Luware

Information Security White Paper

Luware
Nimbus

Luware AG
Pfingstweidstrasse 102
CH-8005 Zürich

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

Document-ID	LUNIM-INFOSEC
Version	1.1
Status	Approved by Michael Jakob
Issue Date	14.03.2022
Valid from	14.03.2022
Valid to	13.03.2023

Table of 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 Cloud 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 Cloud environment for our customers.

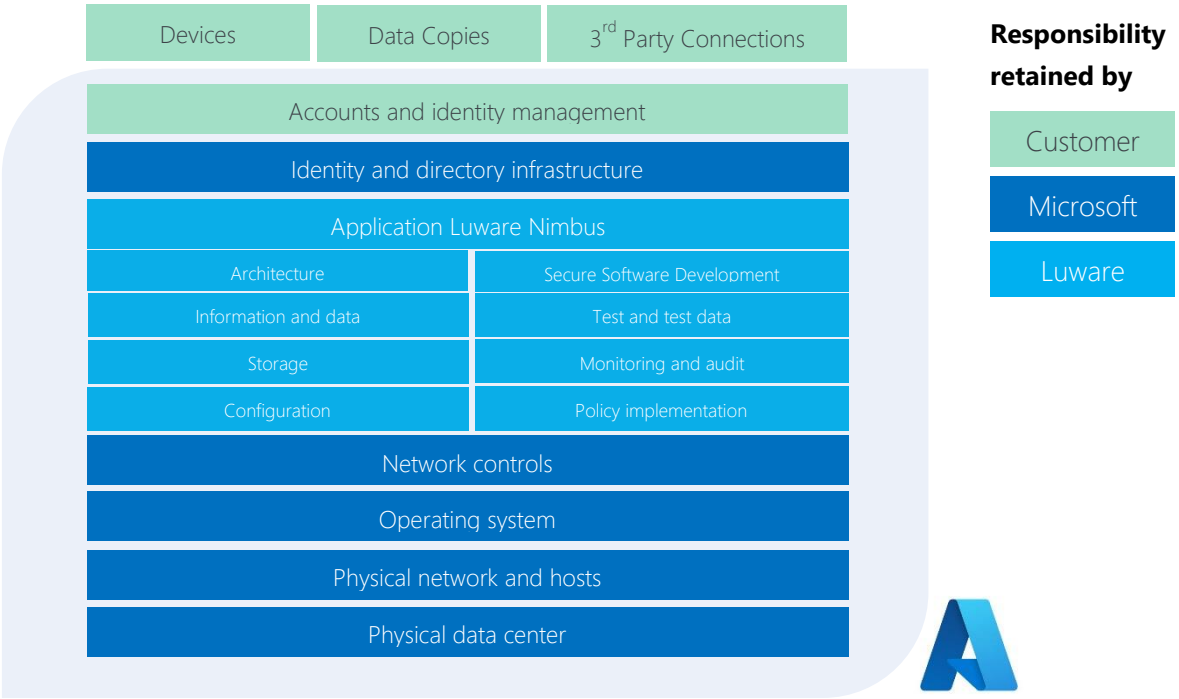
2 Scope

2.1.1 Audience

Luware Nimbus Customers, Technology Partners and Prospects.

2.1.2 SaaS Security Scope

Luware Nimbus is a Microsoft Teams Application developed on the extend model and hosted in the Microsoft Azure Cloud. Multiple layers of the system security are entirely covered by Microsoft and Azure Security Services. This cloud security concept is called Shared Responsibility.
Luware is responsible for security controls of the entire application layer and also related choices and configuration on the Azure platform. Customers are encouraged to pay attention to their own responsibility which is account and identity management, devices, data copies and 3rd party connections such as custom integrations.



3 Data Privacy

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

3.1 Data Locations

3.1.1 Switzerland North 01

The Luware Nimbus Instance CHNO_01 (https://portal.luware.cloud) is hosted in the Microsoft Azure Data center located in Switzerland, with the primary data center being Microsoft Azure Switzerland North (Zurich) and the secondary data center (DR, backup location) being Microsoft Azure Switzerland West (Geneva).

