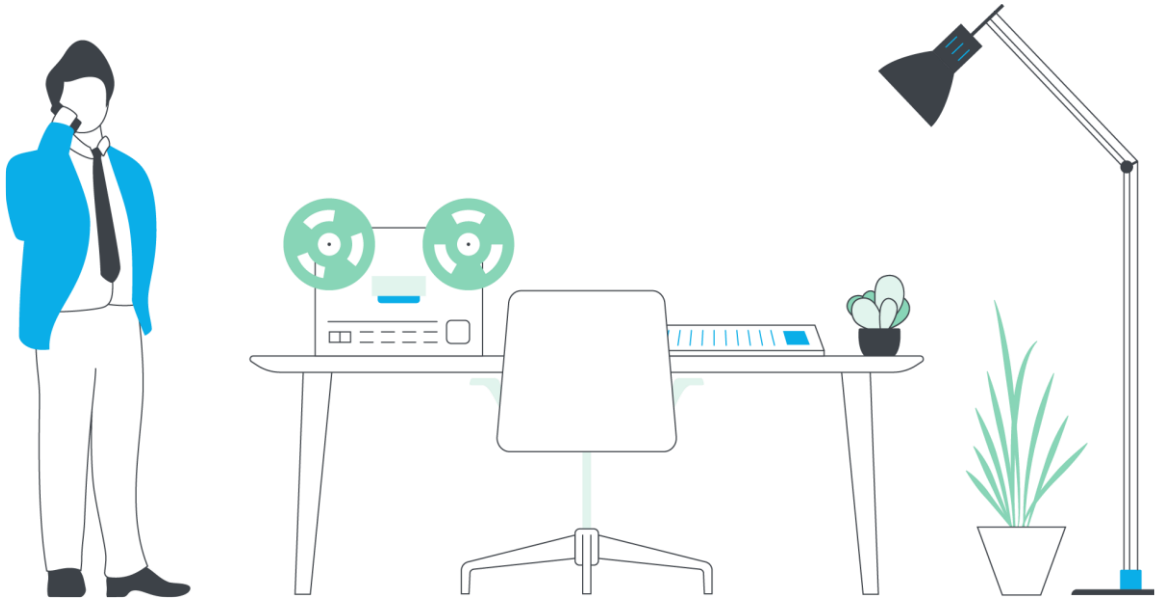
Luware



Information Security White Paper

Luware
Recording

Luware AG
Pfingstweidstrasse 102
CH-8005 Zürich

solutions@luware.com
+41 58 404 28 00
www.luware.com

Document-ID	LUREC-INFOSEC
Version	1.1
Status	Approved by Alexander Grafetsberger
Issue Date	31.01.2022
Valid from	31.01.2022
Valid to	30.01.2023

Contents

1 Introduction

Security and data protection are at the forefront of our efforts to provide our customers with Cloud hosted Software-as-a-Service (SaaS) offerings they can trust and rely upon.
Luware endeavors to meet security industry standards where technically possible. Ensuring the information security policies mandated for our Luware Recording offering are reviewed on a regular basis. This document describes Luware's efforts and measures in place to ensure data safety and security within the Luware Recording environment for our customers.

2 Audience

Luware Recording Customers, Partners and Prospects

3 Data Privacy

This chapter outlines the primary measures Luware is taking to ensure Data Privacy, Access Control and Segregation.

3.1 Data Location

At the time of writing, the Luware Recording Multi-Tenant offering is hosted in the Microsoft Azure Data centers located in Switzerland. The data location of the Luware Recording Private-Tenant offering is defined by the individual customer's requirements.

3.2 Data Access Types

3.2.1 Luware Administrative Data Access

Luware implements the principle of least privilege and 'need to know' in order to minimize the risk of data exposure. Luware personnel are only authorized to access the data they necessarily and reasonably must have access to in order to fulfil their current job role and responsibilities. Data access is reviewed on a regular basis to remediate any unnecessary access privileges. Requests for additional access follow a formal process which includes senior management approval.

3.2.2 Customer Access

Data access, administrative roles and privileges are managed by the customer tenant administrators. It's the customer's sole responsibility to maintain and control the access scope within their own organization.

3.3 Access and Authentication

The Luware Recording platform is a licensed-user only system, where only specific, named individuals are given access to consume the service.

3.3.1 Authentication

User access is authenticated with tight integration to Microsoft's global identity management platform (Azure Active Directory - AAD) and industry standard authentication flows (OAuth2).

