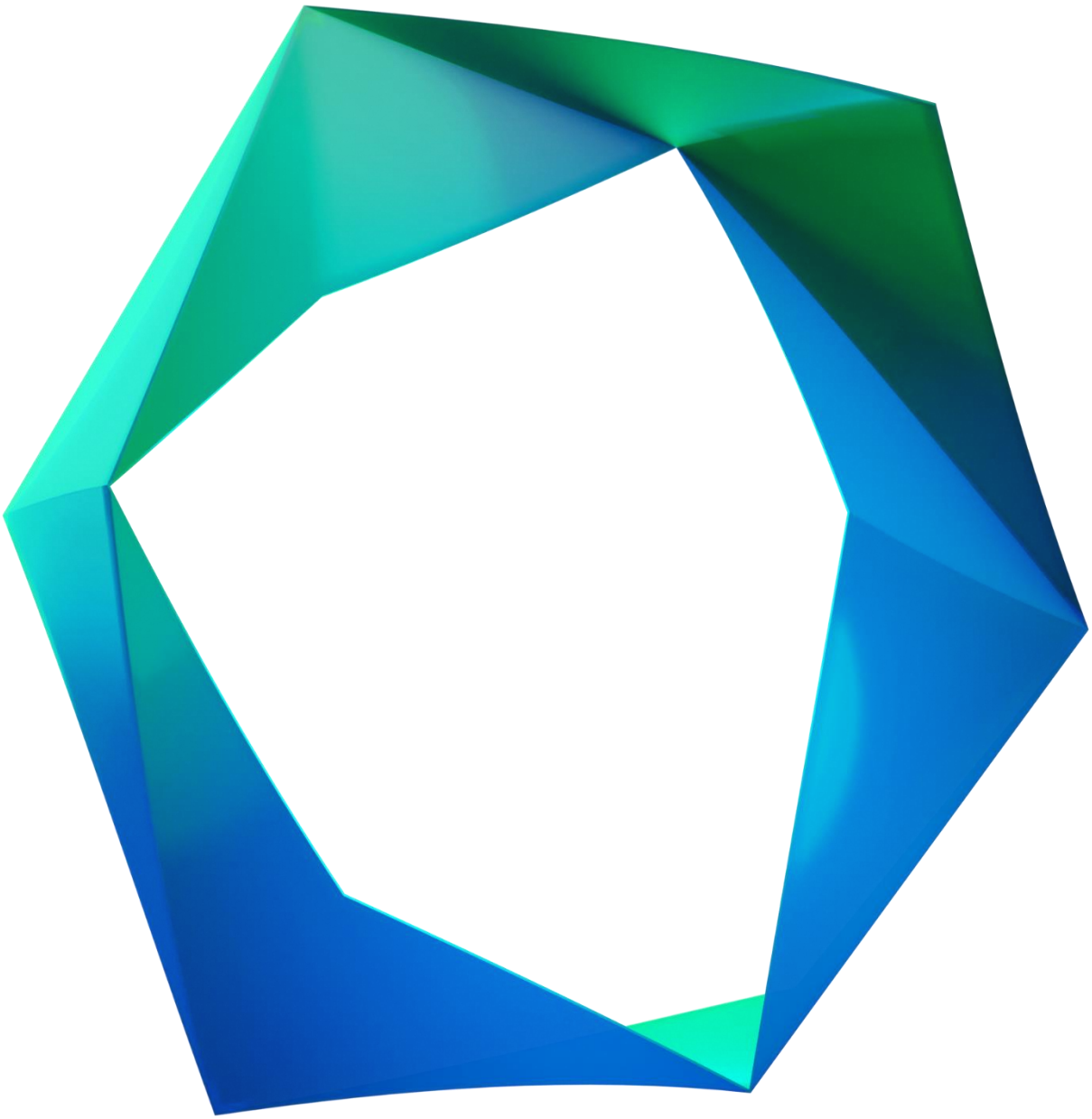


Luware
Recording

Luware Recording Security Whitepaper

Document-ID	LUREC-INFOSECWP
Version	2.2
Status	Approved by Alexander Grafetsberger
Issue Date	11.10.2024
Valid from	11.10.2024
Valid to	until replaced with newer version

Luware AG
Pfingstweidstrasse 102
CH-8005 Zürich

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

Luware

Contents

1 Introduction

Luware Recording is a cloud-based Software-as-a-Service (SaaS) product delivering communication compliance and analytics. To ensure optimal performance, security, and compliance, Luware implements a comprehensive cloud security strategy.

This document outlines the implementation of this strategy and forms an integral part of the **Luware Cloud Services Terms of Use** including the **Luware Data Processing Agreement**, as updated from time to time, or customers individual agreement with Luware, as applicable.

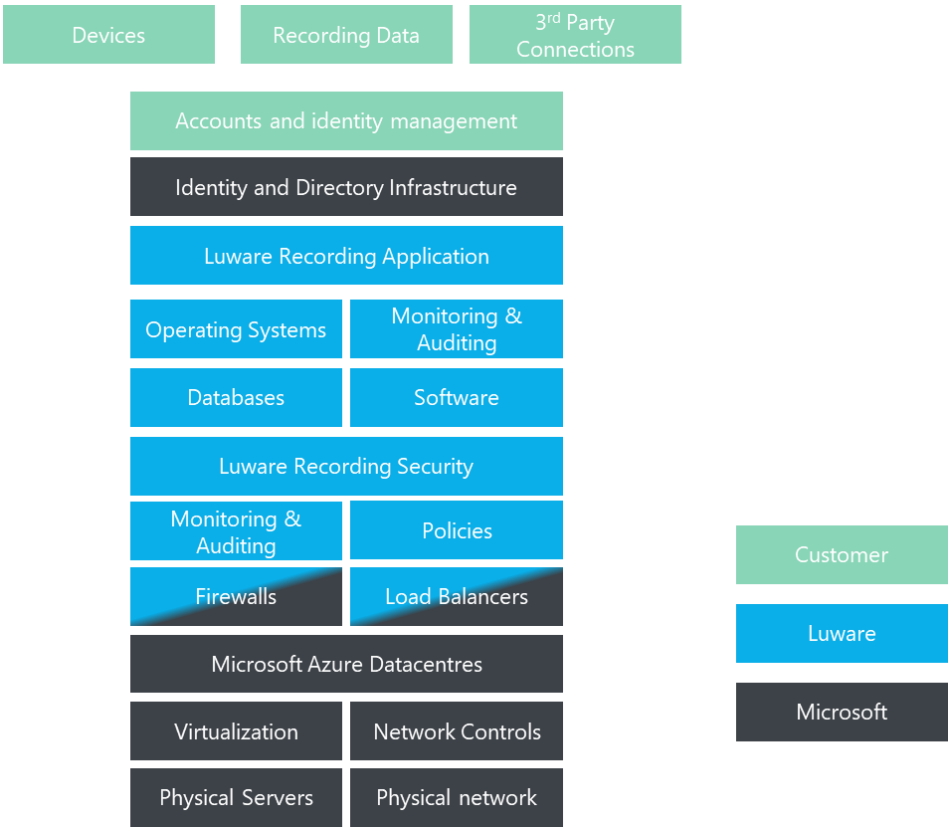
This document is aimed at our current and prospective Luware Recording customers as well as authorized technology partners.

2 Security Scope and Responsibilities

Luware Recording is a compliance recording application based on the Verint Financial Compliance product suite developed by Verint. It includes a native Speech Analytics integration with Intelligent Voice, which is optional. Luware hosts the application in Microsoft Azure datacenters with additional cloud-based services to provide the application as SaaS to customers. Multiple layers of system security are covered by Microsoft and Azure security services. This cloud security concept is called the Shared Responsibility model.

