SaaS Security Questionnaire Lifesize

November 19, 2019

Table of Contents

1 Introduction

This document gives detailed information in regards to security, data protection and other required information for service compliance.

2 IT-Security – certification / regulation

2.1 Does vendor have an ISO 27001 or SAS 70 type II security management certification? Please submit this certificate in addition to this document.

If no certification vendor shall provide other independent and detailed assessment results of the quality of its Information Security Level.

The Lifesize service is entirely hosted in AWS. AWS maintains these certifications. The following link provides additional details on AWS compliance certifications: https://aws.amazon.com/de/compliance/programs/

2.2 Does vendor have an ISO 27018 certificate for cloud and personal data storage.

The Lifesize service is entirely hosted in AWS. AWS maintains these certifications. The following link provides additional details on AWS compliance certifications: https://aws.amazon.com/de/compliance/programs/

2.3 Does vendor have any other certifications, e.g PCI DSS, which are relevant for the provided services offered? Please submit this certificate in addition to this document.

The Lifesize service is entirely hosted in AWS. AWS maintains these certifications. The following link provides additional details on AWS compliance certifications: https://aws.amazon.com/de/compliance/programs/

Lifesize maintains EU-US and Swiss-US Privacy Shield certifications with the US Department of Commerce: https://www.privacyshield.gov/participant?id=a2zt0000000GnHfAAK&status=Active

2.4 You must maintain an up2date and consistent security policy. Please submit your Information Security Policy(ies) in addition to this document.

Alternatively, a detailed description of the parts of the policy relevant for providing the service to customer shall be provided.

Lifesize is in process of updating our entire security process documentation for our new architecture and expect to have that complete by Q1 2020.

2.5 Does your company have ITIL process in place for all aspects of IT Service delivery?

Lifesize utilizes an “infrastructure as code” configuration methodology. This does not fit well in a strict ITIL methodology.

3 Software security

3.1 Please provide details on which software security scanners are used and what kind of scans are performed.

The Lifesize production service operates separately and independently from the Lifesize corporate IT environment. The systems used for source control, build and continuous integration (CI) and the staging environment for quality assurance (QA) are each also maintained in separate and independent environments.

Our processes and controls include the following:
• Source code scans for common vulnerabilities and exposures (CVE) based on constantly updated lists.
• A build and CI process that only accesses our external source code repository, never repositories on engineers' computers. The resulting container images (source code and operating system) are scanned for known CVEs again.
• CI environment promotes container images to staging QA environment, which is completely isolated from the production environment.
• CI environment promotes container images to production environment after approvals.
• Very constrained access control to all systems in the code development pipeline.
• Regular penetration testing by an industry-recognized and independent third party on our production environment.

3.2 Vendor shall have effective, documented and regularly reviewed processes to handle and remediate security vulnerabilities in place.

Lifesize regularly reviews processes through a cross-functional security council that is responsible for implementing, updating, and reviewing security risk/mitigation/policy. This council is comprised of stakeholders from Dev Ops, IT, and Legal. Security control documentation is currently being re-written and is expected to be complete in Q1 2020.

3.3 Vendor must inform Customer about all Security Incidents and Data Protection Incidents that potentially affect Customer data immediately after Vendor becomes aware of such an incident. Vendor shall inform Customer of any measures Customer might implement to mitigate any effects the security incident might have on Customer data (as Vendor provides an interim measure until a root cause fix).

Lifesize is compliant with GDPR protocols surrounding data breach and will notify any impacted customers within the acceptable time frame for incident reporting.

3.4 Vendor shall inform customer of any security vulnerabilities in the service as soon as Vendor becomes aware of them. Vendor shall inform customer of any measures customer might implement to mitigate security vulnerabilities in the service known to Vendor (as Vendor provides an interim measure until a root cause fix).

Lifesize's policy is to inform customers of any security breach. We don't inform customers of all security vulnerabilities.

4 User handling

4.1 Please describe how individuals are authenticated? (Password rules)?

SigleSignOn (SSO) via SAML2.0 is the preferred method of user authentication.

4.2 What are the implemented security measures in the data center against unauthorized access or manipulation?

The Lifesize service is entirely hosted in AWS. AWS maintains the certifications mentioned earlier. The following link provides additional details on AWS data center controls.
https://aws.amazon.com/de/compliance/programs/
https://aws.amazon.com/compliance/data-center/controls/

4.3 Who from Vendor has access to the customer data? How are those individuals authenticated and audited? (this includes vendor or third parties)

Only the staff of the DevOps team and a very small number of Engineering staff have access to customer data. All access must be approved by the VP of DevOps.

