A-LIGN

A-LIGN.com

Type 2 SOC 3

Prepared for:
ContractPod Technologies Inc

Year:
2025

LEAH

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

October 1, 2024 to September 30, 2025

Table of Contents

SECTION 1

ASSERTION OF CONTRACTPOD TECHNOLOGIES INC. MANAGEMENT

ASSERTION OF CONTRACTPOD TECHNOLOGIES INC. MANAGEMENT

January 23, 2026

We are responsible for designing, implementing, operating, and maintaining effective controls within ContractPod Technologies Inc.'s ('Leah' or 'the Company') AI Based Contract Management Solutions Services System and Copilot Services System throughout the period October 1, 2024 to September 30, 2025, to provide reasonable assurance that Leah's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality, and Privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA, *Trust Services Criteria*, and Leah's compliance with the commitments in its Statement of Privacy Practices. Our description of the boundaries of the system is presented below in "ContractPod Technologies Inc's Description of Its AI Based Contract Management Solutions Services System and Copilot Services System throughout the period October 1, 2024 to September 30, 2025" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period October 1, 2024 to September 30, 2025, to provide reasonable assurance that Leah's service commitments and system requirements were achieved based on the trust services criteria. Leah's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in "ContractPod Technologies Inc's Description of Its AI Based Contract Management Solutions Services System and Copilot Services System throughout the period October 1, 2024 to September 30, 2025".

Leah uses Microsoft Azure ('Azure' or 'subservice organization') to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Leah, to achieve Leah's service commitments and system requirements based on the applicable trust services criteria and Leah's compliance with the commitments in its Statement of Privacy Practices. The description presents Leah's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Leah's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve Leah's service commitments and system requirements based on the applicable trust services criteria and Leah's compliance with the commitments in its Statement of Privacy Practices. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of Leah's controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period October 1, 2024 to September 30, 2025 to provide reasonable assurance that Leah's service commitments and system requirements were achieved based on the applicable trust services criteria and Leah's compliance with the commitments in its Statement of Privacy Practices, if complementary subservice organization controls and complementary user entity controls assumed in the design of Leah's controls operated effectively throughout that period.

Anurag Malik
_____

Anurag Malik
President/CTO
ContractPod Technologies Inc

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: ContractPod Technologies Inc.

Subject

We have examined Leah's accompanying assertion titled "Assertion of ContractPod Technologies Inc. Management" (assertion) that the controls within Leah's AI Based Contract Management Solutions Services System and Copilot Services System were effective throughout the period October 1, 2024 to September 30, 2025, to provide reasonable assurance that Leah's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Confidentiality, and Privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*, and Leah's compliance with the commitments in its Statement of Privacy Practices.

Leah uses Azure to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Leah, to achieve Leah's service commitments and system requirements based on the applicable trust services criteria and Leah's compliance with the commitments in its Statement of Privacy Practices. The description presents Leah's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Leah's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Leah, to achieve Leah's service commitments and system requirements based on the applicable trust services criteria and Leah's compliance with the commitments in its Statement of Privacy Practices. The description presents Leah's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Leah's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Leah is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Leah's service commitments and system requirements were achieved. Leah has also provided the accompanying assertion (Leah assertion) about the effectiveness of controls within the system. When preparing its assertion, Leah is responsible for selecting, and identifying in its assertion, the applicable trust services criteria, for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system, and complying with the commitments in its Statement of Privacy Practices.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria and its compliance with the commitments in its Statement of Privacy Practices. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.
Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements

- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Independence and Ethical Responsibilities

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

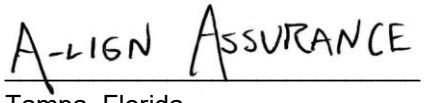
In our opinion, management's assertion that the controls within Leah's AI Based Contract Management Solutions Services System and Copilot Services System were suitably designed and operating effectively throughout the period October 1, 2024 to September 30, 2025, to provide reasonable assurance that Leah's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of Leah's controls operated effectively throughout that period.