Whilst Luware manages security controls for the application layer, operating systems, network controls and server storage on the Azure platform, customers have a significant role to play in ensuring security and data protection. Customers are required to manage their own accounts and identities, devices, and third-party connections such as custom integrations. Customers are responsible for securing the data stored on Azure services in their tenant, for example recordings stored on a customer storage account. These are the areas where customers have sole control and responsibility over their data and security.

In addition, customers are responsible for ensuring that data provided from external third-party systems to Luware Recording, such as custom metadata for call recordings, can compliantly be used and stored in the Luware Recording databases for the duration of the retention period.



3 Authentication and Access

In accordance with SOC2 Type II security requirements, the Luware Recording platform is protected against unauthorized access and data breach. Some of these requirements, such as multi-factor authentication, are a fundamental building block of the Luware Recording security architecture, along with tight integration with the Microsoft's authentication platform.

Luware Recording is a licensed-user platform, where only specific, named individuals who are members of a specified group are given access to consume the service.

3.1 Customer Authentication

Customer access is authenticated with tight integration to Microsoft's global identity management platform (Microsoft Entra ID) and industry standard authentication.

3.1.1 Multi-Factor Authentication

Multi-factor authentication (MFA) is strongly recommended and can be enabled by the customer. This is achieved by leveraging Microsoft Entra multifactor authentication (MFA). Currently, Luware Recording does not support any other MFA providers.

3.1.2 Anonymous Access

Anonymous access is not supported.

3.1.3 Generic User Accounts

Generic service and administration user accounts, also known as local accounts, are not permitted. End-customer users are only granted application-specific account roles and permissions, tied to their named Microsoft Entra ID account. This ensures that customers maintain complete control over their user account security in line with their organizational requirements, such as multi-factor authentication. It also means Luware does not need to store or process user accounts passwords, with authentication being performed by the customers Microsoft tenant.

3.1.4 Shared User Accounts

Accounts shared by more than one end user are not permitted.

3.1.5 Application Accounts

Application accounts, also known as API user accounts, are provisioned on a per-request basis with enforcement of the principle of least privilege. Credentials are protected in Luware Recording conforming to industry security standards. However, customers leveraging application service accounts must also follow best practices for credential management, for example, storing passwords in an encrypted Key Vault, rotating keys regularly, limiting access and monitoring access.

In addition, Luware Recording has in place network controls further restricting API functionality against misuse and ensuring robust monitoring and audit logging.

3.1.6 User Synchronization

The Luware Recording system requires the customer to add user identities to Microsoft Entra ID groups. The group members are synchronized into the solution to assign user roles within the application. The synchronization process occurs twice daily in multi-tenant solutions and can be customized in private-tenant environments.

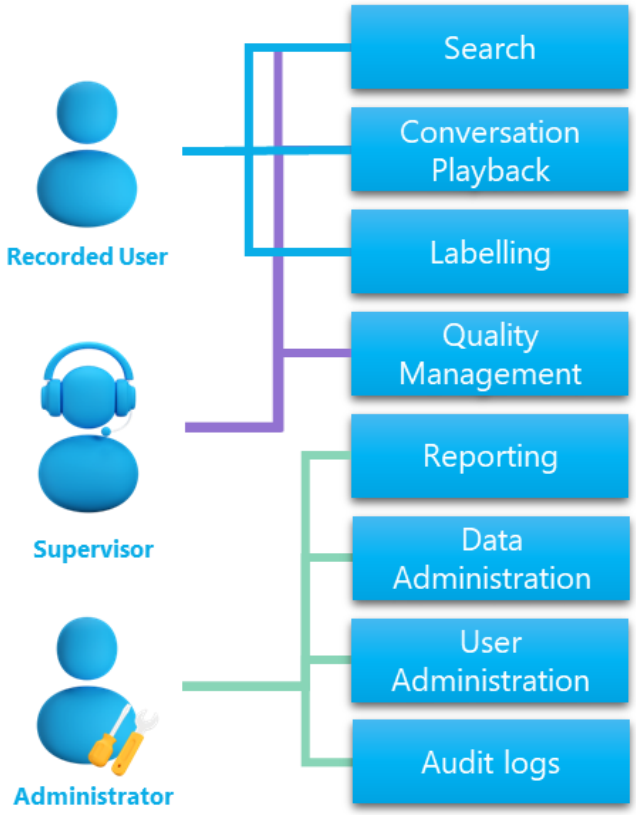
Users' password credentials are not stored in the Luware Recording system, instead the users are re-directed to authenticate with the customers Microsoft Entra identity provider and a token authenticates the users to the Luware Recording system.

3.1.7 Role Based Access Control

Luware Recording provides the customer the ability to restrict and govern the level of access rights for their end users. Pre-built roles are available and consist of:

User Roles	Description
User	An end user whose conversations are recorded in the system. This user can (if required) 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.

Each role can be configured as part of the on-boarding to the Luware Recording system. In the multi-tenant environment, a set of pre-built roles are available with minor customization options such as conversation access restrictions and disabling of features within the purchased user license, however, in private tenant environments the roles are fully customizable.



The customer performs self-administration of access to data, by leveraging the user synchronization process and Role Based Access Control policies built into Luware Recording.

3.1.8 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.

3.2 Luware Authentication

Luware system employee access is authenticated with integration to Microsoft's global identity management platform (Microsoft Entra ID), active directory and industry standard authentication.

3.2.1 Multi-Factor Authentication

Multi-factor authentication (MFA) is enforced on all Luware system accounts with Microsoft Entra ID multifactor authentication, number matching and geographic filtering enabled.

3.2.2 Anonymous Access

Anonymous access is disabled.

3.2.3 Local User Accounts

Local user accounts are permitted under a strict change control process and are reviewed on a case-by-case basis for temporary access to a customer's environment within the Web Application. This can be required in circumstances where a customer requests assistance with environment specific problems, such as, an issue with RBAC permissions within the customers environment. Created local user accounts restrictions are as follows:

- Named users only.
- Creation is disabled without approval.
- Local user accounts are audited and trigger security alerts.
- Not permitted within the reference environment.
- Not permitted with administrative RBAC permissions.

Local user accounts are not permitted for any other purpose.

3.2.4 Shared User Accounts

Accounts shared by more than one Luware system employee are not permitted.

3.2.5 Application Service Accounts

Application service accounts, also known as non-personal accounts, are required to run the underlying software. Each service account has specific functions mandated by our software supplier, for example, authentication of encrypted communication between the application components. All service accounts follow industry best practices, including:

- Principle of least privileges.
- Storing credentials in a secure key vault.
- Access only permitted with senior manager approval via a change control process using Privileged Identity Management (PIM).
- Rotating credentials regularly.
- Monitoring and Auditing.
- Regular recertification.

3.2.6 Luware System Access

This highest access level of a deployment is controlled by an Entra AD group. Only Luware employees can be assigned System Administrator roles using special Admin accounts. With these Admin accounts they can manage all tenant settings within the specified Luware Recording cluster they are granted access to.

On this level, Luware leverages the following technical security rules:

- **Principle of Least Privilege Luware**
  Luware follows the principle of least privilege and 'need to know'. Luware personnel are only allowed to access data that is necessary for them to fulfil their current roles and responsibilities.
- **Privileged account access controls**
  Luware has implemented privileged access management (PAM) for critical operational tasks requiring management approval.
- **Regular Data Access Review**
  There is a regular review process in place to assess and correct any unnecessary access privileges. This ensures that access is kept in line with role requirements.
- **Formal Access Request Process**
  If a Luware employee needs additional access beyond their current permissions, a formal access request process is followed.
- **Access is technically restricted**
  Luware implements multi-factor authentication with number matching, geographical filtering and restrictions on devices to compliant and managed devices owned by Luware. Accounts are technically restricted from logging in from countries outside the EEA and countries with a valid adequacy decision of the EU Commission.
- **Monitoring and auditing**
  Luware monitors access attempts to the Luware Recording system, including access to, web applications, server infrastructure, databases, and Azure. Alerting will detect any anomalies and inform the Luware security operations team. Audit entries for Web Application functions are kept permanently. Further details on access monitoring and auditing is able in section 3.3 Access Monitoring and Auditing.