3.1.2 Germany West Central 01

The Luware Nimbus Instance DEWE_01 (https://portal.dewe-01.luware.cloud) is hosted in the Microsoft Azure Data center located in Germany, with the primary data center being Microsoft Azure Germany West Central (Frankfurt) and the secondary data center (DR, backup location) being Microsoft Azure Germany North (Berlin).

3.1.3 United Kingdom

The Luware Nimbus Instance UKSO_01 (https://portal.ukso-01.luware.cloud) is hosted in the Microsoft Azure Data center located in the UK, in the data center Microsoft Azure UK South (London) and a geo-redundant Nimbus Instance UKWE_01 (https://portal.ukwe-01.luware.cloud) beeing in the data center Microsoft Azure UK West (Cardiff).

3.2 Data Access Types

3.2.1 Luware Administrative Data Access

Luware implements the principle of least privilege and 'need to know' to minimize the risk of data exposure. Luware personnel are only authorized to access the data they necessarily and reasonably must have access to, 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 executive management approval.

3.2.2 Partner Access

Luware technology and integration partners receive access to the system for the management of their customer's Nimbus environment. Data access, administrative roles and privileges are managed by the partner administrators. It's the partner's sole responsibility to maintain and control the access scope within their own organization and for their customer's tenants.

3.2.3 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 Nimbus platform is a licensed-user only system, where only specific, named individuals or members of a licensed team 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). Please refer to Self-service password reset policies - Azure Active Directory | Microsoft Docs for more information about the underlying Azure AD password policies.

3.3.2 Anonymous Access

Anonymous access is not supported.

3.3.3 Multi-Factor Authentication

Multi-factor authentication (MFA) can be enabled by the 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, or their technology partner, performs self-administration of access to data by leveraging predefined Role Based Access Control policies provided by the Luware Cloud products.

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, the Luware Nimbus hosted service 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	Description
User	Any Nimbus user that acts as part of a Service Team. Users have no access to the Admin panel, mainly focusing on daily Usage of Nimbus instead. Nimbus users are directly synchronized from Microsoft Teams.
Service Administrator/ Team Owner	Any Nimbus user that acts as an owner of a Service Team. Team Owners acting as service administrator in addition. They can change their respective Service Settings and Manage Resources (both own + provided by Tenant Admin). Team Owners also may install Power BI to access and evaluate Historical Reporting Data directly from the reporting backend.
Tenant Administrator	Administrates Services and User Administration. Also manages Resources to be available to all Services under the respective Tenant.
Partner Administrator	Administrates Tenant Administration, Services and User Administration. Also manages Resources to be available to all Services under the respective Tenant.

3.3.8 Access Monitoring

Detailed access logging is enabled, security event logs collect at least privileged and non-privileged user access activities, authorized and unauthorized access attempts, credentials management operations, system exceptions, administrator activities. Such logs are retained after the specified data retention period (See 3.5 Data Retention). Customers will not be given access to sensitive security logs

3.4 Data Segregation

All customer configuration and reporting data (including voice messages) is stored and maintained in the shared Luware Nimbus Cloud infrastructure which is segregated logically by the individual Luware Nimbus applications in order to keep the data demarcated, private and secure.

3.5 Data Retention

Data within the Luware Nimbus application is retained for the purpose of system operation and reporting. Data Retention policies are in place to ensure Data isn't kept any longer than necessary to service its purpose. The following Data Retention policies are in place:

Data Type	Retention Period
Aggregated Reporting Data (Call detail records, caller information, call treatment and call journey details)	24 months

Voicemail Records	24 months
Configuration Data	customer contract duration + 30 days
Application Logs (Temporary storage of internal application logs)	30 days We temporarily store internal application logs to help our support engineers troubleshoot the performance and operation of application components.

The defined data retention period cannot be customized. Customers who want to keep the reporting data longer can archive the data into their own infrastructure via the odata interface.

3.6 Data Backup

To ensure service resilience Luware runs a highly available application infrastructure. Due to the dynamic nature of our applications, our data bases are fully backed up daily and additional incremental back-ups are run every 30 minutes. These backups are stored in a geographically separate location within the same region/jurisdiction of azure. The backups are retained for up to one day and kept, until replaced by a new one.