The SOC logo for Service Organizations on Leah's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of Leah, user entities of Leah's AI Based Contract Management Solutions Services System and Copilot Services System during some or all of the period October 1, 2024 to September 30, 2025, business partners of Leah subject to risks arising from interactions with the AI Based Contract Management Solutions Services System and Copilot Services System, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

This report is not intended to be, and should not be, used by anyone other than these specified parties.



Tampa, Florida
January 23, 2026

SECTION 3

CONTRACTPOD TECHNOLOGIES INC'S DESCRIPTION OF ITS AI BASED CONTRACT MANAGEMENT SOLUTIONS SERVICES SYSTEM AND COPILOT SERVICES SYSTEM THROUGHOUT THE PERIOD OCTOBER 1, 2024 TO SEPTEMBER 30, 2025

OVERVIEW OF OPERATIONS

Company Background

Leah was founded in 2012 with the mission to make the end-to-end contract management system more accessible to corporate in-house legal teams and with the aim of eliminating data entry and paralegal related work for the corporate department.

Laying original claim to the phrase ‘by lawyers for lawyers,’ the platform was created as an affordable, out of the box, end-to-end tool. It features repository, contract generation, and third-party review functionality. Since going live in 2015, the platform has been helping legal departments at large-scale corporations across the globe digitally transform their contract management function.

Description of Services Provided

Leah provides complete functionality covering the full spectrum of contract management, from creation through to signature and lifecycle management.

This functionality includes:

- Front door requests to the legal team
- Storage in a highly searchable central repository with Optical Character Recognition (OCR) capability
- Detailed reporting and analytics
- Contract creation and assembly
- Access to Leah, an artificially intelligent contract analyst
- Electronic (E)-signature by Docusign
- Automated workflows and approval process management
- Robust alerts and reminders for key dates and tracking obligations

Leah provides access to Leah, an artificially intelligent contract analyst. Built on technologies including OpenAI, Zuva AI, International Business Machines (IBM) Watson, and other proprietary AIs, Leah will permanently transform contract creation and automation by reviewing, interpreting and analyzing contracts for key dates and an extensive set of standard key obligations. This information is automatically populated into the contract record, providing substantial savings in manual data entry, as well as the time taken to review contracts.

Principal Service Commitments and System Requirements

Leah designs its processes and procedures related to its AI Based Contract Management Solutions System to meet its objectives for its contract management services. Those objectives are based on the service commitments that Leah makes to user entities, the laws and regulations that govern the provision of contract management services, and the operational and compliance requirements that Leah has established for the services. The contract management services of Leah are subject to regulations, as well as privacy and security laws and regulations in the jurisdictions in which Leah operates.

Security commitments to user entities are documented and communicated in agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the AI Based Contract Management Solutions System that are designed to permit users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Use of encryption technologies to protect customer data both at rest and in transit.

Leah establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Leah's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the AI Based Contract Management Solutions System.

Components of the System

Infrastructure

Primary infrastructure used to provide Leah's AI Based Contract Management Solutions Services System and Copilot Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Servers and Infrastructure	Azure	Application hosting and processing
Intrusion Prevention System (IPS)	Azure Intrusion Prevention Threat Scanning	Screens and alerts on network traffic based on "malicious Internet Protocol (IP) addresses and domains" as assessed by feeds from the Microsoft Threat Intelligence service
Firewalls	Windows Firewall Advanced Security	Filters inbound and outbound traffic out of the network
Security Information and Event management (SIEM)	Microsoft Sentinel	For monitoring purposes
Virtual Private Network (VPN)	Azure VPN	VPN services
Structured Query Language (SQL) Server	Windows	Database

Software

Primary software used to provide Leah's AI Based Contract Management Solutions Services System and Copilot Services System includes the following:

Primary Software	
Software	**Purpose**
Leah®	In-scope application for contract management
Microsoft Office 365	Office Productivity
Visual Studio 2019	Development Studio
Docusign	E-Signature
Azure Cognitive Search	Fluid Search Engine
Aspose Portable Document Format (PDF)	Document Convertor