3.3 Access Monitoring and Auditing

Detailed access logging on the customer level is leveraging Entra ID sign-in logs within the customers Microsoft Azure tenant. Luware uses Microsoft Azure Sentinel as a centralized logging solution for all Luware access activities. Event logs are retained for 16 months and are not available to customers. New accounts, changes and removals require change management approval. Access reviews are performed monthly.

Luware Recording customer administrators can have read access to the Audit Log of the Web Application. In the Audit Log customers can find a list of all access attempts, activities and changes made to the customers tenant configuration. This data is kept permanently or until the customer exits the Luware Recording contract.

4 Operational 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 to implement and maintain the baseline security standards for the Luware Cloud Services.

The security baseline is frequently reviewed and if required updated 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 to protect the Luware Recording environment from both external and internal threats. Luware Recording utilizes Microsoft's security stack, mainly its Azure Well-Architected Framework security pillar. Using this Azure framework, Luware implements the state-of-art security delivered in Azure data centers globally relying on the technology that is built with customized hardware, integrated security controls into the hardware and firmware components, and added protections against threats. As part of this approach Luware makes use of additional Azure services such as Azure Sentinel.

Luware leverages Microsoft WAF, the cloud-native service that protects Luware Recording against common web exploits, utilizing industry standard rule sets. It provides complete visibility into the environment and blocks malicious attacks.

4.3 Anti-Malware

Luware implements Microsoft Defender for Cloud which is the overarching product that protects and recommends security enhancements to components within the Luware Recording ecosystem. Defender for Cloud is integrated into all Luware's environments, this includes Defender for Endpoint (Antivirus), which is installed and active on all servers.

4.4 Patching and Roadmaps

Luware maintains a regular patch cycle to keep the Luware Recording platform and the underlying infrastructure up to date and protect it against vulnerabilities. Minor updates for bugfixes or smaller enhancements do not usually incur any downtime, however, major updates may require temporary downtime of the application. Customers are informed of maintenance windows in advance via the Luware status page. Private tenant customers will be informed via the Luware support system.

In cases of imminent threats, vulnerabilities, or system malfunction, Luware reserves the right to announce a maintenance window on short notice, or in an emergency with no notice, to ensure platform security, stability and availability.

Luware publishes a public roadmap quarterly for Luware Recording, which consists of several sprints. The roadmap planning follows feature prioritization framework based on a combination of weighted scoring and value versus complexity. Feature requests are then reviewed by our software supplier and implemented following their internal roadmap process. The published roadmap may be subject to change at Luware's discretion.

4.5 Incident Response

Luware has implemented processes 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 support desk is equipped to respond to incidents directly reported by customers.

Critical incident review is a part of Luware’s security operations policy. Incident causes and outcomes are reviewed quarterly by the Security Operations team to identify process gaps, training needs, or required documentation updates or improvements. Corrective actions are implemented as necessary.

4.6 Change Control

To minimize operational risks resulting in data exposure, service degradation or unavailability, Luware maintains a change management process that controls all non-standard changes made to a production system. All changes that impact a production system are documented, tested, and approved by a Change Approval Board prior to deployment.

Change management tools are used to reflect this process and record the multiple stages of changes including creation, design, documentation, approval, and outcome. All system employees are required to submit a change request on a change management tool, detailing any changes to in-scope platforms and systems. All changes are raised before implementation. For emergency, service-affecting situations an emergency change must be retrospectively raised and approved.

Luware implements change freeze periods for time periods determined as high risk due to peak business periods, significant events, extended public holidays or major public events. This provides Luware an opportunity to minimize the risk of intended disruptions and ensure the reliability and stability of critical services.

The change management process is reviewed annually and updated if changes are required.

4.7 Physical Security

Luware Recording is hosted in Microsoft Azure public cloud infrastructure. Microsoft takes a layered approach to physical security.

Access to the physical data center facilities is tightly controlled by outer and inner perimeters, with increasing security at each level. Security measures include perimeter fencing, security guards, locked server racks, integrated alarm systems, 24-hour video surveillance in the operations center, and multi-factor access control. Only authorized personnel are granted access to Microsoft's data centers. Logical access to Microsoft 365 infrastructure, including customer data, is prohibited from within Microsoft data centers.

Microsoft's Security Operations Centers use video surveillance along with integrated electronic access control systems to monitor data center sites and facilities. Cameras are positioned to effectively cover the facility perimeter, entrances, shipping bays, server cages, interior aisles, and other sensitive security points. As part of their layered security posture, any unauthorized entry attempts detected by the integrated security systems generate alerts to security personnel for immediate response and remediation.

These layers include:

- **Access request and approval:** access must be requested prior to arriving at the datacenter. A valid business justification for the visit must be presented.
- **Visitor access:** all visitors that have approved access to the data center are accompanied by a member of staff.
- **Facility's perimeter:** before entering the data center, visitors must go through a well-defined access point.
- **Building entrance:** the data center entrance is staffed with security officers who have undergone training and background checks. These security officers routinely patrol the data center and monitor the videos of cameras inside the data center.
- **Inside the building:** 2FA is required to move throughout the data center. Once identity is validated, access to an area to which access has been pre-approved is granted.
- **Data center floor:** visitors are only allowed onto the floor that they've been approved to enter. A full body metal detection screening is mandatory. Additionally, video cameras monitor the front and back of every server rack.

Additional 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

Luware's Legal and Compliance team regularly reviews Microsoft Azure's SOC2 Type II audit reports including any bridge letters. This ensures adequate measures can be taken should a control activity fall short of the expected quality standards and may materially impact Luware's security operations.

4.8 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 a pre-defined security framework with regular reviews and a Joiner/Mover/Leaver process. Our Joiner/Mover/Leaver and User review processes are closely aligned with our SOC2 control processes.

5 Data Privacy & Processing

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

5.1 Data Locations

At the time of writing, the Luware Recording Multi-Tenant offering is available in the Microsoft Azure regions Switzerland and Germany. The data location of the Luware Recording Private-Tenant offering is defined in the individual customer agreement.

5.1.1 Switzerland

The Swiss Luware Recording Multi-tenant environment, also referred to as MT-CH, is hosted in Microsoft Azure Switzerland North (Zurich) as a primary datacenter and Azure Switzerland West (Geneva) as the secondary datacenter.

5.1.2 Germany

The German Luware Recording Multi-tenant environment, also referred to as MT-DE, is hosted in Microsoft Azure Germany West Central (Frankfurt) as a primary datacenter and Germany North (Berlin) as the secondary datacenter.

5.1.3 Private-Tenant

Luware Recording private-tenant environments can be deployed to Azure regions available based on the customers' requirements. For a list of available Azure regions use the below link (Some regions may not be publicly listed due to available resources):
https://azure.microsoft.com/en-gb/explore/global-infrastructure/geographies

5.2 Data Subjects

When using Luware Recording, Luware processes personal data of licensed recorded users, supervisors or administrators utilizing Luware Recording services, and any participants involved in call recordings captured by the system (e.g. caller ID).

5.3 Type of Data Processed

The table Data Types - Processing, Erasure and Retention outlines the types of personal data being processed when using Luware Recording.

5.4 Data Subject Rights

Luware adheres to the GDPR principles of the Right to be Informed, the Right of Access, the Right of Erasure, the Right of Restricting Processing, the Right to Object and the Right to withdraw Consent. In some cases, these rights may be limited due to applicable law. Details are set out in our Luware Data Processing Agreement and Luware Privacy Policy.

