# DATA SECURITY EXHIBIT

This Data Security Exhibit ("Exhibit") lists the technical and organisational measures implemented by LeanIX to protect the security and confidentiality of Customer Data. This Exhibit is incorporated into the Agreement and any term not defined herein shall have the same meaning defined elsewhere in the Agreement. Note that the Subscription Service is hosted on Microsoft® Azure®. For additional information concerning the security measures offered by Microsoft as a Subprocessor of LeanIX please check: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA.

## 1. Technical and Organisational Measures of LeanIX

LeanIX will maintain an Information Security Program which will at a minimum include administrative, technical and physical controls relating to information classification, data privacy, encryption, data handling, e-mail use and retention, password management, security configuration for network, OS, applications and desktops, change control, network and user system access, security incident management, physical access, external communication and asset management, as listed below. LeanIX will update and develop over time its Information Security Program to maintain consistency with evolving industry standard, face new security threats, comply with applicable laws and ensure continued availability of the Subscription Service. However, any change or update to the Information Security Program will not diminish the overall level of security of Customer Data.

1.1. Measures of pseudonymisation* and encryption of personal data.

1.1.1. Encryption at rest. LeanIX shall encrypt data at rest using AES-256 bit algorithm. LeanIX uses Azure Database for PostgreSQL for storing Customer Data.

1.1.2. Encryption in transit. LeanIX shall use TLS 1.3 with strong ECDHE ciphers for encrypting data in transit.

1.1.3. HTTPS. LeanIX application shall be accessible only via HTTPS.

**Note that the features of the Subscription Service (e.g. audit trail) are tied to the identity of a User so full pseudonymization is not possible. However, only personal data strictly necessary for the use of the Subscription Service are required.*

1.2. Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services.

1.2.1. Certifications. LeanIX shall implement measures in line with ISO 27001:2013 standard. LeanIX is SOC 2 Type 2 certified covering Security, Availability, Confidentiality and Privacy Trust Service Criterias (TSC).

1.3. Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.

1.3.1. BC and DR. LeanIX shall implement and maintain industry standard Business Continuity and Disaster Recovery plans. The current version of these plans can be made available upon request. Such plans shall include, without limitation:

- full daily back-ups of Customer Data, configurations and LeanIX application functions to the Read-Access Geo-redundant storage (RA-GRS);
- synchronization of back-ups across three storage clusters in one data centre in a single region and additionally asynchronously to another data centre in a secondary region;
- restoration testing performed on a quarterly basis;
- Recovery Point Objective of at least 24 hours and Recovery Time Objective of at least 48 hours;
- In case of a disaster, restoration of Customer Data from RA-GRS to servers in primary regions. If the primary regions are not available, restoration of in the secondary region;

1.4. Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

1.4.1. Audits. LeanIX shall conduct security audits internally and by external auditors at least annually. The audits shall be conducted for compliance with standards and best practices such as ISO 27001:2013, SOC 2 TSCs and OWASP Top 10.

1.4.2. Penetration Testing. To identify risks and remediation options that help increase security LeanIX shall (i) perform internal penetration tests on the LeanIX application at least once a quarter; (ii) contract a third party to execute a penetration test at least once a year. LeanIX will make executive reports from the penetration testing execute by third parties available to Customer upon request (provided that adequate non-disclosure obligations are in place).

1.4.3. Vulnerability scanning. LeanIX shall perform regular vulnerability scanning on the infrastructure and applications that store or process Customer Data to identify threats and potential vulnerabilities and provide for remediation.

1.5. Measures for user identification and authorisation

1.5.1. Internal Access Control. In normal operation of the Subscription Services, LeanIX employees do not access Customer Data. While addressing a support-related issue, LeanIX customer support shall only access customer workspace post consent from the customer and log out post the said purpose is achieved. LeanIX shall provide access to its employees on the basis principle of least privilege. Access shall be granted based on job roles and by following proper approval process based on Access Management Policy. Access privileges are reviewed on a half yearly basis.

1.5.2. Password. Strong password policies shall be implemented, including password complexity requirements, account lockout after 10 failed attempts, etc. Passwords are hashed using bcrypt algorithm with salt.

1.5.3. 2-factor Authentication. Access to servers shall be via 2-factor authentication.

