request to sales@remo.co for evaluation and assistance. As we expand and provide more meaningful connections to our ever-growing list of clients and partners, Remo is ever diligent and will always be vigilant to all applicable aspects of privacy and security. We have a comprehensive Privacy Policy hand-in-hand with our Data Protection and other security-related policies. At the very start of your journey with us, you will clearly experience Remo’s permission-based approach in data privacy and security. You basically provide data inside our web application only when it is with your consent and permission. As for any content during the event, Remo do not intercept or record it unless you as the host actually record it. Our data privacy and security commitment is further strengthened with GDPR in all our Data Processing Agreements (DPAs) for US, European, and other international clients for mutual consideration of obligations. Whenever you have clarifications prior to entering an agreement or sharing any information with Remo, our support teams are available.

Secure real-time human interactions

Making the online interactions transformed into a humanized experience is our noble goal in Remo. With the accessible technology, we protect your connected experience end-to-end with your data and your privacy secured real-time. Everything in our events is focused with your vital interest and with your consent. Remo adheres to a data minimization principle. Remo strives to limit the scope of information used, requested, and processed to the minimum. A speaker or guest only needs to indicate the name & email address to get access to the platform. Guests can also register using only their names or nicknames without surnames. The Host (Account Owner) is responsible for all the content produced and reproduced during the event and Remo does not monitor events actively and can't be held responsible for what happens in the events as explained in our Customers Terms of Service and Users Terms of Service. Furthermore, using an alias and made up emails is possible. We only need information about the account owner (individual or corporation). Remo’s secured platform has the ability to make your event as private as you want and with the right participants that you want by allowing you or the event owner to expel and ban users from your event real-time. All these perks of privacy and security, the responsibilities, and the things that govern your access to and use of Remo are found in our Customers Terms of Service and Users Terms of Service along with our Privacy Policy and Cookie Notice. We further protect you and secure your online experience with how Remo processes sensitive information and our Data Protection. You can rest assured that your interactions and human connections are safe with Remo and our platform. All you have to focus is growing your network, enjoying your events while making meaningful human connections.

Security Awareness

We at Remo give additional focus and extra care to the security of the sensitive data and all information entrusted to us. We constantly take all reasonable steps to safeguard and only process personal information relevant to the purpose for which it needs to be collected with user consent in accordance with our Privacy Policy, Data Protection and our security-related policies. We employ strong Password Policy and 2-Factor Authentication (2FA) is mandatory within Remo. Role-based access and a need-to-know basis of availability are at the forefront of our strict Access Control Policy. Our secure system allows user data access only to fulfill customer requests. Further detailed information can be found in our security-related policies and support articles which include what security standards does Remo adhere to.

Security Compliance and standards – the reliability of our Cloud technology

Remo is built on highly secured Cloud technology and leverages inherent extra layers of security, encryption, protection, compliance, and other redundancies provided by our trusted Cloud technology partners. They also provide extra protection in our secure transactions and subscription management, necessary alarms and alerts, continuous data transmission and backup, data loss prevention, identity and access management, global and flexible firewalls, and Cloud security scanning among others.

Security and Compliance is a pair of inherent leverages together with a shared responsibility between our Cloud technology providers and Remo. This shared model and partnership provides Remo the powerful business edge as our providers operate, manage and control the Cloud infrastructure for Remo – the components, the systems involved and even the virtualization layer down to the physical security of the facilities in which the services they offer operate. They also provide us the security of the Cloud and the necessary protection and monitoring of the global infrastructure that runs all the services we partnered with them. As they provide us the Infrastructure as a Service (IaaS), we also inherit their secured physical and environmental controls including database security, best practices, and a variety of IT security standards, including:

- SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70)
- SOC 2
- SOC 3
- FISMA, DIACAP, and FedRAMP
- DOD CSM Levels 1-5
- PCI DSS Level 1
- ISO 9001 / ISO 27001 / ISO 27017 / ISO 27018
- ITAR
- FIPS 140-2
- MTCS Level 3
- HITRUST

The Cloud technology platform additionally provides inherent flexibility and control allowing Remo to deploy solutions that meet several industry-specific standards, including:

- Cloud Security Alliance (CSA)
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)

- Motion Picture Association of America (MPAA)
- Criminal Justice Information Services (CJIS)

You can find more detailed security information about our main partners and their services below:

- Google Cloud
- AWS (Amazon Web Services)
- MongoDB
- Stripe
- Chargebee
- Freshworks

Data Processing

We carefully and securely handle all data Remo collects about users. Our business model is to provide a paid service to users who need additional features on top of the trial version and does not rely on widespread collection of general user data. We at Remo are committed to safeguarding the privacy of our users. We will only collect information that we need to deliver the service to you and continue to maintain and develop the service. Our database security, video and audio streaming along with other network security, role-based permissions control, data encryption, Customers Terms of Service, Users Terms of Service, Privacy Policy, Data Protection, Cookie Notice, and how Remo processes sensitive information encapsulate our protection to user account information and event security as we partner with highly encrypted Cloud technology mentioned above.

Data Encryption

All communications between our platform in Remo along with underlying access to Cloud databases, storage layers and other services are all encrypted via AES-256 and AES-128 algorithms in different situations, all data integrity verified and using HTTPS connections. Our highly secured Cloud technology platform provides us numerous at rest storage encryption and other protection with all database systems fully redundant across multiple availability zones and backup in the Cloud.

Remo also leverages Cloud technology in using dedicated server infrastructure to allow more users in the conversation enjoying quality interactions with better stability. Streams will always be encrypted with the AES-256 algorithm in transit and will be decrypted and re-encrypted when passing through highly secured infrastructure of video routers strategically distributed across the world. The video router servers and all our infrastructure adhere to strict security standards and inherent security compliance preventing any eavesdropping or interruption of the video/audio streams.

Highly secured firewall solution

Remo further protects all users and their data via a highly secured firewall solution in place that filters both ingress and egress traffic, secures all communication instances, and adheres to high standards of Cloud technology. We also have a very comprehensive Gear Test available handy to check user's network compatibility including secure firewalls. Inherent layers of protection and higher levels of security are afforded by our secure web application with the firewall solution deployed on the network and all its virtual interface as Remo is built and maintained by a highly skilled and experienced team of SaaS Engineers and QA.

GDPR journey and other compliance

Remo processes and protects data based on legitimate interests, vital data protection and user consent along with their rights and obligations per our Customers Terms of Service, Users Terms of Service, Privacy Policy and Data Protection. As a startup, we are taking our GDPR journey seriously and have numerous wins and positive outlook on our roadmap ahead together with other compliance journey below:

- **GDPR at Remo**
- **GDPR Roadmap**
- **FERPA**
- **HIPAA**
- **CCPA**
- **COPPA**

Security & Accessibility in our knowledge base

Secured, timely and easy-to-follow steps to assist all users on common Security and Accessibility-related solutions are found and updated in our knowledge base section below:

https://help.remo.co/en/support/solutions/63000134089

Something we didn't cover?

Connect with us via our 24/7 Chat Support at the bottom right of remo.co, Help Desk or email legal@remo.co.