Should Luware receive a data subject request on behalf of a customer being the data controller, the request is forwarded to the controller. In some instances, customers can change or delete their data themselves, however this is not the case for all requests. Therefore, if instructed by the customer as the data controller, Luware acts upon requests which are to be sent via the support (https://helpdesk.luware.cloud/) channel.

Data Types - Processing, Erasure and Retention outlines each data subject and the corresponding erasure process.

5.5 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 30 days after retention expires.

5.6 Data Retention

Data within the Luware Recording application is retained for the purpose of system operation and reporting. Customers are solely responsible for the correctness, accuracy, and lawfulness of information they put in or store in their Luware Recording environment.

The data retention period for conversation recordings is configurable on a user group level and it is the sole responsibility of the customer or partner to ensure they meet any legal or regulatory requirements by configuring the necessary retention.

The retention period per data type can be found in Data Types - Processing, Erasure and Retention.

5.7 Third Party Processors

Microsoft Ireland Operations Limited.
Luware Recording is implemented on the Microsoft Azure cloud environment. Microsoft Azure complies with all EU guidelines, in particular GDPR. This includes the implementation of Standard Contractual Clauses. Microsoft has implemented the Processor-to-Processor clauses (P2P SCCs) included in Module III of the SCCs. By having Microsoft entities sign the P2P SCCs as both data importer and exporter, Microsoft confers a direct benefit on the customer by assuming increased compliance responsibilities for data transfers.

Amongst numerous other certifications and reports, Microsoft is audited against SOC 2 Type II principles and has an ISO 27001 certification.

Luware Affiliates.
Services related to Luware Recording such as support, maintenance and development are performed from Luware affiliate locations in Switzerland, the UK and the EU. Both Switzerland and the UK hold a valid adequacy decision by the EU Commission. No other third parties are directly involved in the provision of services to customers. Internal Business Infrastructure. Please refer to the Luware Privacy Policy for more information

5.8 Group Data Protection Officer

The Data Protection Officer for all Luware group companies can be contacted via compliance@luware.com. Applicable references must be made according to the Luware Privacy Policy.

5.9 Data Protection

5.9.1 Protection of Data at Rest

All backend databases containing sensitive data (including but not limited to; configuration data, reporting data, conversation metadata records, user data, audit logs) are encrypted using transparent database encryption (AES256). Luware uses an internal Luware certificate authority to generate certificates for encryption of the data at rest.

Any customer data stored at rest within the Luware Recording environment underlies the following security measures.

- Physical Access Control
- Logical Access control: only named individuals with the necessary access privileges can access the logical data storage.

Recording media and metadata files which are stored on customer supplied storage accounts should be encrypted using a customer supplied encryption certificate meeting Luware specified standards or a standard Luware AES-256/SHA-256. Luware recommends customers bring their own certificate to provide an additional layer of security and control over their call recording data. Customer supplied encryption certificates are securely stored in the local machine certificate stores, or in a Luware-hosted Key Vault. Access to the Key Vault requires privileged identity management approval.

The protection of data at rest matrix can be found in Data Protection – Protection of Data at Rest.

5.9.2 Protection of Data in Transit

Any information transmitted between Luware Recording and the end customer via public networks is encrypted using strong public key encryption.

Traffic transmitted between Microsoft and the Luware Recording system is encrypted using strong public key encryption. Microsoft signs all communications to Luware Recording using a secure JWT token generated by OpenID ensuring only messages from Microsoft are processed. All other inbound traffic is unauthenticated and dropped by the service.

The protection of data at rest matrix can be found in Data Protection – Protection of Data in Transit.

5.9.3 Data Segregation

Multi-Tenant

All customer configuration, user, audit history and recording metadata is stored and maintained in the shared Luware Recording Cloud infrastructure, which is segregated logically at a tenant level to keep the data demarcated, private and secure.

Recordings conversations created in the Luware Recording platform are stored directly in customer provided Storage and hence are fully segregated. Recording data uploaded to the customer provided storage account is solely the responsibility of the customer.

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, user, audit history 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 at a tenant-level to ensure segregation of customer data.

Recordings conversations created in the Luware Recording platform are stored directly in customer provided storage and hence are fully segregated. Recording data uploaded to the customer provided storage account is solely the responsibility of the customer.

5.9.4 Data Redundancy

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 regularly backup our application server’s configuration and their associated configuration databases.

Database transaction logs are backed up every 15 minutes, differential backups are performed daily, and full backups are performed weekly. These backups are retained for up to 30 days for the sole purpose of disaster recovery, before being purged. All data backups are encrypted.

6 Business Continuity Management

Businesses of varying 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.

6.1 Business Continuity Program

Luware has implemented a Business Continuity Program (BCP) specifically for Luware Recording. Via the risk management process, resources that are critical to maintain operation including people, processes, and technology have been identified. As part of this program, plans are created for each critical business function pertaining to the operation and support of the Luware Recording platform.

The established BCPs are internal documents and processes that outline the procedures, detailed steps and all necessary information for the continuation and restoration of critical business processes and systems in the event that various resources become unavailable including the loss of premises, infrastructure, human resources, data and equipment. These documents and processes are confidential and can therefore not be shared with external parties for reasons of data security, confidentiality, and protection of intellectual property.

BCPs are reviewed, tested, and approved by the respective teams and coordinated by the respective team-leads in conjunction with Security Operations. All BCP plans are tested at least on an annual basis, but where applicable more often (for example, during system upgrades, patch cycles or backup/restore exercises). Relevant gaps, learnings and findings are tracked to resolution in Luware's process management system.

6.2 Risk Management

Luware conducts an annual group-wide risk assessment to identify and evaluate key risks to general business operations and services. By assigning subject matter experts to each risk category, we ensure that evaluations are thorough and transparent enabling Luware's Group Management and the Board of Directors to take informed decisions for the organization.

We continually monitor emerging risks, changes to existing categorizations and risk ratings and the status of risk mitigation plans. The process is owned and overseen by Legal and Compliance.

6.3 Security Incident Management

Luware follows a defined Incident Management process conforming to SOC2 security standards. The process provides guidelines, assigns roles and responsibilities and information on how to respond to and communicate any security incidents and system failures.

An incident management tool is used to log security incidents. The category and priority of a security incident is determined as part of the incident management process. Security incidents are verified by Security Operations monthly and assigned to the applicable incident owner who evaluates the root cause and assigns remedial actions. Implementation of actions are tracked by Security Operations.

The health status of the system is generally available on the Luware status page. The incident team coordinates and analyses the situation and reports frequently on the status. Where customers are affected, they will be informed immediately.

The CISO reviews the security incident management process annually and if required makes necessary changes.

6.4 Incident Response

Luware has developed incident response protocols that include triggers and escalation criteria based on the severity of an incident. This consists of processes for activating plans, assembling recovery teams, and making critical decisions to deal with and remediate any incidents.

The Incident Response Team consists of selected Luware employees who act as the Incident Manager for any incidents that occur. All team members can be the first point of contact in the case of an incident, regardless of the platform or product. This process has been designed to acknowledge that the “most ideal” person to act as the Incident Manager at the point of identification may not be available, and time is crucial in our response. Therefore, the first available person in this team accepts the responsibility to act as the Incident Manager until such a time as a more appropriate Incident Response Team Member becomes available and a handover can take place.

Incidents may span over long time periods, and this is likely to include evenings, night times and weekends, therefore having the ability to ensure multiple people are skilled and trained to take over the management of any individual incident allows Luware to ensure that a handover can take place to ensure full focus and attention to the incident.

6.5 Crisis Management

A crisis management plan is in place to govern a global response following an incident impacting Luware. The plan includes the assembly of a core team of leaders and procedures for fast decision making and timely communications.