Primary Software	
Software	**Purpose**
Aspose Word	Document Convertor
Aspose for DotNet	Document Convertor
Microsoft.NET	Development Framework
C#	Development Language
IBM Watson AI	AI
Zuva AI	AI
ABBy Fine Reader	OCR Platform Services
Sentry.io	System and Error Logging and View
SharePoint	Document Repository
Entra ID	Manages users and devices throughout the organization
Azure Storage Service Encryption (SSE)	Encryption-at-rest tool
OpenAI	Large Language Model Services
Anthropic	Large Language Model Services
Qlik	Reporting and Graphing for Deep Sights
SendGrid	E-mail Send Service
Jitterbit	API connectivity for non-standard integrations
Cohere	Large Language Model Services
Google AI/ML	Large Language Model Services

People

Leah is organized in the following functional areas:

Senior management staff have overall functional responsibility for commercial, technical, and operational aspects of the business globally. The technical arm is managed out of the Mumbai office.

Finance and Human Resources (HR)/Admin are responsible for the accounts, accounts payable and receivable, and management accounting on a global basis. The team of HR professionals are in three offices, performing HR management, talent acquisition, and payroll/admin functions.

Technology and Development Operations are based largely out of the Mumbai office and involved in platform enhancement, customization, and bug support.

Marketing runs as a global function from the Toronto office and is focused primarily on communications, content, demand, and events.

Sales is globally managed from the New York City and London offices. Both teams consist of leadership, account executives, sales development representatives, and sales engineers.

Transformation is based largely out of London and services the globe. The team consists of implementation managers that run customer implementations from end to end, liaising with the Technology team in Mumbai where necessary.

Their entry point on each client project takes place via a handover from the Sales Engineer, at which point the agreement is defined before the point of contract signature. They then own and run the agreement, which defines each client's configuration of the software, and are responsible for client delivery and onboarding.

The Transformation team also features a team of legal engineers, who test and refine the AI review capabilities of the software, feeding back to Technology as appropriate and liaising on the client side to optimize and improve machine learning efficiency on an ongoing basis.

The Customer Success team is based in the New York City office and is a global function. The team takes over each customer just after go-live via a handover from the implementation manager. It is their responsibility to act as a single point of contact for the customer on their user journey with the software, with a responsibility to retain and renew the license as appropriate.

Data

- Transaction data: comes from the creation of contracts in the system. This includes metadata of the contracts and the contract file
- Output reports: Reports that are generated from the system for/by the end users of the system
- Audit Trails: Generated by the Contract Lifecycle Management (CLM) solution for user and system actions
- System files/Code Files: Published code files for the Leah Software as a Service (SaaS) solutions
- Error logs: Generated by Leah SaaS product and Windows OS and infrastructure

Privacy Commitments

The following table describes the information included as part of the AI Based Contract Management Solutions Services System and Copilot Services System of Leah:

Client Data	Reporting
• Leah-Required Data (Minimal): Username and e-mail address - the only information Leah requires for user authentication and account management • Customer-Supplied Personal Data: Any personal data customers choose to upload to Leah within documents, including but not limited to: names, titles, positions, employer information, contact information (phone, e-mail, business address), identification data (IP addresses when generated by platform usage), and any other personal data embedded within contracts, e-mails, and business communications. Leah processes this data only because customers intentionally include it in their uploaded documents • Security & Audit Data (Generated by Leah): IP addresses, session data, audit trail logs, and other technical data generated by platform usage necessary for security, system integrity, and compliance purposes only	• Compliance & Audit Reports: SOC 2 Type II audit reports, security incident notifications (within 48 hours of discovery), data export and deletion confirmations, audit findings; provided to Customer upon request • Usage & Access Reports: User access logs, login activity, document activity logs, and system usage analytics provided to Customer account administrators through the platform • Data Export & Deletion Services: Upon Customer request, Leah provides export of Customer Personal Data in CSV or similar format (within 30 days) or securely deletes Customer Personal Data per Section 8.2 of the DPA

Leah does not collect customer business data. Instead:

- Leah requires only: username and e-mail address for user account creation and authentication
- Leah generates only: security/audit metadata (IP addresses from login sessions, audit trail logs, timestamps) necessary for system operation and security
- Customers supply everything else: Any personal data in documents, communications, contract metadata, contact information for vendors/prospects/employees, or other personal data that customers choose to upload or input into the platform

When customers upload contracts, e-mails, or other documents to Leah, those documents may contain personal data (names, contact information, employment details, etc.). Leah processes this personal data solely because customers have intentionally uploaded it as part of their business workflow. Leah does not extract, harvest, or independently collect this data-it is embedded in customer-selected documents.