1.5.4. Users. Customer administrators shall be responsible for managing User accounts within the Subscription Service.

1.6. Measures for the protection of data during transmission

1.6.1. Encryption in transit. LeanIX shall use TLS 1.3 with strong ECDHE ciphers for encrypting data in transit.

1.7. Measures for the protection of data during storage

1.7.1. Encryption at rest. LeanIX shall encrypt data at rest using AES-256 bit algorithm.

1.7.2. Antivirus. LeanIX shall implement enterprise grade antivirus solution.

1.7.3. HIDS. Host Intrusion Detection System (HIDS) shall be deployed on servers. Azure Network Security Group is configured to filter traffic and a firewall has been deployed on the internal network to safeguard against network attacks.

1.7.4. Separation Control. Customer Data shall be separated from those of other customers using dedicated database schemas.

1.8. Measures for ensuring physical security of locations at which personal data are processed

1.8.1. LeanIX Premises. Access to LeanIX premises shall be restricted using physical access tokens, door locks, video surveillance, nightly checks by security company, etc. Formal procedures are in place for granting, revoking and periodic review of physical access.

1.8.2. Microsoft Azure. LeanIX is hosted in Microsoft Azure datacentres which are ISO 27001, SOC 1, 2, 3 certified.

1.9. Measures for ensuring events logging

1.9.1. Logs. Logging shall be enabled on all critical information assets including application servers, network devices, operating system, database, web servers, and security devices.

1.9.2. Log retention. Logs shall be retained in accordance with LeanIX's applicable retention policy.

1.10. Measures for ensuring system configuration, including default configuration

1.10.1. Systems shall be configured and hardened as per LeanIX defined baselines.

1.11. Measures for internal IT and IT security governance and management

1.11.1. Incident and change management. LeanIX shall implement formal incident and change management process. All requests shall be logged and processed via ticketing system with formal approval process.

1.11.2. Risk Management Methodology. LeanIX shall maintain a defined Risk Management Methodology to manage risk within LeanIX. The approach is based on 8 stages i.e. from identifying assets to identifying residual risks. The process is monitored by Enterprise Risk Management Committee (ERMC).

1.11.3. Security Training. LeanIX shall offer adequate and regular security and privacy training to its employees that may process Customer Data.

1.11.4. Vendor Risk Management. LeanIX shall maintain programs and processes to ensure that all vendors that process Customer Data provide appropriate security controls, including periodic re-assessments.

1.12. Measures for certification/assurance of processes and products

1.12.1. Policies. LeanIX shall maintain policies, processes, procedures and controls in line with ISO27001:2013 standard and SOC2 TSCs.

1.13. Measures for ensuring data minimisation

1.13.1. Data Minimisation. Customer is solely responsible for uploading Customer Data on the Subscription Service. The Subscription Service is designed to require the input of only the personal information directly relevant and necessary to accomplish the relevant purpose. Also, will retain the data only for as long as is necessary to fulfil that purpose or till contract ends.

1.14. Measures for ensuring data quality

1.14.1. Quality features. LeanIX provides features such as Quality Seal to ensure data quality and integrity. It is the responsibility of Customers to use such features within the application and to grant and revoke access to LeanIX Subscription Services to its Users.

1.15. Measures for ensuring limited data retention

1.15.1. Deletion after termination/expiration. Customer Data are deleted after termination or expiration of the Agreement, latest within 30 days.

1.15.2. Deletion as part of back-ups. Customer Data deletion as part of backups in regular process 30 days upon collection, latest deletion in general, upon 60 days upon collection.

1.16. Measures for ensuring accountability

1.16.1. Accountability. LeanIX shall be responsible and accountable for operations and maintenance of LeanIX application including availability, upgrades, backup and patching. However, ownership of data within the application shall be with the customer.

1.17. Measures for allowing data portability and ensuring erasure

1.17.1. Customer Data export. Customer Data can be exported by Customer using available API's or excel export anytime during the Subscription Term.

1.17.2. Deletion. LeanIX shall be responsible for deleting Customer Data from its end and to provide certificate of destruction upon request. Since LeanIX provides a multi-tenant Subscription Service, LeanIX cannot wipe the VM. Microsoft Azure wipes the servers in line with Standards such as NIST 800-88. As part of Microsoft Azure data deletion, all data writes are sequential and requires updating the pointers to objects every time they are written. Once new values are written, pointers will be updated such that there is no way to find the deleted value anymore.