6.6 Third-Party Assurance

Luware evaluates the business continuity capabilities of key vendors and third parties through a vendor assessment process overseen by Legal and Compliance. Key vendors such as Microsoft, are assessed quarterly against their performance by the Supplier Relationship Manager. Any actions resulting from such assessments are tracked until resolved.

7 High Availability and Disaster Recovery

7.1 Definition

Luware adopts the following definition of Business Continuity derived from the ISO 22301 standard: “The capability of the business to continue the delivery of products and services at acceptable, predefined levels following a business disruption.”

7.2 Resilient System Architecture

Luware Recording is built on Microsoft Azures platform and is optimized to leverage the availability, scalability, and redundancy that the Azure cloud provides. The services are deployed in paired Azure regions and utilize multiple datacenters within those regions using availability groups, protecting against geographic threats such as loss of connectivity, power, or other common location specific failures.

7.2.1 Call Recording Resiliency

The Luware Recording software has in-built self-healing and seamless state restoration. In the event a service on a recording server fails, it is automatically detected and restored within 60 seconds by an independent service watcher. If the media capture service fails, the director service will automatically transfer the capture of the recording to another recording server in the same Azure region. Any partial captures on the server are saved and uploaded to the database and data at rest storage location on automatic service restart.

All Luware Recording deployments, unless otherwise agreed with private tenant designs, are deployed with N+X recording servers. The number of available recording servers within an Azure region is dependent on load sizing calculations. All recording servers within a single Azure region are configured to failover to any other recorder in the same Azure region in the event of an infrastructure or software failure. For Multi-tenant Switzerland, they are also configured to failover to the secondary active Azure region.

In private tenant deployments and certain multi-tenant regions the solution can also be deployed with 2N recording. This provides an additional layer of resiliency between Microsoft Teams and the receiving recording servers as two requests are sent to different Azure regions simultaneously and handled independently. In the event an inbound request fails to an Azure region, Microsoft will not fail-close a call recording if the second Azure region responds to the request in a timely manner.

7.2.2 Fail-Close for Compliance Recording

For customers capturing recordings for compliance purposes, it is highly recommended that the Microsoft Teams Compliance Policy is configured as fail-close. This means that, in the unlikely scenario that an API fails to be received by Luware Recording, fails to be processed in a timely manner or is missing critical information from Microsoft, the Microsoft Teams conversation will be dropped rather than failing to record. For customers that are capturing for quality or require capture on critical communications lines, the policies can be deployed as fail-open. This would mean that if the recording fails for any reason, the Teams call will not be dropped.

7.2.3 Web Application Resiliency

The Web Application service within Luware Recording is deployed in with N+1 resiliency across two geographically dispersed Azure regions. Azure Front Door is utilized to geographically distribute traffic between both active regions. An Azure Web Application Gateway with enabled WAF rulesets provides additional layer of security and serverless scalability to ensure the stability and availability of the Web services.

The Web Application service has in-built self-healing, which is controlled by an independent service watcher, which will restore the service within 60 seconds. Web Application Gateways automatically scale to handle unexpected traffic increases.

7.2.4 Database Resiliency

All configuration, user, auditing and recording metadata is stored within a highly available database that is replicated in near real time across two azure regions. In the event a primary database server fails, the secondary will automatically become the primary with no impact to data processing.

The recording services are designed to work independently of database access, so in the event a database is unavailable on the primary and secondary database servers, the recording services continue to function by caching required application data for recording, maximizing data retention and minimizing any compliance impact.

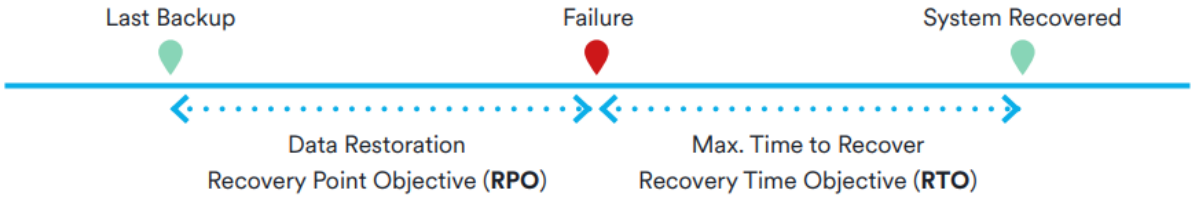
7.3 Backup and Restore Strategy

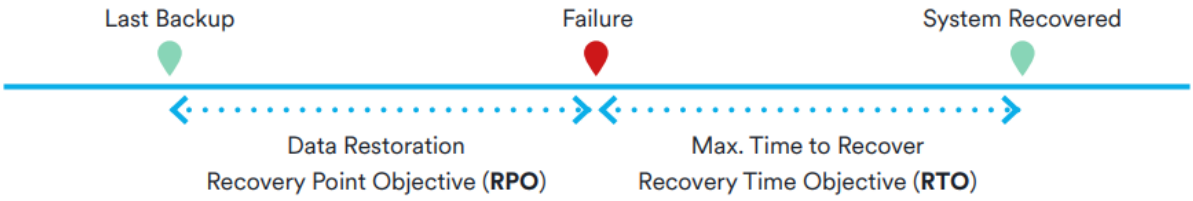
Luware Recording production databases are backed up to the secondary Azure region to protect availability in the event of a location-specific catastrophic event. Luware also retains a full backup copy of production data in a remote location significantly distant from the location of the primary operating environment but within the same geographical region/jurisdiction. Database transaction logs are backed up every 15 minutes, differential backups are performed daily, and full backups are performed weekly.

All recording media and metadata files are stored independently on the data at rest storage account and could be restored if required, which provides an additional layer of resiliency in the very unlikely event of a major disaster.

7.3.1 RPO and RTO Backup and Restore Strategy

Due to the resilient design as well as the chosen infrastructure and backup and restore strategy, recovery times after the failure of key Luware Recording components can be kept to a minimum. The below recovery point objective (RPO) and recovery time objective (RTO) are defined for the Luware Recording service.





Measure	Description	Data Type	Objective
Recovery Point Objective (RPO)	A measure of tolerance of data loss in terms of time, i.e. the duration of time for which data loss is acceptable	Data at Rest i.e. SQL	Up to 15 mins loss initially but can mitigate this data loss by importing the customers data back into SQL from the data at rest storage location.
		Data in Transit i.e. Ongoing Recording	No loss due to 2N+X model with fail close Microsoft Teams compliance recording policy.
Recovery Time Objective (RTO)	A measure of how much time can elapse before full recovery, i.e. the maximum length of time within which a business	Data in Transit i.e. Recording	For single regional outage 0 RTO. For multi-regional rebuild of the recording services up to 2 hours.

	process must be restored after a disruption		

Backups are stored on Azure storage accounts. These storage accounts are configured with geographically redundant storage (GRS) and an immutable blob policy. GRS replicates the data to a linked Azure region within the same geographical zone.

Access to the storage accounts is monitored and only approved for privileged system employees. Backups therefore have the least access authorization according to the “Least Privilege principle”. Backups are stored separately from the actual data and can be archived, for example, through a media break. Each environments backups are monitored by Luware’s monitoring platform. Any errors are alerted on, and corrective action is taken. Changes to the recovery process are validated by carrying out the change and restore process.

All recovery testing is reviewed by a third party and documented in a comprehensible manner, in particular whether the maximum recovery time is achieved or not.

8 Further Organizational Measures

8.1 General IT Infrastructure

Critical core IT Infrastructure for the day-to-day operations of Luware including e-mail, telephony, CRM and ERP systems are designed in a resilient fashion with most of those systems being cloud-hosted or pure SaaS solutions. This ensures that in a disaster scenario where business premises or a single data center is lost, Luware is still able to fully operate its business remotely. The necessary security measures are in place to ensure the safety and security when working remotely, including MFA and access to sensitive data via corporate VPN.

