Security, Privacy and Architecture of the Calipsa Software

Published: 23 March 2021

1. **Calipsa's Corporate Trust Commitment**

Calipsa is committed to achieving and maintaining the trust of our customers. Integral to this mission is providing a robust security and privacy program that carefully considers data protection matters across our suite of services, including data submitted by customers to our services ('**Customer Data**').

2. **Services covered**

This documentation describes the architecture of the security and privacy-related audits and certifications received for, and the administrative, technical, and physical controls applicable to, the following Calipsa services (collectively, for the purposes of this document, the '**Covered Services**'):

(a) remote video monitoring platform: Service sold through monthly or yearly contract; and

(b) Calipsa engine: Service sold through monthly or yearly contract.

3. **Architecture and data segregation**

The Covered Services are operated in a multitenant architecture that is designed to segregate and restrict Customer Data access based on business needs. The architecture provides an effective logical data separation for different customers via customer-specific unique identifiers and allows the use of customer and user role based access privileges. Additional data segregation is ensured by providing separate environments for different functions, especially for testing and production. The specific infrastructure used to host Customer Data is described in the 'Infrastructure and sub-processors' section below.

4. **Control of processing**

4.1 Calipsa has implemented procedures designed to ensure that Customer Data is processed only as instructed by the customer, throughout the entire chain of processing activities by Calipsa and its sub-processors. In particular, Calipsa and its affiliates have entered into written agreements with their sub-processors containing privacy, data protection, and data security obligations that provide a level of protection appropriate to their processing activities.

4.2 Compliance with such obligations as well as the technical and organizational data security measures implemented by Calipsa and its sub-processors are subject to regular audits.

5. **Security controls**

5.1 The Covered Services include a variety of security controls. These controls include:

(a) unique user identifiers allow customers to assign unique credentials for their users and assign and manage associated permissions and entitlements;

(b) controls to ensure initial passwords must be reset on first use;

(c) controls to limit password re-use;

(d) password length and complexity requirements; and

(e) customers have the option to manage their application users, assign or define roles, and apply permissions and rights within their implementation of the Covered Services.

5.2 Some Covered Services use AWS, as described above; further information about security provided by AWS is available from the AWS Security website, including AWS Security website, including AWS's overview of security processes.

6. **Security policies and procedures**

The Covered Services are operated in accordance with the following policies and procedures to enhance security:

(a) user passwords are stored using a salted hash format and are not transmitted unencrypted;

(b) user access log entries will be maintained, containing date, time, User ID, URL executed or identity ID operated on, operation performed (accessed, created, edited, deleted, etc) and source IP address;

(c) if there is suspicion of inappropriate access to the Covered Services, Calipsa can provide customers log entry records to assist in forensic analysis. This service will be provided to customers on a time and materials basis;

(d) user access logs will be stored in a secure centralized host to prevent tampering;

(e) user access logs will be kept for a maximum of 30 days; and

(f) Calipsa personnel will not set a defined password for a user.

7. **Intrusion detection**

Calipsa, or an authorized independent third party, will monitor the Covered Services for unauthorized intrusions using network-based intrusion detection mechanisms. Calipsa may analyze data collected by users' web browsers (eg, device type, screen resolution, time zone, operating system version, browser type and version, system fonts, installed browser plugins, enabled MIME types, etc) for security purposes, including to prevent fraudulent authentications, and to ensure that the Covered Services function properly.

8. **Security logs**

All Calipsa systems used in the provision of the Services Covered, including firewalls, routers, network switches and operating systems, log information to their respective system log facility or a centralized syslog server (for network systems) in order to enable security reviews and analysis.

9. **Incident management**

Calipsa maintains security incident management policies and procedures. Calipsa notifies impacted customers without undue delay of any unauthorized disclosure of their respective Customer Data by Calipsa or its agents of which Calipsa becomes aware to the extent permitted by law.

10. **User authentication**

Access to the Covered Services requires a valid user ID and password combination, which are encrypted while in transmission, as well as machine specific information for identity validation as described under '**Security controls**' above. Following a successful authentication, a random session ID is generated and stored in the user's browser to preserve and track session state.

