Annex I

Zendesk Technical and Organizational Security Measures – Innovation Services

The technical and organizational measures for protecting Service Data in connection with the Innovation Services are defined in the Zendesk Innovation Security Measures.

Zendesk's information security program includes documented policies and standards governing the processing of Service Data in compliance with applicable laws, as well as administrative, technical, and physical safeguards designed to ensure the confidentiality and integrity of Service Data. Zendesk reserves the right to update its security program from time to time, provided that such updates do not materially reduce the level of protection described in this Annex I.

1. Physical Access Controls

Zendesk implements appropriate measures to prevent unauthorized persons from gaining physical access to Service Data.

2. System Access Controls

Zendesk implements appropriate measures to prevent unauthorized use of Service Data.

3. Data Access Controls

Zendesk ensures through suitable measures that Service Data can only be accessed and processed by duly authorized personnel.

4. Transmission Controls

Zendesk implements appropriate measures to monitor and ensure to which entities Service Data is transmitted during data transfer activities. Service Data is protected against unauthorized reading, copying, alteration, or removal during electronic transmission or transport.

5. Input Controls

Zendesk ensures through appropriate measures that it can be determined whether, by whom, and when Service Data has been entered, modified, or deleted within data processing systems. Furthermore, any transfer of Service Data to third-party providers takes place exclusively through secure transmission channels.

6. Logical Separation

Data from different Zendesk customer systems is logically separated to ensure that Service Data belonging to different controllers remains segregated.

7. Security Policies and Personnel

Zendesk maintains and operates a comprehensive security program to identify risks and implement preventive technologies and measures against common threats. Zendesk further maintains a dedicated information security team responsible for protecting networks, systems, and services and for developing and delivering security training to employees in accordance with Zendesk security policies.

Technical and Organizational Security Measures of Neteleven – Enterprise Services

The technical and organizational measures for protecting Service Data used within Enterprise Services are included in the Neteleven Enterprise Security Measures. Neteleven reserves the right to update its protection program from time to time, provided that no update materially reduces the level of protection described in this Annex I.

Information Security Program and Team

Neteleven's protection program includes documented policies and standards governing administrative, technical, physical, and organizational safeguards for handling Service Data in accordance with applicable law. The program is designed to protect the confidentiality and integrity of Service Data, considering the nature, scope, context, and purposes of processing as well as the risks to affected individuals. Together with its partner Zendesk, Neteleven maintains a globally operating security team available around the clock to respond to security alerts and incidents.

Security Certifications

Neteleven holds the following security-related certifications issued by independent third-party auditors:

- SOC 2 Type II
- ISO 27001:2013
- ISO 27018:2014

Physical Access Controls

Neteleven implements appropriate measures, including security personnel and secured facilities, to prevent unauthorized physical access to Service Data and verifies that third parties operating data centers on its behalf maintain equivalent controls.

System Access Controls

Neteleven implements appropriate measures to prevent unauthorized use of Service Data. Depending on the type of processing, these controls may include password authentication, two-factor authentication, documented authorization procedures, documented change management processes, and multi-level access logging.

Data Access Controls

Neteleven implements appropriate measures to ensure that Service Data is accessible and manageable only by properly authorized personnel, that direct database access is restricted, and that application access rights are established and enforced so that individuals may access only the Service Data for which they are authorized. Service Data may not be read, copied, altered, or removed without authorization during processing.

Transmission Controls

Neteleven implements appropriate measures to ensure that it can be verified and determined which entities transmit Service Data via data transmission facilities, thereby preventing unauthorized reading, copying, alteration, or removal during electronic transmission or transport. Service Data is encrypted in transit when communicated through Neteleven user interfaces (UIs) and application programming interfaces (APIs) using industry-standard HTTPS/TLS (TLS 1.2 or higher).

Input Controls

Neteleven implements appropriate measures enabling the verification of whether and by whom Service Data has been entered, modified, or removed in data processing systems, and ensuring that any transfer of Service Data to external service providers occurs via secure transmission mechanisms.

Logical Separation

Data from different Neteleven customer environments is logically separated within systems managed by Neteleven to ensure that Service Data collected by different controllers remains segregated.

No Backdoors

Neteleven has not implemented any backdoors or similar mechanisms that would enable governmental authorities to bypass security controls in order to access Service Data.

Data Center Architecture and Security

Neteleven primarily hosts Service Data in data centers certified as compliant with ISO 27001, PCI DSS Service Provider Level 1, and/or SOC 2 standards.

Network Architecture and Security

Neteleven systems are hosted in security zones appropriate to their function, information classification, and associated risk level.

Testing, Monitoring, and Logging

Each year, Neteleven engages independent security experts to conduct comprehensive penetration testing of its production and corporate networks. Neteleven utilizes a Security Incident Event Management (SIEM) system.

Data Hosting Location

Neteleven offers customers the option to select the location where Service Data is hosted when purchasing the Data Center Location add-on.

Availability and Business Continuity

Neteleven maintains a publicly accessible status webpage containing details regarding system availability, scheduled maintenance, historical service incidents, and relevant security events.

Personnel Security

Neteleven conducts background checks on all employees prior to hiring.

Regular Backups and Recovery Processes

Neteleven performs regular backups and recovery operations to ensure data security and availability.

Logging and Monitoring

All access activities are logged and reviewed for irregularities at frequent intervals.

Patch and Update Management

Neteleven is committed to regularly providing all systems used for processing personal data with security updates and patches. Critical security vulnerabilities are addressed immediately after they become known. Patch and update management processes are documented and reviewed regularly.