8.2 People

Luware operates with a geographically dispersed workforce with locations in Switzerland, United Kingdom and the EU (Germany, Poland and Spain). Luware ensures that system critical roles have substitutes in place with the necessary skills and expertise to take over the day-to-day operations in case of a local emergency. Processes, procedures, and systems of mission critical roles are designed in a way that they can be executed remotely without having physical access to Luware premises.

8.3 Background Checks

Luware performs background checks on every System Employee within the company as permitted by local law. The range of background checks performed depends on the role the person holds as well as the level of access they need to perform their daily work. Background checks may include but are not limited to criminal history checks, adverse financials checks, education verification as well as employment history verification.

8.4 Security Awareness

All Luware employees undergo regular security awareness training starting with the onboarding process followed up by regular refresher courses and online trainings during the year. Based on the role as well as the level of access an employee needs for their daily work, the level and depth of security awareness training differs. Training topics include secure coding, scam and fraud awareness, general secure working practices, risk awareness, compliance and regulatory adherence training.

8.5 Basic principles for Luware User Accounts

Luware has two types of user accounts: the “employee account” and the “privileged account”. For system administrative tasks, users will be provided with a privileged account. Each user account is personal, non-transferable, and can only be used by the assigned employee.

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.

Luware enforces multi-factor authentication for all types of user accounts.

Passwords must be created according to Luware’s password policy, which includes complexity rules. Passwords for privileged users require a higher level of protection. Therefore, it is prohibited to use pins with those accounts. Access to Luware IT infrastructure is technically restricted to compliant and managed devices owned by Luware. For applications that manage confidential or secret information, access must be regulated by individual user permissions.

8.6 Audit Reports and Certifications

Luware Recording is annually audited by an independent external third party on adherence to Security Organizational Controls (SOC) 2 Type II trust service criteria relating to Security.

Additionally, Luware AG is certified according to ISO 27001 and ISO 9001 standards. Any processes related to these standards are rolled out group wide including all affiliate locations. Luware annually conducts an internal as well as an external audit regarding adherence to these standards.

8.6.1 Security Organizational Controls 2 - Type II

A SOC 2 Type II report is an internal controls report capturing how a company safeguards customer data and how well those controls are operating. This report is based on the AICPA’s Trust Services Criteria (TSC) and is currently conducted by PWC. It provides an independent, third-party assessment of the controls that an organization has implemented with regards to the audited TSC. Luware is audited within the scope of the anticipated trust service criteria for Security.

Details of the SOC 2 Type II report are strictly confidential and are provided to selected customers upon request and subject to signature of a separate non-disclosure agreement. Luware will provide a letter of confirmation of the report to customers upon request which is to be issued with the responsible sales representative.

8.6.2 Microsoft 365 Certified

Luware's Microsoft 365 Certified application status demonstrates that the company has met the rigorous standards set by Microsoft for data privacy, security, and compliance. This certification involves passing assessments across 113 controls, which are categorized into Application Security, Operational Security, and Data Handling and Privacy. This status confirms Luware's commitment to being a trusted application provider.

Evidence of certification can be found on learn.microsoft.com.

8.6.3 ISO 27701

ISO 27001 provides guidelines to manage the confidentiality, integrity, and availability of information assets by assessing and controlling associated risks. It outlines requirements for an information security management system (ISMS), encompassing policies, procedures, and controls to safeguard data like personal, intellectual, and financial information. It aids in risk identification, data breach prevention, and effective response to security incidents by managing information security risks.

Luware AG’s current ISO 27001 certification is provided to customers upon request via the responsible sales representative.

8.6.4 ISO 9001

ISO 9001 is an international standard that sets out the requirements for a quality management system (QMS) within an organization. It provides a framework for organizations to establish, maintain and continually improve data security and privacy practices requiring organizations to identify, assess and manage risks related to information security. This includes implementing appropriate controls to protect against unauthorized access, theft, loss, damage, or destruction of information.

Luware AG’s current ISO 9001 certification is provided to customers upon request via the responsible sales representative.

9 Appendix

9.1 Data Types - Processing, Erasure and Retention

Data Type	Processing details	Erasure	Retention
Call Detail Records	Recordings captured by the Luware Recording platform create a Call Detail Record (CDR) in the database containing the following data: ▪ Users name ▪ Users UPN ▪ User Object ID ▪ User Email Address ▪ User Location and/or Department ▪ Any other user data synced at the request of the customer. ▪ Participants name, phone number, SIP address or User Object ID. ▪ To phone number or SIP address ▪ Participants IP Addresses ▪ Conference Participants name, email address and/or phone number ▪ Meeting subject, organizer id, organizer display name, tenant id. ▪ Participants device ▪ Start and end time of the recording ▪ Duration of the recording ▪ Direction of the recording ▪ Conversation modality ▪ Forward reasons ▪ Nimbus service line ▪ Nimbus agent details ▪ End of retention date ▪ Storage location ▪ Encryption certificate name ▪ Assigned labels Technical call details Instant Message recording additionally store: ▪ Instant Message Transcript	Automatically deleted at the configured end of retention date. If retention date is not set, data can be deleted from the Web interface. **GDPR Erasure Request**: A ticket must be created with Luware support to remove the retention from the recording in the database. The customer can then manually remove the call recording from the platform using the standard delete functionality. **IMPORTANT**: It is the customer's sole responsibility to adhere to any regulatory compliance obligations if the system is leveraged for compliance recording purposes.	Date specified by customer

Data Type	Processing details	Erasure	Retention
	▪ Animated GIFs, Stickers, Praises, and other rich content ▪ File attachment name ▪ File Attachment content type ▪ File attachment URL ▪ File attachment storage location		
Call Recording Metadata Files	Conversation recordings, except, Instant Messages, generate a metadata (.xml) file that is uploaded to the data at rest storage location. This file contains: ▪ Users name ▪ Users UPN ▪ User Object ID ▪ User Email Address ▪ User Location and/or Department ▪ Any other user data synced at the request of the customer. ▪ Participants name, phone number, SIP address or User Object ID. ▪ To phone number or SIP address ▪ Participants IP Addresses ▪ Conference Participants name, email address and/or phone number ▪ Meeting subject, organizer id, organizer display name, tenant id. ▪ Participants device ▪ Start and end time of the recording ▪ Duration of the recording ▪ Direction of the recording ▪ Conversation modality ▪ Forward reasons ▪ Nimbus service line ▪ Nimbus agent details ▪ End of retention date ▪ Storage location ▪ Encryption certificate name ▪ Assigned Labels ▪ Technical call details	Automatically deleted at the configured end of retention date. If retention date is not set, data can be deleted from the Web interface. **GDPR Erasure Request**: A ticket must be created with Luware support to remove the retention from the recording in the database. The customer can then manually remove the call recording from the platform using the standard delete functionality. **IMPORTANT**: It is the customer's sole responsibility to adhere to any regulatory compliance obligations if the system is leveraged for compliance recording purposes.	Date specified by customer