4.4 Please describe the implemented authentication concept for customer accounts?
Do you support ADFS / SAML2 mechanism for customer accounts?
What technique is used for account creation in the cloud?

Lifesize supports single sign-on (SSO) via SAML2.0. SSO allows you to extend your own password retention, complexity and controls consistently to Lifesize. SSO also allows you to control which users have access to your Lifesize cloud-based subscription and which do not. More importantly, when using SSO with Lifesize, Lifesize authentication will occur directly between your users and your identity provider (IdP).

To provide SSO, Lifesize integrates with your IdP via SAML 2.0, which is the recognized standard for secure authentication to cloud services. Lifesize has validated interoperability with many top-tier IdPs, including Microsoft ADFS, Azure AD, OneLogin, Ping Identity and Okta.

Accounts for SAML users are created automatically upon successful authentication.

4.5 Which interactions by an authorized individual with your system are audited?

As a video conferencing service, user interaction with the service is primarily limited to placing and receving calls. An end customer administrator is able to review basic metadata about these calls, eg who has made calls, when, and the duration and quality of the call.

4.6 From your solution, how can data be downloaded or uploaded? Is there an interface? Do you provide an interface for mass up or downloads / data changes.

As a video conferencing service, this question does not fully apply. There is a limited concept of data transfers in the context of the Lifesize service, user interaction with the service is primarily limited to placing and receving calls.

4.7 Vendor shall provide a role concept that supports Segregation of Duties (e.g. a user with role HR cannot assign own salary).

As a video conferencing service, this question does not fully apply. User interaction with the service is primarily limited to placing and receving calls.

Licensed users can be assigned one of three roles within the Lifesize service. These roles and their capabilities are as follows.

User
As a User, you can:
• Place and receive calls
• Mute your own audio or video
• Create and own a meeting
• Set or change a passcode for a meeting you own
• Hide a meeting you own from the directory
• Add or remove individual or all participants in a meeting you own
• Mute individual or all participants in a meeting you own
• Chat with users or a group (if the Administrator has enabled chat)
• Live stream a meeting in a meeting you own (if the Administrator has enabled the meeting room for live streaming)
• Record a meeting (if the Administrator has enabled recording)
• Specify who can view a recording for a recording you own

Superuser
As a Superuser, you have the same permissions as a User plus you can:
• View usage reports
• Promote a User to a Superuser
• Demote a Superuser to a User
• Manage and delete Superusers and Users
• Manage and delete any meetings
• Hide any meeting from the directory
• Hide any User or Superuser from the directory
• Hide any room system from the directory that is not associated with the Administrator
• Enable or disable chat
• Enable or disable recording (if applicable with subscription level)
• Enable or disable live streaming on specific meetings (if applicable with subscription level)
• Enable or disable Lifesize Icon event alerts
• Configure single sign-on (SSO) (if applicable with subscription level)
• Configure integration with common calendaring services for one-click calling
• Configure dial-in PSTN phone numbers for meeting invites (if applicable with subscription options)
• Configure call details for meeting invites
• Customize Lifesize Icon wallpaper and Lifesize® PhoneTM HD user interface
• Configure meeting layouts
• Restrict the user email domains allowed to create new accounts in the Lifesize app

Administrator
As an Administrator, you have the same permissions as a User and a Superuser plus:
• Your account and permissions cannot be changed or deleted by a User or Superuser
• You can hide yourself from the directory
• You can hide room systems associated with your own user account from the directory

5 Protection of customer Information

5.1 Vendor describes in detail the architecture and data flow (incl. technical details such as products used and mechanisms implemented) and concepts that ensure that any data in motion is encrypted.
Vendor will inform customer before any changes to these elements are made and seek customer's approval for the change.

The Lifesize service, room systems and client software provide secure and encrypted video, audio, presentation (media) and call setup (signaling) in every call end to end. Encryption cannot be disabled by either administrator or user. All calls are encrypted with no trade-off in quality.

The Lifesize service, room systems and client software employ WebRTC. Encryption is a mandatory component of WebRTC and applies to both signaling (via DTLS) and media (via SRTP/AES-128).