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 one day 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 established on industry standards and regular internal infosec 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 Nimbus infrastructure.

4.2 Threat Prevention

Luware implements policies, tools, and technology in order to protect the Luware Nimbus environment from both external and internal threats. These include, but are not limited to, 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 to keep the Luware Nimbus platform 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 to ensure platform security, stability, and availability.

4.4 Secure Software Development

Luware has implemented Secure Software Development practices including, but not limited to, mandatory security awareness trainings for software developers, secure design principles and coding practices, automatic security auditing for every new software build. This also includes OWASP Top 10 vulnerability checks and Whitesource 3rd party library validation as well as a large array of automated tests prior to production deployment. The Secure Software Development process is reviewed on an annual basis and updated as needed.

4.5 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 Nimbus 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.

4.6 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.

4.7 Physical Security

The Luware Nimbus services are hosted in data centers of Microsoft Azure. It's within the services providers responsibility to restrict physical access and ensure maximum security to the cluster infrastructure.

4.8 Logical Security

Access to systems and data within the Luware Nimbus offering 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 in to 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.

4.9 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 XChaCha20-Poly1305-IETF encryption according to industry standards.
General Data Storage	Any customer data stored at rest within the Luware Nimbus environment underlies the following security measures. **Physical Access control** – https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security **Logical Access control** – only named individuals with the necessary access privileges can access the logical data storage.

4.10 Protection of Data In Transit

Data Type	Protective Measures
Web Applications	Any information transmitted between the Luware Nimbus and the end customer via public networks is encrypted using strong encryption. Luware leverages SSL certificates issued by "Let's Encrypt Authority X3" supporting the TLS 1.2 protocol and AES256 encryption with SHA2 signature.
System API's	Any system API's are secured with a token-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 Nimbus and the end customer via public networks is encrypted using strong encryption. Luware leverages SSL certificates issued by "Let's Encrypt Authority X3" supporting the TLS 1.2 protocol and AES256 encryption with SHA2 signature.

5 Business Continuity

Businesses of varying sizes, across the globe, rely on the Luware Nimbus Solution to ensure effective communication across their organization. Due to the nature of the offered service, 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

This chapter provides an overview of the Luware Nimbus Business Continuity measures.

5.1 Business Continuity Program

Luware has implemented a Business Continuity Program specifically for our Luware Cloud Services, which is managed by our Information Security Officer in conjunction with the Luware Cloud Operations Team. As part of this program, Business Continuity Plans (BCPs) are created for critical business functions, pertaining to the operation and support of the service. 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. BCPs are created and maintained in the Luware internal Process Management System and are classified as confidential. These documents and procedures cannot be shared with external parties for reasons of data security, confidentiality, and protection of intellectual property.
For transparency towards our customers, this document contains high-level information regarding the essential parts of our Business Continuity Program. The plans in general include System Operations, Technical Support and vital business operations that support BCPs. BCPs are reviewed, exercised, and approved by the respective teams coordinated by the respective team-leads or BCP-coordinators in conjunction with our Information Security Officer.

5.2 Business Impact Analysis

Luware performs an annual business impact analysis (BIA) to understand business requirements, set recovery objectives and identify gaps and areas of vulnerability. The requirements and objectives set during the BIA inform the strategy analysis and planning processes. Risks identified during the BIA are reported to the Information Security Officer as well as the respective Business Process Owners for prioritization and are tracked through a formal mitigation process documented in the Luware Internal Process Management System.

5.3 Risk Management

In conjunction with the annual business impact analysis (BIA), Luware conducts a risk assessment to identify and evaluate key risks facing the operation and provision of our services. Luware is continually monitoring emerging risks, changes to existing categorizations and risk ratings and the status of risk mitigation plans. The process is owned and overseen by Luware's Group Management committee in collaboration with the Luware compliance team.

5.4 Approach

Luware has implemented a prioritized top-down approach in order to ensure the business continuity program and its processes, warrants the prompt recovery of the services we deliver to our customers; including the teams, functions and resources that support their delivery.