Leah identifies and implements controls to meet data protection requirements through:

1. Data Processing Addendum (DPA): Leah executes a DPA with each customer that specifies:
    - The scope of personal data processing (Schedule 1)
    - Technical and organizational security measures (Schedule 2)
    - Cross-border transfer mechanisms for EU, UK, and Swiss data (Schedule 3)
    - Region-specific requirements including CCPA/CPRA compliance (Schedule 4)
2. Data Protection Laws Compliance: Leah complies with applicable data protection laws including:
    - EU GDPR and UK GDPR (via Standard Contractual Clauses and UK International Data Transfer Addendum)
    - Swiss Federal Act on Data Protection (FADP)
    - California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)
    - Other applicable regulations in Customer's jurisdiction(s)
3. Privacy by Design: Leah's data handling practices are designed to:
    - Minimize personal data processing (customers control what data is uploaded)
    - Limit access to authorized personnel only
    - Implement industry-standard security controls
    - Enable customer data portability and deletion upon request

Leah is committed to protecting the personal data entrusted to it by customers and the individuals whose data is contained within customer documents. As a data processor, Leah does not determine how personal data is used-customers (as data controllers) make those determinations and retain full control over their data.

Leah communicates privacy practices in the following

- To Data Subjects: Customers (as Controllers) are responsible for communicating privacy notices to individuals whose personal data may be processed within Leah (e.g., employees, prospects, vendors, business partners whose information appears in customer documents). Leah provides customers with transparency regarding Leah's data handling practices to support customers' compliance obligations
- To Customers (User Entities): Leah communicates its privacy practices to customers through:
    - The Data Processing Addendum (DPA), which documents Leah's processing scope, obligations, and controls
    - The Privacy Notice available at the Leah website/privacy portal
    - The Data Protection Policy and Privacy by Design Standard (available upon request)
    - Annual SOC 2 Type II audit reports demonstrating technical and organizational control implementation
    - Security incident notifications (within 48 hours of discovery, per DPA Section 5.2)

Processes, Policies and Procedures

Formal information technology (IT) policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. Teams are expected to adhere to the Leah policies and procedures that define how services should be delivered. These are located on the Company's SharePoint site and can be accessed by any Leah team member.

Physical Security

The in-scope system and supporting infrastructure is hosted by Azure. As such, Azure is responsible for the physical security controls for the in-scope system. For a listing of controls implemented by Azure, please refer to the "Subservice Organizations" section, below.

Logical Access

Leah uses role-based security, and it requires users to be identified and authenticated prior to any system resources. The application protects its users with its native identity management system.

SharePoint and OneDrive are used as document repositories and rely on authentication from Entra ID user credentials. Both services are hosted on Microsoft Office365.

Employees and approved vendor personnel sign on to the Leah network using an Entra ID user identification (ID) and password. Users are also required to separately sign on to any systems or applications that do not use the shared sign-on functionality of AD. Passwords conform to defined password standards and are enforced through parameter settings in AD. These settings are part of the configuration standards and force users to change passwords at a defined interval, disable the user ID's ability to access the system and components after a specified number of unsuccessful access attempts, and mask workstation screens, requiring reentry of the user ID and password after a period of inactivity.

Customer employees access Leah's AI-Based Contract Management Solutions Services System through the Internet using the Secure Sockets Layer (SSL) functionality of their web browser. These customer employees supply a valid user ID and password to gain access to customer cloud resources. Passwords conform to password configuration requirements configured on the Application or system.

Upon hire, employees are assigned to a position in the HR management system. Prior to the employee's start date, HR raises the request to the IT Helpdesk system for assets allocation and access to be granted. This request is then used by the IT Administrator team to allocate the assets and access to specific tools and services as per their role. Access to the tools and services are defined by the employee's line manager and then, as per the tools and services, the request traverses through respective assets/Service owners to provide access. The system lists also include employees with position changes and the associated roles to be changed within the access.