Third-party H.323 systems will join video calls in a secure fashion when configured for H.235 encryption. Third-party SIP systems will join in a secure fashion when configured for SIP TLS.

5.2 Vendor describes in detail the architecture and data flow (incl. technical details such as products used and mechanisms implemented) and concepts that ensure that any data at rest is encrypted. Vendor will inform customer before any changes to these elements are made and seek customer's approval for the change.

• Lifesize Live Stream and Record and Share are encrypted using AES-128 for data in-flight (streaming, recording, or playback) and AES-256 for data at rest (storage).

• Lifesize chat is encrypted in flight (AES-128) and at rest (AES256) and is hosted on AWS, which is designed for security across all geographies and verticals. Learn more about AWS Security

5.3 Vendor shall have documented requirements and audit procedures (e.g. for network security) in place to ensure that third parties will not compromise the Vendor's infrastructure.

Regular penetration testing is conducted by an industry-recognized and independent third party on our production environment. Remediation plans can be shared under NDA.

6 Secure Infrastructure and physical security

6.1 Which transport layer security is being used?

The Lifesize service, room systems and client software provide secure and encrypted video, audio, presentation (media) and call setup (signaling) in every call end to end. Encryption cannot be disabled by either administrator or user. All calls are encrypted with no trade-off in quality.

The Lifesize service, room systems and client software employ WebRTC. Encryption is a mandatory component of WebRTC and applies to both signaling (via DTLS) and media (via SRTP/AES-128).

Third-party H.323 systems will join video calls in a secure fashion when configured for H.235 encryption. Third-party SIP systems will join in a secure fashion when configured for SIP TLS.

6.2 What techniques are implemented to encrypt saved data in the cloud or system?
Data a rest, which includes stored call recordings and chat, is encrypted using AES-256.
6.3 How is an isolated storage of data guaranteed? (Multitenancy)
Tenants are logically isolated using a UID uniquely identifying their group (ie, their tenancy).
6.4 In case of usage of a hypervisor, please name technology. What is the protection against failures / privilege escalation? (f.e. Intel Spectre / Meltdown)
The Lifesize services is hosted entirely in AWS and leverages the redundancy within and between AWS availability zones. Lifesize has implemented a containerized microservices architecture. Each microservice only has access to the resources necessary. Secure communication is used between microservices.
6.5 Do you utilize a certain reference architecture? What hardening measures are implemented?
The Lifesize services is hosted entirely in AWS and takes advantage of AWS' inbuilt security practices in addition to our own as a service vendor.
6.6 Vendor shall describe how IT components (e.g. servers) that store or process customer data are protected against malicious attacks (e.g. denial of service attacks, intrusion attempts).
The AWS network provides DDoS and some malicious attack protection. They will dynamically detect abuse and notify us of the situation. Lifesize also uses additional techniques including rate limiting, encryption at rest, and access control lists to limit access from blacklisted sources.
6.7 Vendor shall provide a detailed diagram of vendor's infrastructure (network and systems) used to provide the service to customer.
The Lifesize services is hosted entirely in AWS. We currently maintain service capacity in seven AWS regions worldwide. We are happy to discuss any specifics that are of interest.

6.8 Vendor shall provide details on how the compliance of vendor's systems with vendor's security policies is ensured (frequency of checks, methods used,…).

Server and network components are validated by AWS. Application compliance is verified at deployment time. All services are built and deployed via a CI/CD process and are validated as part of testing. We are also in process of implementing additional validation using AWS Config.

6.9 If applicable, vendor shall provide details on how third parties are involved in providing the service (e.g. code generated externally, hosting provider, customer service, …) and how vendor ensures that these third parties do not negatively impact the security level of the service.

Our data subprocessors can be found here:
https://www.lifesize.com/~/media/Documents/Other%20Documents/Legal%20Compliance/data-processing/Lifesize%20Data%20Subprocessor%20List%20Effective%20512018.ashx?la=en

Lifesize reviews the interaction with any third party services during design and implementation. We only work with third parties that meet or exceed our security requirements.

6.10 How is it ensured, that the processing of personal data is strictly conducted according to the instructions of the end customer?

Details on our handling of personal data can be found in our GDRP Compliance Statement located here:
https://www.lifesize.com/~/media/Documents/Related%20Resources/Corporate%20Documents/Lifesize-GDPR-Compliance-Statement.ashx

Our publicly available privacy policy can also be reviewed here:
https://www.lifesize.com/en/company/legal-notices/privacy

7 Business continuity management and disaster recovery

7.1 How is the constant availability and consistency of the data guaranteed? How many data centers are involved in the service? Hot or Cold standby?