3.3.2 Anonymous Access

Anonymous access is not supported.

3.3.3 Multi-Factor Authentication

Multi-factor authentication (MFA) can be enabled by customers by leveraging Microsoft's Azure MFA system integrated in AAD (Azure AD) or ADFS (Active Directory Federation Services).

3.3.4 Role Based User Access

Administrative users that require access to operate the platform (both from a customer perspective and Luware systems administration) must have their administrative permissions explicitly granted and are only given the minimal level of access enforced via Role-based Access Control (RBAC).

The customer performs self-administration of access to data, by leveraging pre-defined Role Based Access Control policies built in to Luware Recording.

3.3.5 Generic User Accounts

Generic service and administration user accounts are not permitted. End-customer users are only ever granted application-specific account roles / permissions, tied to their named AAD account. This ensures that our customers maintain complete control over their user account security in line with their

organizational requirements (including Multi-Factor Authentication). Moreover, it ensures that Luware has no need to store or process user account passwords with authentication being performed within the customer's environment.

3.3.6 Service Accounts

All internal application service accounts are provisioned on a per-application basis, with enforcement of minimal permissions. Service Account details are protected conforming to industry security standards.

3.3.7 Application User Roles

As previously mentioned, Luware Recording provides the customer the ability to restrict and govern the level of access rights for their end users.
This section details the RBAC policies that can be used today.

User Roles
User – an end user whose conversations are recorded in the system. This user can (if desired) be enabled to access the Web Interface of Luware Recording to retrieve and play back their own recordings. **Supervisor** – an end user who has access to search, retrieve and play back the recordings of recorded users and execute reports in the Luware Recording system. **Administrator** – a customer (or partner) user who has access to configure customer specific system components like data management policies, storage targets and user provisioning.

3.4 Data Segregation

Multi-Tenant

All customer configuration data and ca recording metadata is stored and maintained in the shared Luware Recording Cloud infrastructure, which is segregated logically on a tenant-level in order to keep the data demarcated, private and secure.
Voice recordings created in the Luware Recording platform are stored directly in customer provided Azure Storage and hence are fully segregated.
If the customer chooses the Luware-provided storage option for convenience recording, the recordings are stored on a customer specific storage account which is fully segregated from other customer data.

Private-Tenant

All customer configuration data and recording metadata is stored and maintained in the customer specific Luware Recording Cloud infrastructure which is segregated at resource group, network and server layer on a tenant-level in order to 100% segregation of customer data.
Voice recordings created in the Luware Recording platform are stored directly in customer provided Azure Storage and hence are fully segregated.

3.5 Data Retention

Data within the Luware Cloud applications is retained for the purpose of system operation and reporting. Data Retention policies are in place to ensure Data is not kept any longer than necessary to service its purpose. The following Data Retention policies are in place:

Product	Data Retention
Luware Recording	**Media and CDR Records:** Configurable by the customer **Configuration Data:** Customer Contract duration +30 days

Internal application logs: Luware temporarily stores internal application logs to help our support engineers troubleshoot the performance and operation of application components. This data is transient in nature, with old log data being purged regularly – typically in less than 72 hours.

3.6 Data Backup

To ensure service resilience we run a highly available application infrastructure with no single point of failure within the data center. Additionally, to enable fast recovery of our applications in the unlikely event of critical infrastructure failure we also backup our application servers and their associated configuration databases.

Due to the dynamic nature of our applications, our application servers are backed up daily, and configuration databases hourly. These backups are retained for up to 30 days for the sole purpose of disaster recovery, before being purged. All backups are encrypted using a Luware internal certificate.

3.7 Data Disposal

Where reasonably possible and legally permitted, Customer Data is removed immediately from Luware's storage infrastructure after contract termination. Any backups are automatically deleted after 30 days after retention expires.

4 Data Protection and Security

This chapter outlines the primary measures Luware takes to ensure Data Protection and Data Security.

4.1 Security Baseline

Luware has established a security baseline based on industry standards and regular internal info-sec reviews. The security baseline defines the minimum standard as well as guidelines in order to implement and maintain the baseline security standards for the Luware Cloud Services.
The security baseline is frequently reviewed and if required updated in order to adjust to changing business needs, evolving technology as well as emerging market requirements. The security baseline includes a set of documentation outlining reference architecture, system hardening procedures, implementation guides and security principles which must be adhered to when implementing, upgrading, migrating or decommissioning a system within the Luware Recording infrastructure.