On an annual basis, access requests for each role are reviewed by a working group composed of security help desk, Infrastructure admin team, customer service, and HR personnel. In evaluating role access, group members consider job description, duties requiring segregation, and risks associated with access.

HR personnel create the request in the IT Helpdesk system for the terminated employee on the day of termination. The system then notifies the respective access administrators to revoke the respective access and assigned assets collection.

On an annual basis, HR runs a list of active employees and sends the request to the IT and other system/services owners who manage the access to the other systems and services. The respective access owners check and reconcile the active employee list and remove/revoke access to any tool and service. Any discrepancy in the access is logged into the system and remediation or action is logged.

Computer Operations - Backups

Customer data is backed up and monitored by operations personnel for completion and exceptions. In the event of an exception, operations personnel perform troubleshooting to identify the root cause and then re-run the backup job immediately or as part of the next scheduled backup job, depending on customer indicated preference within the documented work instructions.

Customer's data is hosted within their designated region on Azure in a northern European, United States, and Asia-Pacific (APAC) datacenter along with a continuous replication within the same continental region at a western European, United States, and APAC datacenter. Daily and hourly backups are retained for 90 days within their respective continental region.

The backups of the systems are stored on Azure for quick access when required.

On the workstations side, employees are advised to store data to their respective OneDrive accounts.

Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to IT incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network.

Leah' s dedicated Infrastructure team monitors capacity for both internal and customer instances to ensure uninterrupted service.

The Infrastructure team ensures adherence to a rigorous patch management program within Leah. Security patches are applied to the systems after rigorous testing.

Business continuity and disaster recovery plans are developed, updated, and tested annually. Additionally, backup restoration tests are also performed annually.

Change Control

Leah maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, code review, quality assurance (QA) testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. QA testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Customer Success or Implementation Managers approve changes prior to migration to the production environment and document those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate build code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Leah has implemented a patch management process to ensure Leah customer and infrastructure systems are patched in accordance with vendor-recommended operating system patches. Leah system owners review proposed operating system patches to determine whether the patches are applied. Leah are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. Leah staff validate that patches have been installed and, if applicable, that reboots have been completed.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal Internet protocol (IP) addresses. Administrative access to the firewall is restricted to authorized employees, controlled by Entra ID.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant system is configured to take its place.

Penetration testing is conducted to measure the security posture of a target system or environment on an annual basis. The third-party vendor uses an accepted industry-standard penetration testing methodology specified by Leah. The third-party vendor's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider, or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications, and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed by a third-party vendor on a quarterly basis. The third-party vendor uses industry standard scanning technologies and a formal methodology specified by Leah. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as-needed basis. Scans are performed during non-peak windows. Tools requiring installation in the Leah system are implemented through the Change Management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Authorized employees may access the system using VPN technology. Employees are authenticated through multi-factor authentication (MFA) system via AD.

Boundaries of the System

The scope of this report includes the AI Based Contract Management Solutions Services System and Copilot Services System performed in the London, England; New York City, New York; San Francisco, California; Mumbai, India; Glasgow, Scotland; and Toronto, Canada facilities.

This report does not include the cloud hosting services provided by Azure at multiple facilities.

Changes to the System Since the Last Review

No significant changes have occurred to the services provided to user entities since the organization's last review.

Incidents Since the Last Review

No significant incidents have occurred to the services provided to user entities since the organization's last review.

Criteria Not Applicable to the System

The following criteria are not applicable to the system:

Criteria Not Applicable to the System		
Category	**Criteria**	**Reason**
Privacy	P3.2, P5.1, P5.2	Leah does not directly gather data subject personal information. Leah customers are the data owners and data controllers of data subject information. As such, this criterion is the responsibility of user entities of the system.

Subservice Organizations

This report does not include the cloud hosting services provided by Azure at multiple facilities.

Subservice Description of Services

Azure is a cloud computing service created by Microsoft for building, testing, deploying, and managing applications and services through Microsoft-managed data centers.