Data Type	Processing details	Erasure	Retention
Call Recording Media Files	Conversation recordings, except, Instant Message, generate a metadata (.xml) file that is uploaded to the data at rest Azure location. This file contains: ▪ Audio data of all parties in a recorded conversation ▪ Video data of all parties in a recorded conversation ▪ Screen share data of any user who shares the screen with a recorded user. Instant Message File attachment recording additionally stores: ▪ File attachments including contents.	Automatically deleted at the configured end of retention date. If retention date is not set, data can be deleted from the Web interface. **GDPR Erasure Request**: A ticket must be created with Luware support to remove the retention from the recording in the database. The customer can then manually remove the call recording from the platform using the standard delete functionality. **IMPORTANT**: It is the customer's sole responsibility to adhere to any regulatory compliance obligations if the system is leveraged for compliance recording purposes.	Date specified by customer
User Data	Licensed users who have access to the Luware Recording system will have data stored in the database of the environment they are onboarded to. This data is used for system sign-on, role-based access control, audit logs, call metadata and system functions such as upload policies: ▪ Users name ▪ Users UPN ▪ User Object ID ▪ User Email Addresses ▪ User Location and/or Department ▪ User Group membership and history ▪ User role assignment ▪ User time zone ▪ User Language ▪ Any other user data synced at the request of the customer.	Required for role-based access control to call recording data its advised that user data remain in the system. User data can be deleted at any time but will have the below impact: Recordings will no longer be assigned to a user and may not be searchable using user or group-based access control. New call recordings will not be assigned to the user. The user will not be able to access the Luware Recording system. Audit logs will not be associated to the user.	Customer contract duration + 30 days.
Reporting Data	The data combines call detail records, user data, configuration data and audit data to provide aggregated views. The	Generated reports can be deleted from the Web interface. Data processing after download from	Generated reports are deleted from the Luware Recording

Data Type	Processing details	Erasure	Retention
	reports are downloadable from the Web interface and any data transferred out of the system is no longer the responsibility of Luware.	the system is not Luwares responsibility.	system every 30 days.
Audit logs	All activities performed on the web interface are stored in the database. It stores data linked to on-boarded users such as: ▪ Users name ▪ Users UPN ▪ User Object ID ▪ User Email Address ▪ User sign in and out events including date, time, device and IP address. ▪ Search queries ▪ Playback events ▪ Download events ▪ Export events ▪ Labelling ▪ Role changes ▪ Group changes ▪ Extension changes ▪ Configuration actions performed on the web interface, including date, time, action, and result. ▪ Any other functionality enabled during on-boarding	Audit logs must be permanently kept for privacy and security.	Customer contract duration + 30 days.
Application Logs	Temporary storage of application logs is required for the purpose of incident and problem troubleshooting. Data processed includes user data, configuration data, call detail records, call recording metadata and media files: ▪ Users name ▪ Users UPN ▪ User Object ID ▪ User Email Address ▪ User Location and/or Department ▪ Any other user data synced at the request of the customer. ▪ Participants name, phone number, SIP address or User Object ID.	Application logs are automatically removed from the system when specified buffer limit overflows. Requests for log deletion are not supported.	Up to 30 days

Data Type	Processing details	Erasure	Retention
	▪ To phone number or SIP address ▪ Participants IP Addresses. ▪ Conference Participants name, email address and/or phone number. ▪ Meeting subject, organizer id, organizer display name, tenant id. ▪ Participants device. ▪ Start and end time of the recording. ▪ Duration of the recording. ▪ Direction of the recording. ▪ Conversation modality. ▪ Forward reasons. ▪ Nimbus service line. ▪ Nimbus agent details. ▪ End of retention date. ▪ Storage location. ▪ Encryption certificate name. ▪ Assigned Labels. ▪ Technical call details.		
Configuration Data	The customer's tenant is configured during the on-boarding or during operational changes. A history of all changes is permanently stored in the audit log.	Application logs cannot be deleted from the system.	Customer contract duration + 30 days
Speech Analytics Database Records	Speech analytics if enabled, will process a combination of user data, configuration data, call detail records, call recording metadata and media files to generate the below new data: Language and dialect detection ▪ Speech-to-text. ▪ Transcription text. ▪ Translation text. ▪ Diarization. ▪ Generative summary of conversation. ▪ Emotional and semantic analysis. ▪ Speech characteristics. ▪ Keyword analysis.	Speech analytics database records are stored in the Luware Recording database. ▪ Data is not stored in the speech analytics software. ▪ Data is not available to other customers. ▪ Data is not processed by any other party. ▪ Data is not used to improve the model. ▪ Data is not available to 3rd party products or services. Automatically deleted at the configured end of retention date. If retention date is not set, data	Date specified by customer

Data Type	Processing details	Erasure	Retention
		can be deleted from the Web interface. **GDPR Erasure Request**: A ticket must be created with Luware support to remove the retention from the recording in the database. The customer can then manually remove the call recording from the platform using the standard delete functionality. **IMPORTANT**: It is the customer's sole responsibility to adhere to any regulatory compliance obligations if the system is leveraged for compliance recording purposes.	
Speech Analytics Transcript Files	Speech analytics if enabled, will process a combination of user data, configuration data, call detail records, call recording metadata and media files to generate the below new data: ▪ Language and dialect detection. ▪ Speech-to-text. ▪ Transcription text. ▪ Translation text. ▪ Diarization. ▪ Generative summary of conversation. ▪ Emotional and semantic analysis. ▪ Speech characteristics. ▪ Keyword analysis.	Speech analytics transcript files are stored in the customers storage account. ▪ Data is not stored in the speech analytics software. ▪ Data is not available to other customers. ▪ Data is not processed by any other party ▪ Data is not used to improve the model. ▪ Data is not available to 3rd party products or services. Automatically deleted at the configured end of retention date. If retention date is not set, data can be deleted from the Web interface. **GDPR Erasure Request**: A ticket must be created with Luware support to remove the retention from the recording in the database. The customer can then manually remove the call recording from the platform	Date specified by customer

Data Type	Processing details	Erasure	Retention
		using the standard delete functionality. **IMPORTANT**: It is the customer's sole responsibility to adhere to any regulatory compliance obligations if the system is leveraged for compliance recording purposes.	

9.2 Data Protection – Protection of Data at Rest

Location	Data Types	Protective Measures
Azure Microsoft SQL Database	▪ Call Detail Records ▪ User Data ▪ Reporting Data ▪ Audit Logs ▪ Configuration Data ▪ Speech Analytics Database Records	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.
Customers Storage Account	▪ Call recording Metadata File ▪ Call Recording Media File ▪ Speech Analytics Transcript Files	Recordings which are stored on customer supplied storage are encrypted using standard Luware AES-256/SHA-256 encryption or with customer supplied encryption certificate.
Azure Storage Account (Database backups)	▪ Call Detail Records ▪ User Data ▪ Reporting Data ▪ Audit Logs ▪ Configuration Data ▪ Speech Analytics Database Records	The backend databases are backed up onto an Azure Storage Account which is encrypted with transparent database encryption (TDE) using AES-256/SHA-256 encryption according to industry standards. The backup is encrypted using Microsoft Backup encryption using different AES-256/SHA-256 asymmetric keys. The Azure storage account is encrypted using 256-bit AES encryption.
Azure Virtual Machines	▪ Application Logs ▪ Reporting Data	Virtual machines are encrypted with Azure storage encryption using server-side encryption (SSE) with 256-bit AES.

9.3 Data Protection – 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.
Teams Recording	Traffic transmitted between Microsoft and the Luware Recording system is encrypted using strong public key encryption. Traffic is encrypted using SSL certificates issued by DigiCert Inc. DigiCert SHA2 Secure Server CA supporting the TLS 1.2 protocol and AES256 encryption with SHA2 signature. Microsoft signs all communications to Luware Recording using a secure JWT token generated by OpenID ensuring only messages from Microsoft are processed. All other inbound traffic is unauthenticated and dropped by the service.
Customers Storage Account	Traffic transmitted between Luware Recording and the customers Azure storage account uses the Microsoft Managed Network. Luware recommends using a Luware supplied Azure private endpoint to secure the connectivity. Web traffic to the Azure Storage Account should be enabled for secure transfer and TLS 1.2 minimum, which enforces HTTPS only transfer using industry standards (The customer is responsible for configuring security on the Azure Storage Account). Customers using a storage account from another vendor or cloud provider, such as AWS S3, will have their data transferred over the public internet in an encrypted format via HTTPS with TLS 1.2. It is the customer's responsibility to ensure that security standards and guidelines are properly configured on customer supplied storage accounts to ensure data security.
Azure Key Vault	Luware Recording securely stores all new customers call encryption and signing certificates within an Azure Key Vault. Existing customers certificates will be migrated to Key Vaults as part of a migration project. The Luware Recording service retrieves the certificate on certain events, such as service start, playback, export and then at a predefined interval to check validity. All communication between the application and Azure Key Vault is encrypted using TLS to ensure data integrity and confidentiality during transmission. Authentication and authorization are managed through the OAuth 2.0 protocol, leveraging Azure Entra ID for secure access control.
System API's	Any system APIs 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.