5.5 Standards and Certification

Luware AG holds the ISO 9001 and ISO 27001 certification which requires business continuity to be implemented. In order to deliver the high-quality service our customers expect from a state of the art compliance solution, Luware went a step further and built our entire program to be aligned to and based on the principles of ISO 22301, the International Business Continuity Management Systems standard (BCMS). 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/. The bespoke certifications have been obtained by Luware AG headquarters in Switzerland. All processes are rolled out group wide.
Luware AG is currently in the course of the SOC 2 Type II audit report project. Once the audit report is obtained, SOC 2 Type II will apply to all Luware's cloud-based services, including Luware Nimbus.

5.6 Incident Response

Luware has developed incident response protocols that include triggers and escalation criteria based on the severity of an incident. This includes processes for activating plans, assembling recovery teams, and making critical decisions.

5.7 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.

5.8 Third-party assurance

Luware evaluates the business continuity capabilities of key vendors and third-parties through a vendor assessment process overseen by the Information Security officer and compliance according to the ISO certifications. This process in continually monitored and improved. We want to assure our customers that we only trust best of breed vendors to be involved in providing our services.

5.9 BCP Testing

All BCP plans will be tested at least on an annual basis, but where applicable more often (for example, during system upgrades, patch-cycles or backup/restore exercises). All gaps, learnings and findings are tracked to resolution in our process management system.

6 High Availability and Disaster Recovery

6.1 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."
The ultimate aim is to provide our customers and partners the highest level of confidence in our ability to provide our products and continue our business. Maintaining this level of resilience requires continual effort, as our business and the environment that we operate in changes every single day. This chapter describes at a high level the Business Continuity Measures in place to ensure the above.

6.2 Resilient System Architecture

Luware Nimbus is built on a highly scalable Microservice Architecture which is configured and optimized to be resilient against service outages with features such as automatic healing and seamless state recovery, auto-scale and auto-restart in case of a failure. Due to the distributed nature of a Microservice based application, failures of single components only have minor effect on the stability of the general system. Luware Nimbus services run in the primary data centers of the Azure regions outlined in the Data Location chapter of this document. In case of a full data center outage, the services will be restored to the secondary Azure data center within region and service can resume within the RTO.

6.3 Database resilience

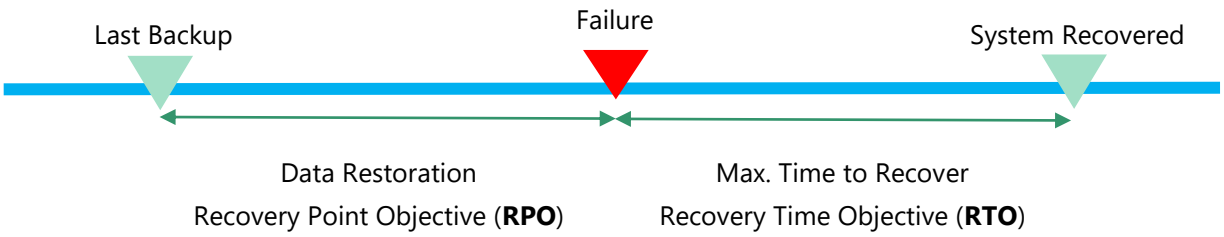
Critical application data is stored in databases that are replicated in near real-time across multiple database instances within the same Azure data center. In case of failure of the primary database or the full data center, the application will be failed over to a database backup in the secondary data center within region.

6.4 Backup and Restore

Production databases are backed up to the secondary Azure Data Center within region to protect the availability of Luware's service 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. Full backups are saved to this remote location at least once per day and incremental backups are saved in 30 minute intervals. Luware tests backups at least twice yearly to ensure they can be successfully restored.

6.5 RPO and RTO

Due to the resilient design as well as the chosen infrastructure and Backup and Restore strategy, recovery times after the failure of the Luware Nimbus systems can be kept to a minimum. Please find below the RPO and RTO defined for the Luware Nimbus 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 (configuration and reporting data)	Up to 30 minutes based on the last available transactional database backup
Recovery Time Objective (RTO)	A measure of how much time can elapse before full recovery; that is, the maximum length of time within which a business process must be restored after a disruption.	Any	Up to 120 minutes for a full system failover to secondary Azure Data Center.