Complementary Subservice Organization Controls

Leah's services are designed with the assumption that certain controls will be implemented by the subservice organization. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Leah's services to be solely achieved by Leah control procedures. Accordingly, the subservice organization, in conjunction with the services, should establish their own internal controls or procedures to complement those of Leah.

The following subservice organization controls should be implemented by Azure to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - Azure		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4, CC7.2	Procedures have been established to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors.
		Security verification and check-in are required for personnel requiring temporary access to the interior datacenter facility including tour groups or visitors.
		Physical access to the datacenter is reviewed quarterly and verified by the Datacenter Management team.
		Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals.
		The data center facility is monitored 24x7 by security personnel.
Availability	A1.2	Datacenter Management team maintains datacenter-managed environmental equipment within the facility according to documented policy and maintenance procedures.

Subservice Organization - Azure		
Category	**Criteria**	**Control**
		Environmental controls have been implemented to protect systems inside datacenter facilities, including temperature and heating, ventilation, and air conditioning (HVAC) controls, fire detection and suppression systems, and power management systems.
		Datacenter physical security management reviews and approves the incident response procedures on a yearly basis. The incident security response procedures detail the appropriate steps to be taken in the event of a security incident and the methods to report security weaknesses.
		Backups of key Azure service components and secrets are performed regularly and stored in fault tolerant (isolated) facilities.
		Critical Azure components have been designed with redundancy to sustain isolated faults and minimize disruptions to customer services.
		Customer data is automatically replicated within Azure to minimize isolated faults.
		Data Protection Services (DPS) backs up data for properties based on a defined schedule and upon request of the properties. Data is retained according to the data type identified by the property. DPS investigates backup errors and skipped files and follows up appropriately.
		Backup restoration procedures are defined, and backup data integrity checks are performed through standard restoration activities.
		Offsite backups are tracked and managed to maintain accuracy of the inventory information.
		Production data is encrypted on backup media.
		Azure services are configured to automatically restore customer services upon detection of hardware and system failures.

Leah management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Leah performs monitoring of the subservice organization controls, including the following procedures:

- Holding periodic discussions with the subservice organization
- Reviewing attestation reports over services provided by the subservice organization
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

COMPLEMENTARY USER ENTITY CONTROLS

Leah's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to Leah's services to be solely achieved by Leah control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Leah.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Leah.
2. User entities are responsible for notifying Leah of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Leah services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Leah services.
6. User entities are responsible for providing Leah with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Leah of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.
8. User entities are responsible for protecting data sent to Leah by appropriate methods to ensure confidentiality, integrity, and non-repudiation.
9. User entities are responsible for reviewing data input and output from the system for completeness and accuracy.
10. User entities are responsible for collecting consent form data subjects whose personal information was collected and providing evidence of data subjects' consent.
11. User entities are responsible for maintaining a record of personal information to track personal information and authorization.
12. User entities are responsible for reviewing personal information for accuracy and completeness against the purposes for which it is to be used.
13. User entities are responsible for reviewing the effectiveness of controls over personal information and compliance with the privacy policies.
14. User entities are responsible for reviewing methods of collecting personal information before they are implemented to confirm that personal information is obtained fairly, without intimidation or deception, and lawfully.
15. User entities are responsible for confirming the identity of data subjects who request access to their personal information is authenticated before they are given access to their personal information.
16. User entities are responsible for providing personal information to data subjects in an understandable and reasonable manner.
17. User entities are responsible for disclosing personal information to third-parties with the explicit consent of data subjects.
18. User entities are responsible for communicating the need for consent, as well as the consequences of a failure to provide consent for the request for personal information.

19. User entities are responsible for managing user accounts and access permissions within Leah.
20. User entities are responsible for immediately notifying Leah of any compromised, suspected compromised, or unauthorized account access.
21. User entities are responsible for cooperating with Leah in investigating and remediating incidents.
22. User entities are responsible for protecting API keys, credentials, and other authentication materials.
23. User entities are responsible for requesting deletion of Customer Personal Data from Leah upon contract termination or expiration.