The Lifesize service is hosted entirely in AWS. We currently maintain service capacity in seven AWS regions worldwide. At a high-level, the service operates on the concept of containers and orchestration. Spare "hot" capacity is maintained. "Cold" standby is accomplished by deployment of additional containers.

7.2 How often are data backups done?

Daily

7.3 Vendor shall provide detailed information on how Customer data is backed up, including - Are backups sent to an off-sitelocation? - Are external vendors used for storage or transport of backups? - Description of how it is ensured that a user retrieving data from the backup can only access data for which the user has formal access rights.

Service backups are performed within the AWS environment. They are not sent to an offsite location and do not involved external vendors. There is not a concept of a user backup or a situation where a user would retrieve back up data in the context of our service.

7.4 What system availability are guaranteed?

A financially backed service level agreement of 99.9% uptime is available from Lifesize for our video conferencing service. More information on our SLA can be found here: https://www.lifesize.com/en/resources/product-papers/lifesize-cloud-extreme-support-service-level-agreement

8 People and employees

8.1 Vendor shall provide a detailed description of the *vendor's* role concept (incl. list of roles and their responsibilities and access level to Customer's data) and how access to Customer's data is restricted based on that.

As a video conferencing service, Lifesize stores very limited customer data in comparison to other cloud services. The details of the data we store can be found below.

Only the Lifesize DevOps team and a limited number of Engineering staff have full access to customer data. Level 3 support engineers and customer success managers are given read access to limited amounts of customer data.

Call Data Retention
Video communication data is transient in nature and encrypted in flight. Lifesize does not view, record or otherwise store any video conference media (audio, video or presentation).

Call Information
Lifesize stores basic metadata of each call so that customer administrators can access usage reports and information. This data does not include any media. Should you choose to leave the Lifesize service, this information will be permanently deleted 180 days following the end of your contract. Similarly, server logging is retained for the purposes of technical support engagements and troubleshooting for 30 days. This data does not include any media.

User Information
Lifesize stores only basic information for each of our customers' user accounts. Should you choose to leave the service, this information will be deleted 180 days following the end of your contract.
Administrator:
• Email address (which is also the username)
• Password (for non-SSO accounts only)
• First name, last name
• Display name
• Telephone
• Address
• Company

User and Superuser:
• Display name
• Email address (which is also the username)
• Password (for non-SSO accounts only)

Lifesize Stream, Record and Share
Lifesize offers streaming and recording services as an additional option for our customers. Recorded calls are stored in secure Amazon Web Services facilities. Access to view recordings may be globally restricted to users within your organization only by the administrator.
• Lifesize Record and Share is available to subscribers of the Lifesize cloud-based service. Record and Share is disabled by default and must be purposefully enabled by an administrator before users are able to record any calls.
• Content distribution may be restricted to only your own organization.
• Lifesize Live Stream and Record and Share are encrypted using AES-128 for data in-flight (streaming, recording, or playback) and AES-256 for data at rest (storage).
• Lifesize Record and Share is hosted on AWS, which is designed for security across all geographies and verticals. Learn more about AWS Security.
• Initiation of recordings requires manual intervention whereby a user of the Lifesize cloud-based service must activate the feature to record the conference session.

• An on-screen notification will be displayed to all video participants taking part in the conference to notify users that the call is being recorded and by whom.

Chat
Lifesize chat is encrypted in flight (AES-128) and at rest (AES256) and is hosted on AWS, which is designed for security across all geographies and verticals. Learn more about AWS Security

8.2 Vendor will ensure full commitment to information security and data protection requirements of all employees as well as any external partners. Vendor will provide proof that all these parties are aware of the respective rules and are contractually bound to follow them.

Lifesize has data processing agreements in place with third parties.

8.3 Vendor shall create awareness for Information Security among its employees and shall check the Information Security skills of the employees at least annually.

Lifesize uses a Learning Management System (LMS) to track employee's completion of annual security training.

8.4 Vendor shall take appropriate measures to prevent information security breaches by insiders, with special emphasis on privileged insiders.

Lifesize uses audit logging to validate that insiders are only accessing data as required by performing their job function.