6.6 Data Centers

Luware has chosen Microsoft Azure Data Centers to run the Luware Nimbus Services for their security, resiliency and connectivity, which all play a vital role in the context of business continuity and disaster recovery. Microsoft Azure Data Centers are designed and built in a way that strictly controls physical access to the areas where our customer's data is stored. Microsoft understands the importance of protecting their customer's data and is committed to helping secure the data centers that contain it. Detailed and up-to-date information regarding facilities, premises and physical security of Microsoft Azure Data Centers can be found at https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security.

6.7 People

Luware operates with a geographically dispersed workforce with locations in Switzerland, the UK and the EU (Germany and Poland). 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 or outbreak. Processes, procedures, and systems of all mission critical roles are designed in a way that they can be executed remotely without having physical access to Luware premises.

6.8 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 would be lost, Luware would still be able to fully operate its business remotely. The necessary security measurements are in place to ensure safety and security when working remotely, including Multi-Factor authentication, access to sensitive data is only via corporate VPN etc.

6.9 Coronavirus (COVID-19) Measures

In light of the global Coronavirus pandemic and its impact on Businesses and Individuals, Luware has taken the necessary steps to ensure a friction-less operation of day-to-day business. Our geographically diverse teams have always ensured resilient operations, yet we recently updated our operations approach throughout our business — including relationships to vendors and other thirdparty service providers — specifically to ensure that our services will remain up and running in a climate where the health of our employees is less predictable. We identified critical processes and teams within each of our business functions and created a contingency plan for each. The new plans include a staffing backup plan for each of our geographic locations, including primary, secondary, and tertiary contacts for the team. Due to the fact, that Luware's workforce is highly mobile and distributed, our business infrastructure is based on tools and technologies which can be used remotely and are not relying on any Luware premises.

7 Organizational Measures

7.1 Background Checks

For the peace of mind of our customers and ourselves, Luware performs background checks on every new-hire within the company as permitted by local law. The range of background checks performed depends on the role the person holds within the company 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.

7.2 Security Awareness

All Luware stuff undergoes regular security awareness training starting with the onboarding process followed up by regular refresher courses and online trainings. 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 etc.

8 Data Processing

8.1 Consent

By using the Luware Nimbus 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.

8.2 Information Held

All relevant data held by Luware's Nimbus SaaS have been reviewed as being necessary to support the functionality of Luware's Nimbus SaaS products.

8.3 Third Party Processors

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.

8.4 Data Protection Officer

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

8.5 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 routed via the Nimbus platform creates a Call Detail Record in the backend database containing the following data: • Caller's phone number or SIP address • Start/End Time of the call • Routing Decisions • User(s) who answered the call • Voice messages left from a caller on a Nimbus service
User Details	For every user that is created in the Nimbus platform the following data is stored in the backend database: • Firstname • Lastname • DisplayName • E-Mail address • UPN / SAM account name
Transfer History	The history of transfer targets per caller ID is stored in the Attendant Console. Dependent on the call type, this can either be: • Office 365 ID of the transfer target

- SIP-address of the transfer target
- Phone number of the transfer target

8.6 How Is Data Beeing Processed

Any data transmitted between Luware Nimbus and the end customer via public networks is encrypted and communication of this data is secured over TLS. Any system API's are additionally secured with a token-based authentication system. (See 4.10 Protection of Data In Transit).

8.7 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 Nimbus SaaS solution either by themselves or by logging a request with the Luware Support desk depending on the solution.

Data Type	Erasure Process
Call Detail Records	For the purpose of consistent reporting, Call Detail Records cannot be erased, but they can be fully anonymized. For this purpose, please raise a request via support@luware.com.
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 the complete access to the system and Reporting data linked to those users will be anonymized.
Transfer Targets	Please raise a request via support@luware.com in order to request a deletion of Transfer Targets.

8.8 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.

8.9 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.

/end