4.2 Threat Prevention

Luware implements policies, tools, and technology in order to protect the Luware Recording environment from both external and internal threats. These include, but are not limited to, both physical and logical access control, network segregation, firewalls, virus- and malware protection, proactive alerting as well as IDS and IPS policies.

4.3 Patching

Luware maintains a regular patch cycle in order to keep the Luware Recording platform and the underlying infrastructure up to date and protect it against vulnerabilities. These patch cycles are usually executed within maintenance windows which will be communicated to the customer in advance. In cases of imminent threats, vulnerabilities or system malfunction, Luware reserves the right to announce a maintenance window on short notice in order to ensure platform security, stability and availability.

4.4 Secure Service Administration

Luware has implemented processes in order to be able to respond and address incidents as and when they arise. System monitoring and alerting tools are in place to pro-actively detect incidents arising in the Luware Cloud infrastructure. The Luware service desk is equipped to respond to incidents directly reported by customers. Incident's root causes and outcomes are reviewed on a regular basis in order to identify process gaps, training needs or necessary documentation updates/improvements and derive the necessary corrective measures.

4.5 Change Control

In order to minimize operational risks resulting in data exposure, service degradation or unavailability, Luware implements a change management process which controls all non-standard changes executed on a production system. All changes with impact on a production system are documented, tested and approved by a Change Approval Board before deployment.

4.6 Physical Security

The Luware Recording services are hosted within Microsoft Azure Data Centers. Microsoft ensure industry standard physical protection for the servers and system infrastructure hosted in their environment. It's within the services providers responsibility to restrict physical access and ensure maximum security to the server infrastructure. More details regarding the physical security of the Microsoft Azure Data Centers can be found here:
https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security

4.7 Logical Security

Access to systems and data within the Luware Recording environment is restricted based on a stringent and hardened role-based access control system enforced over multiple system layers from the virtualization layer through the Operating System layer and into the end user applications. Where in Luware's control, the logical access and security controls are controlled in pre-defined security framework with recurring reviews and Joiner/Mover/Leaver process.

4.8 Protection of Data At Rest

Data Type	Protective Measures
Backend Databases	All Backend Databases containing sensitive data (configuration data, reporting data, transaction records) are encrypted using transparent database encryption (TDE) using AES-256/SHA-256 encryption according to industry standards.
General Data Storage	Any customer data stored at rest within the Luware Recording environment underlies the following security measures. **Physical Access control** – only named individuals with the necessary access privileges can access the physical data center location. **Logical Access control** – only named individuals with the necessary access privileges can access the logical data storage.
Call Recording Data on Customer Storage	Call Recordings which are stored on customer supplied Azure storage are encrypted using standard Luware AES-256/SHA-256 encryption or with customer supplied encryption certificate.

4.9 Protection of Data In Transit

Data Type	Protective Measures
Web Applications	Any information transmitted between the Luware Recording web application and the end customer via public networks is encrypted using strong encryption. Luware leverages SSL certificates issued by DigiCert Inc. DigiCert

SHA2 Secure Server CA supporting the TLS 1.2 protocol and AES256 encryption with SHA2 signature.

System API's

Any system API's are secured with a user-based authentication system. Access to APIs will be logically segregated within the system backend based on the same mechanism as the Web Applications. Any information transmitted between Luware Recording and the end customer via public networks is encrypted using strong encryption. Luware leverages SSL certificates issued by DigiCert Inc. DigiCert SHA2 Secure Server CA supporting the TLS 1.2 protocol and AES256 encryption with SHA2 signature.

Internal Data

Any information transmitted between services in the Luware Recording environment is encrypted using strong encryption. Luware leverages SSL certificates issued by its own internal Certificate authority using SHA256/TLS 1.2.

5 High Availability and Business Continuity

Businesses of all sizes, across the globe, rely on the Luware Recording Solution to ensure compliance across their organization. Due to the nature of the offered service, High Availability and Business Continuity plays a vital part of providing this service to our customers.

It is well understood that the availability and reliability of our platform is essential to the day-to-day operations of our customers and partners. The measures we take to protect our customers, their data and the services we provide to them include, but are not limited to;

- Maintenance of a Business Continuity Program
- Business Impact Analysis
- Risk Management
- High-availability Platform Architecture
- Geo-Resiliency
- A stringent Software Lifecycle Management Process

More details regarding our Business Continuity measures can be found in the Luware Recording Business Continuity Whitepaper which can be obtained from your Luware Account Manager.