9 Operation

9.1 Vendor will run penetration tests of the application and the application environment before whenever a major change is implemented, but at least annually. Vendor will make the detailed test report available to customer and fix any identified vulnerabilities promptly.

Regular penetration testing is conducted by an industry-recognized and independent third party on our production environment. Remediation plans can be shared under NDA.

9.2 Vendor shall have effective, documented and regularly reviewed processes for the installation and secure configuration of operating systems, applications and network components (e.g. routers, firewalls) and further hardening measures in place.
Operating system configuration is done at the container level and is updated as services are updated in production. EC2 instance configuration is done at the AMI level. Lifesize uses known secure AMIs recommended by AWS. Lifesize does not build our own custom AMIs. Lifesize uses managed networking services from AWS. Configuration of security groups, load balancers, and network access control lists is done regularly.
9.3 Vendor will audit any successful and unsuccessful connection attempts, every activity of a privileged account, operations on sensitive data as well as any other information that can help identify inappropriate use of the system intrusion attempts and unauthorized access to customer's data. Vendor shall make this information available to customer in a format that can easily be processed by customer.
Lifesize only provides audit information to customers in the event of a breach situation.

9.4 If applicable, vendor shall describe in detail how networks, servers or other elements used for delivery of the service are managed remotely, including technologies (e.g. VPN) and authentication mechanisms (e.g. two-factor authentication) used.
Lifesize uses AWS VPC connections to limit remote access to the production environment. All access must be from the Lifesize internal network. Access to the Lifesize internal network is controlled via two-factor authentication via Okta.
9.5 Vendor shall describe how system/network logs are monitored and analysed, including information on tools used to analyze log data.
System logs are only used by engineers to analyze customer reported issues.
9.6 Vendor shall describe how suspicious activity is detected and how the escalation process works
The AWS abuse team analyzes network logs to identify suspicious activity and notifies Lifesize to evaluate any suspicious activity.
9.7 Vendor shall describe how it is ensured that no unauthorized IT components (e.g. modems, WLAN access points) is introduced into the environments used to provide service.
Lifesize has no physical access to AWS data centers. AWS controls have been documented previously in this docuement.
9.8 Vendor shall ensure a 4-eye-principle of administrative access to customer's data.
Requests for access are reviewed by both IT staff and DevOps staff before being granted.

9.9 Vendor shall ensure that system access and data access follow the principles of least privilege and need-to-know. There shall be no administrators with unrestricted access to networks, systems or customer's data.

Lifesize does conform with access control providing least privilege and need-to-know controls.

10 Incident Management

10.1 Was there a security breach in the SaaS solution software recently?

No

10.2 Is there an escalation matrix for security incidents? If yes, please attach it to this document.

Lifesize is updating our security process documentation and expect to complete it in Q1 2020.

10.3 How are the rights of access modified within a client?

As a video conferencing service, this question does not fully apply. User interaction with the service is primarily limited to placing and receving calls.

Licensed users can be assigned one of three roles within the Lifesize service. These roles and their capabilities are as follows.

User
As a User, you can:
• Place and receive calls
• Mute your own audio or video
• Create and own a meeting
• Set or change a passcode for a meeting you own
• Hide a meeting you own from the directory
• Add or remove individual or all participants in a meeting you own
• Mute individual or all participants in a meeting you own
• Chat with users or a group (if the Administrator has enabled chat)
• Live stream a meeting in a meeting you own (if the Administrator has enabled the meeting room for live streaming)
• Record a meeting (if the Administrator has enabled recording)
• Specify who can view a recording for a recording you own

Superuser
As a Superuser, you have the same permissions as a User plus you can:
• View usage reports
• Promote a User to a Superuser
• Demote a Superuser to a User
• Manage and delete Superusers and Users
• Manage and delete any meetings
• Hide any meeting from the directory
• Hide any User or Superuser from the directory
• Hide any room system from the directory that is not associated with the Administrator
• Enable or disable chat
• Enable or disable recording (if applicable with subscription level)
• Enable or disable live streaming on specific meetings (if applicable with subscription level)
• Enable or disable Lifesize Icon event alerts
• Configure single sign-on (SSO) (if applicable with subscription level)
• Configure integration with common calendaring services for one-click calling
• Configure dial-in PSTN phone numbers for meeting invites (if applicable with subscription options)
• Configure call details for meeting invites
• Customize Lifesize Icon wallpaper and Lifesize® PhoneTM HD user interface
• Configure meeting layouts
• Restrict the user email domains allowed to create new accounts in the Lifesize app

Administrator
As an Administrator, you have the same permissions as a User and a Superuser plus:
• Your account and permissions cannot be changed or deleted by a User or Superuser
• You can hide yourself from the directory
• You can hide room systems associated with your own user account from the directory

10.4 Vendor shall inform customer if any security vulnerabilities have been found in released versions of the service so far and how vendor reacted.