11. **Physical security**

Production data centers used to provide the Covered Services have access control systems. These systems permit only authorized personnel to have access to secure areas. These facilities are designed to withstand adverse weather and other reasonably predictable natural conditions, are

secured by around- the-clock guards, two-factor access screening, including biometrics, and escort-controlled access, and are also supported by on-site back-up generators in the event of a power failure.

12. **Reliability and backup**

All infrastructure components are configured in a high availability mode or in a redundant fashion. All Customer Data submitted to the Covered Services is stored on infrastructure that supports high availability and is backed up on a regular basis. This backup data is retained for 30 days.

13. **Disaster recovery**

The Covered Services' production systems are protected by disaster recovery plans which provide for backup of critical data and services. A comprehensive system of recovery processes exists to bring business-critical systems back online within the briefest possible period of time. Recovery processes for database security, systems administration, and network configuration and data provide a roadmap for personnel to make processes available after an outage. The Covered Services' disaster recovery plans currently have at least the following standard target recovery objectives:

(a) restoration of the Covered Services (RTO) within 132 hours after Calipsa's declaration of a disaster; and

(b) maximum Customer Data loss (RPO) of 72 hours; excluding, however, a disaster or multiple disasters causing the compromise of both data centers at the same time, and excluding development and test bed environments, such as the Sandbox service.

14. **Data encryption**

The Covered Services use, or enable Customers to use, industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer's network and the Covered Services including through Transport Layer Encryption (TLS) leveraging at least 2048-bit RSA server certificates and 128 bit symmetric encryption keys at a minimum.

15. **Return of customer data**

During the contract term, customers may export a copy of any Customer Data that is made available for export through the Covered Services. Within 30 days of termination of the applicable Covered Service, customers may:

(a) request return of Customer Data by contacting info@calipsa.io;

(b) access their account to export or download Customer Data; or

(c) contact their account manager to download or export reports.

16. **Deletion of Customer Data**

16.1 After termination of one or more of our services, to request deletion of Customer Data submitted to such service, contact info@calipsa.io. After termination of the services, following the 30-day period for return of Customer Data, Customer Data is retained in inactive status for up to 30 days, after which it is securely overwritten or deleted. After termination of the service, Customer Data is removed within 30 days. For the Covered Services, back-up data may be retained for an additional 90 days after deletion of Customer Data, after which it is securely overwritten or deleted.

16.2 This process is subject to applicable legal requirements. Without limiting the ability for customers to request return of their Customer Data submitted to the Covered Services, Calipsa reserves the right to reduce the number of days it retains such data after contract termination. Calipsa will update this Calipsa Cloud Security, Privacy and Architecture Documentation in the event of such a change.

17. **Sensitive data**

17.1 Important: The following types of sensitive personal data may not be submitted to the Covered Services:

17.2 Government-issued identification numbers; financial information (such as credit or debit card numbers, bank account numbers, and any related security codes or passwords). Additionally, information related to an individual's physical or mental health and information related to the provision or payment of health care may not be submitted to our Covered Services.

17.3 Additionally, Calipsa uses Customer Data consisting of CCTV footages from various sites being monitored. Calipsa anonymises this data prior to storing such that no personally identifiable information is contained in the Anonymized Data, nor any data that would identify customers, their users, customers' clients, or any individual, company or organization. Calipsa combines the Anonymized Data to improve its algorithms to provide increasing benefits to customers. We also refer to this as '**Aggregate Data**'.

18. **Infrastructure and sub-processors**

Service Provider/ Processor	**Purpose**	**Jurisdiction**
Amazon Web Services	Data hosting and backup	UK and EEA
Google Cloud Platform	Data hosting and backup	UK and EEA
RapidSwitch	Data hosting and backup	UK
Sunix Global Services	Video and image data annotation	India
Calipsa Ltd. (service provider/sub-processor of Calipsa LLC)	Providing our Services and resolving any technical issues related to the same	UK
Calipsa LLC (service provider/sub-processor of Calipsa Ltd.)	Providing our Services and resolving any technical issues related to the same	USA