6 Standards and Certification

Luware AG holds the ISO 9001 and ISO 27001 certification which requires stringent Information Security measures to be implemented. All ISO 9001 and ISO 27001 measure have been rolled out group wide to all Luware subsidiaries and cloud hosting offerings.

In December 2021 Luware started a SOC2 Type II audit report project with PWC as auditor. At the time of writing Luware is in project phase 1 of 3 and the aim is to finalize the SOC2 Type II project by the end of 2022. As part of this project, the Luware Recording solution will be fully audited and tested. This certification meets a very high standard and will provide our Luware Recording customers with even more peace of mind regarding information security in the cloud.

In addition to that, our data center provider Microsoft Azure holds over 90 compliance certifications, which can be verified here: https://azure.microsoft.com/en-gb/overview/trusted-cloud/compliance/

7 Data Processing

7.1 Consent

By using the Luware Recording SaaS services, the customer agrees to Luware's general terms of use. As a Data Controller according to the GDPR, the customer engages with Luware, acting as a Data Processor, for the purpose of storing and processing data on the customer's behalf. Details on the processing principles are governed by Luware's general terms of use.

7.2 Information Held

All relevant data held by the Luware Recording system have been reviewed as being necessary to support the functionality of Luware Recording.

7.3 Third Party Processors

A part of Luware's Cloud Service is implemented on Microsoft Azure. The European Union (EU) data protection authorities, known as the Article 29 Working Party, have approved the Microsoft Azure Data Processing Agreement (DPA), assuring customers that it meets the high standards of EU data protection laws.
No other third parties are presently involved in Luware's SaaS service provision in handling data regulated by the GDPR.

7.4 Data Protection Officer

The Data Protection Officer for all Luware group companies is the General Counsel who can be contacted via compliance@luware.com.

7.5 What Data Is Being Processed

This chapter outlines the types of Personally Identifiable Information (PII) being processed by the individual Luware Cloud applications.

Data Type	Processing Details
Call Detail Records	Every call which is recorded via the Luware Recording platform creates a Call Detail Record in the backend database containing the following information: - Azure Object User ID - Azure User Email Addresses - Azure User Location/Department - Caller's phone number or SIP address - Callee's phone number or SIP address - Start/End Time of the call - Technical Call Details - Contact Center Call Details (in case of a Contact Center Call)
Call Recordings	Every call which is recorded via the Luware Recording platform creates one or multiple media files containing the following information depending on the recorded modalities: - Audio Recording of the conversation - Video Recording of the conversation - Video Recording of the screen or application share - Chat transcript of the conversation
User Details	For every user that is using the Luware Recording platform the following data is stored in the backend database:

- Azure Object User ID
- Azure User Email Addresses
- Azure User Location/Department
- UPN
- First Name
- Last Name
- E-Mail address
- SIP address (if user is recorded)
- Microsoft Azure User ID (if user is recorded)
- Telephone number (if user is recorded)

7.6 Right To Be Forgotten (Erasure)

The GDPR regulation defines the right to be forgotten for data subjects. Luware ensures that this right is adhered to and customers have the possibility to erase or anonymize the data stored about their consumers or employees in the Luware Recording solution, either by themselves or by logging a request with the Luware Support desk.

Data Type	Erasure Process
Call Recordings	Customer Administrators can leverage the standard search and replay functionality within the Luware Recording system to find and delete call recordings belonging to certain data subjects. **IMPORTANT**: It is the customer's sole responsibility to adhere to any regulatory compliance obligations if the system is leveraged for compliance recording purposes.
Call Detail Records	Customer Administrators can leverage the standard search and replay functionality within the Luware Recording system to find and delete call recordings belonging to certain data subjects. **IMPORTANT:** It is the customer's sole responsibility to adhere to any regulatory compliance obligations if the system is leveraged for compliance recording purposes.
User Details	The storage of user details is essential for the correct operation of the system. User details can only be removed from the system by deleting the user, which means that the subject will lose complete access to the system and data linked to those users will be anonymized.

7.7 Right Of Access

Luware provides the possibility to export Personally Identifiable data in a human readable data format for individual data subjects upon customer request to support@luware.com.

7.8 Right To Data Portability

Luware provides the possibility to export Personally Identifiable data in a machine-readable data format for individual data subjects upon customer request to support@luware.com.