Lifesize has been informed of security vulnerabilities in our Icon room systems. Most of these vulnerabilities were addressed in patches or future releases, depending on the severity. Some vulnerabilities were deemed very low risk when Icon room systems were properly configured behind customer firewalls.

11 Support & Cooperation

11.1 Which response times are guaranteed in the event of system failure?

1 hour (Lifesize Extreme Support)

https://www.lifesize.com/en/resources/product-papers/lifesize-cloud-extreme-support-one-pager

11.2 Which response times are guaranteed in the event of recovery of deleted data?

Lifesize does not guaranteed response times for recovery of deleted data. The response time will vary depending on the age of the data and the system used to archive the data. As a video conferencing service, Lifesize stores a limited amount of data as previously described. Any event that impacts a customer's ability to use the service would be treated with highest priority.

11.3 Are there defined contact persons for support and change requests?

The Lifesize technical support team is available up to 24/7 with the Extreme Support Tier. Lifesize technical support may be engaged online or via telephone.

11.4 How can data from the SaaS solution be partly or completely exported?

This question is somewhat out of scope for a video conferencing service. Video calls, for instance, are transient data that exists in real time only. However, user created recordings can be downloaded by authorized users.

11.5 Is there an option of inspection of audit documents?

Lifesize does not share audit information with customers except in a breach situation.

11.6 Can the end customer conduct own audits in your company?

No

12 Data Protection

12.1 Is data protection according to EU GDRP law guaranteed? If no, which national data protection law applies?

Lifesize GDPR Compliance Statement:
https://www.lifesize.com/~/media/Documents/Related%20Resources/Corporate%20Documents/Lifesize-GDPR-Compliance-Statement.ashx

12.2 Do you transfer personal data to non-EU organisations or countries?

If vendor provides a solution for Non-EU end customer companys' local law must be applied.

Yes. Please reference Lifesize EU-US and Swiss-US Privacy Shield certifications.

12.3 Data Transfers – Companies should verify that they are EU-U.S. Privacy Shield certified. If no EU-US. Privacy Shield verification, then an EU Model Contractual Clauses must be used.

If vendor provides a solution for Non-EU end customer companies' local law must be applied.

Lifesize complies with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework.

12.4 Which categories of personal data are stored in your solution?

Category A: General processing of personal data.

Category B: Sensitive personal data such as racial or ethnic origin of the data subject, political opinions, religious beliefs or other beliefs of a similar nature, member of a trade union, biometric and genetic data, data concerning health and sexual life.

Category C: Bank and credit card information.

Category A:
Lifesize stores only basic information for each of our customers' user accounts. Should you choose to leave the service, this information will be deleted 180 days following the end of your contract.
Administrator:
• Email address (which is also the username)
• Password (for non-SSO accounts only)
• First name, last name
• Display name
• Telephone
• Address
• Company

User and Superuser:
• Display name
• Email address (which is also the username)
• Password (for non-SSO accounts only)

12.5 Are there defined contact persons in the case of changes to instructions from end customer to the processing of personal data?

privacy@lifesize.com

12.6 Where is the data saved? (Physical storage location, including backup, disaster recovery system / storage of backup tapes).

All data is stored in AWS managed services – DynamoDB, RDS, S3, and Glacier.