9.4 Application Permissions

In the Azure AD, there are two types of permissions:

- **Delegated permissions** are used in the delegated access scenario. These are permissions that allow the application to act on a user's behalf. In this access scenario, a user has signed into a client application. The client application accesses the resource on behalf of the user. Delegated access requires delegated permissions. Both the client and the user must be authorized separately to make the request.
- **Application permissions** are used in the app-only access scenario. These are permissions that allow an application to act on its own behalf. In this access scenario, the application acts on its own with no user signed in. Application access is used in scenarios such as automation and backup.

For more information about these two types of permissions, you can refer **to this overview**.

Luware Recording requires rights within the Microsoft 365 environment being recorded to allow for functions such as, user logging into the Web application, Bot recording a call and pulling metadata to make a recording decision. These permissions are only used for the Luware Recording solution and without them the solution cannot function.

A detailed description of the Microsoft Application Permissions can be found on the Graph permission reference website as well as on the Microsoft Entra API permission description website.

In any case, the use of the application permissions follows the principle of least privilege. A detailed description of all permissions by products can be found in our Knowledge Base.

9.5 Links

Description	Link
Luware Privacy Policy	Privacy Policy | Luware
Luware Status Page	Status Page | Luware
Luware Knowledge Base	Knowledge Base | Luware
Luware Support	Support | Luware
Azure Physical Security	Physical Security of Azure Data Centers – Microsoft Azure
Shared Responsibility Model	Shared responsibility in the cloud – Microsoft Azure

9.6 Glossary

Term	Description
Anonymous Access	Access to a system with no authenticated credentials.
Application Accounts	Typically an account not assigned to an individual used for system access, such as an API account.
Business Continuity Program	A business continuity program is an organization's strategic and procedural framework designed to ensure the continuation of critical operations during and after a significant disruption, such as a natural disaster or cyber-attack.
Call Detail Records (CDR)	Call Detail Records (CDRs) are data records produced by the recording system that document the details of communication between individuals or groups of users.
Data at Rest	Data at rest refers to any data that is stored on a device or in a storage system and is not actively being moved or processed. It includes all types of data stored, such as databases, files, and backups, residing on physical or cloud storage.
Data In Transit	Data in transit refers to any data that is being transferred between devices or networks over the internet or another type of network. This can include data moving from a local storage device to a cloud storage service, data being sent between users through the internet, or any other data actively moving through a network. Typically any data cached for less than 60 seconds is considered data in transit.
Entra ID	Entra ID, part of Microsoft's Entra suite of identity and access management solutions, is designed to provide secure, seamless authentication and access control for users across various applications and services. It enables organizations to implement and manage digital identities, ensuring that the right individuals can access the right resources at the right times for the right reasons
Environment	A logically segregated environment within the system.
Intelligent Voice	Intelligent Voice is a software-based product used for speech analytics (https://intelligentvoice.com/)
ISO 27001	ISO 27001 is an international standard that outlines the requirements for an information security management system (ISMS). It provides a systematic

	approach for organizations to manage sensitive company information so that it remains secure, encompassing people, processes, and IT systems by applying a risk management process.
ISO 9001	ISO 9001 is an international standard that specifies requirements for a quality management system (QMS)
Microsoft Azure	Microsoft Azure is a cloud computing service created by Microsoft for building, testing, deploying, and managing applications and services through Microsoft-managed data centers. It provides a wide range of cloud services, including those for computing, analytics, storage, and networking. Users can pick and choose from these services to develop and scale new applications, or run existing applications, in the public cloud.
Multi-Factor Authentication (MFA)	Multi-factor authentication (MFA) is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction.
Multi-Tenant	A multi-tenant system consists of multiple environments hosted on the same infrastructure. Each environment is logically segregated within the database.
Private-Tenant	A private-tenant system consists of one environment hosted on infrastructure dedicated to that environment. The database is dedicated to a single environment.
Recovery Point Objective (RPO)	Recovery Point Objective refers to the maximum amount of data that can be lost after a recovery from a disaster, failure, or comparable event before data loss will exceed what is acceptable to an organization 1. In other words, it is the time period between two data backups
Recovery Time Objective (RTO)	Recovery Time Objective refers to the maximum amount of time that an organization can tolerate for systems and applications to be unavailable after a disaster or disruption. It is the time period within which an IT resource must fully recover from a disruptive event. The RTO is an essential component of a Disaster Recovery Plan (DRP) and is part of a Business Impact Analysis. The RTO is usually determined by the criticality of the application, with more critical applications requiring shorter RTOs than those that are less critical.
Shared Responsibility Model	The Shared Responsibility Model is a framework that outlines the responsibilities of cloud service providers and customers for securing every aspect of the cloud environment. This includes hardware, infrastructure, endpoints, data, configurations, settings, operating system (OS), network

	controls and access rights. It describes the responsibility of each participant of the scenario.
Shared User Account	A user account shared by more than one individual.
SOC2 Type II	SOC 2 Type II is an audit procedure that evaluates the effectiveness of a service organization's controls over time, focusing on security, availability, processing integrity, confidentiality, and privacy of a system. It requires evidence of how effectively these controls are operated over a defined period.
Software as a Service (SaaS)	SaaS is a software licensing model that allows users to access programs via the Internet on a subscription basis using external servers.
User	An individual within an organization
Verint Financial Compliance (VFC)	Verint Financial Compliance is a software based product offered by Verint to capture and analyze recordings from various communication platforms. (https://www.verint.com/financial-compliance/)
Web Application Firewall (WAF)	A Web Application Firewall (WAF) is a security solution designed to monitor, filter, and block malicious traffic to and from web applications. By inspecting HTTP traffic, a WAF can prevent attacks stemming from web application security flaws, such as SQL injection, cross-site scripting (XSS), and file inclusion, ensuring the protection of web applications from a wide array of threats.

10 Change History

Version	Date	Editor	Changes
2.2	11.10.2024	Joshua Wood	▪ 7.3.1 Updates to clarify RPO and RTO.
2.1	12.08.2024	Joshua Wood	▪ Minor branding updates ▪ 8.6.2 Microsoft 365 Certified Added. ▪ 5.9.1 Protection of data at rest updated. ▪ 10 Change History added. ▪ Updated references to customer “Azure storage” to “storage” as other vendors are now supported. ▪ 9.3 Data Protection – Data In Transit updated.
2.0	28.03.2024	Joshua Wood	▪ Branding updates ▪ Authentication and access updated. ▪ Operational Security updated. ▪ Data Privacy, processing and protection updated. ▪ Business Continuity Management updated. ▪ Further organizational measures updated. ▪ Data Types added to appendix. ▪ Application permissions added to appendix.
1.2	19.01.2023	Alexander Grafetsberger	▪ Branding updates. ▪ Audit Reports & Certifications added. ▪ Data processing updates. ▪ GDPR updates.
1.1	31.01.2022	Alexander Grafetsberger	▪ Branding updates.
1.0	22.05.2020	Alexander Grafetsberger	▪ Original release.

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