12.7 Upon termination or expiration of the contract or at customer advice vendor shall return customer Data to customer in the defined format (details to be defined for the specific cases). Notwithstanding the sentence above the returned data shall be in a format easily be processed by customer. Vendor hereby waives its right of retention, if any, with respect to the customer Data. Upon customers, written request vendor shall delete the data from vendors systems in its entirety (including but not limited to backups and copies). Vendor shall confirm the deletion in writing.
There is a limited concept of customer data within the context of the Lifesize service. Customer data will be deleted automatically 180 days following the termination or expiration of the contract. Our terms of service will be the governing document with respect to the Lifesize Service. https://www.lifesize.com/en/company/legal-notices/terms-of-service Requests for deletion can be made to privacy@lifesize.com.
12.8 Vendor shall provide the opportunity to customer to delete data in particular circumstances, either per individual or based on the elapse of certain retention periods. The IT-System must be able to support different storing-/ deleting periods with an automatic process.
There is a limited concept of customer data within the context of the Lifesize service. Requests for deletion can be made to privacy@lifesize.com.
12.9 Vendor shall provide the customer with contact details of the person responsible for data protection (vendor's Data Protection Officer). Additionally, vendor must provide defined communication interfaces to be used in case of data protection, information security, service continuity/ IT crisis management, incident handling, etc.
Lifesize does not have an individual DPO. A cross-functional team responds to issues communicated through either contact points listed in our online Trust Center (privacy@lifesize.com) or contacts via our Technical Support team.

12.10 Vendor may only award subcontracts with the prior written consent of the customer. The same shall apply to the use of a company affiliated to the vendor within the meaning of Section 15 et seq. of the German Stock Corporation Act (Aktiengesetz). Irrespective hereof, the vendor must ensure that his subcontractors are also subject to at least those obligations that exist under this contract and that the customer is also able to assert corresponding rights and claims directly against subcontractors and to verify the subcontractors' compliance. The vendor shall also make adequate checks by himself to ensure that subcontractors comply with the requirements, shall document the results of these checks and shall grant the customer access to the relevant contractual materials and documentation at the latter's request. The vendor shall follow customer directives, i.e. instructions issued by the customer in relation to a specific action by the contractor regarding the protection of the data (for example use, anonymization, blocking, deletion or restoration).

Our terms of service will be the governing document with respect to the Lifesize Service.
https://www.lifesize.com/en/company/legal-notices/terms-of-service

12.11 Please describe the procedure and time limit for the privacy compliant deletion of data?

The Lifesize publically available privacy policy details this procedure in Section 7:
https://www.lifesize.com/en/company/legal-notices/privacy

"In addition, you have the ability to direct us to update or delete/deactivate certain information pertaining to you. You can also contact us to request removal of your personal information from the blog, community forums or other public areas on our Site. Lifesize may not be able to remove some or all of your personal information, in which case we will let you know why. Please contact us using the information in Section 10 below. For your protection, we may only implement requests with respect to the personal information associated with the particular email address that you use to send us your request, and we may need to verify your identity before implementing your request."

12.12 How is the reliability and training of a person eligible to the processing of personal data being checked?

Relevant Lifesize employees are subject to a criminal background check and must complete annual privacy and information security training in order to reinforce policies and procedures relating to GDPR obligations.

12.13 Are all employees obliged to the data secrecy?
Yes
12.14 Vendor will have adequately trained teams in place that are responsible for the security of customer’s data (e.g. information security, data protection, physical security).
Yes
12.15 Vendor shall provide a detailed description of the vendor's role concept (incl. list of roles and their responsibilities and access level to Customer's data) and how access to Customer's data is restricted based on that.
Please refer to the answer in section 4.7.
12.16 Vendor shall take appropriate measures to prevent information security breaches by insiders, with special emphasis on privileged insiders.
Please refere to the answer in section 8.4.
12.17 Vendor shall provide the customer with contact details of the person responsible for data protection (vendor's Data Protection Officer). Additionally, vendor must provide defined communication interfaces to be used in case of data protection, information security, service continuity/ IT crisis management, incident handling, etc.
Please refer to the answer in section 12.9.

12.18 Which sub-contractors (name and principal office) are active for the cloud service and have possibly access to the data of the end customer?
Lifesize data sub-processors can be found here: https://www.lifesize.com/~/media/Documents/Other%20Documents/Legal%20Compliance/data-processing/Lifesize%20Data%20Subprocessor%20List%20Effective%20512018.ashx?la=en
12.19 If applicable, vendor shall provide details on how third parties are involved in providing the service (e.g. code generated externally, hosting provider, customer service, …) and how vendor ensures that these third parties do not negatively impact the security level of the service.
Please refer to the answer in section 6.9.
12.20 Vendor may engage subcontractors only with the prior, written permission of the end customer.
Our terms of service will be the governing document with respect to the Lifesize Service. https://www.lifesize.com/en/company/legal-notices/terms-of-service
12.21 Is there an option of inspection of audit documents?
Lifesize respectfully declines such requests.
12.22 Can the end customer conduct own audits in your company?
Lifesize respectfully declines such requests.