Anhang I

Technische und organisatorische Sicherheitsmaßnahmen von Zendesk – Innovation Services

Die technischen und organisatorischen Maßnahmen zum Schutz von Servicedaten im Rahmen der Innovation Services sind in den Zendesk Innovation Security Measures festgelegt.

Das Informationssicherheitsprogramm von Zendesk umfasst dokumentierte Richtlinien und Standards zur Verarbeitung von Servicedaten in Übereinstimmung mit geltendem Recht sowie administrative, technische und physische Schutzmaßnahmen, die darauf ausgelegt sind, Vertraulichkeit und Integrität der Servicedaten zu gewährleisten. Zendesk behält sich das Recht vor, sein Sicherheitsprogramm von Zeit zu Zeit zu aktualisieren, wobei jedoch sichergestellt ist, dass durch solche Aktualisierungen das in diesem Anhang I beschriebene Schutzniveau nicht wesentlich verringert wird.

1. **Physische Zugangskontrollen:** Zendesk ergreift angemessene Maßnahmen, um unbefugten Personen den physischen Zugang zu Servicedaten zu verwehren.
2. **Systemzugangskontrollen:** Zendesk ergreift angemessene Maßnahmen, um die unbefugte Nutzung von Servicedaten zu verhindern.
3. **Datenzugriffskontrollen:** Zendesk stellt durch geeignete Maßnahmen sicher, dass Servicedaten ausschließlich von entsprechend autorisierten Mitarbeitenden eingesehen und verarbeitet werden können.
4. **Übertragungskontrollen:** Zendesk trifft angemessene Maßnahmen, um nachzuvollziehen und sicherzustellen, an welche Stellen Servicedaten im Rahmen der Datenübertragung übermittelt werden. Dabei wird gewährleistet, dass Servicedaten während der elektronischen Übertragung oder des Transports nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.
5. **Eingabekontrollen:** Zendesk stellt durch geeignete Maßnahmen sicher, dass nachvollzogen werden kann, ob und von wem Servicedaten in Datenverarbeitungssysteme eingegeben, verändert oder gelöscht wurden. Zudem erfolgt jede Übermittlung von Servicedaten an Drittanbieter ausschließlich über sichere Übertragungswege.
6. **Logische Trennung:** Daten aus den unterschiedlichen Kundensystemen von Zendesk werden logisch voneinander getrennt, sodass sichergestellt ist, dass Servicedaten verschiedener Verantwortlicher voneinander segregiert sind.
7. **Sicherheitsrichtlinien und Personal:** Zendesk unterhält und betreibt ein umfassendes Sicherheitsprogramm zur Identifikation von Risiken sowie zur Implementierung präventiver Technologien und Maßnahmen zur Abwehr gängiger Angriffe. Zudem verfügt Zendesk über ein dediziertes

Informationssicherheitsteam, das für den Schutz der Netzwerke, Systeme und Dienstleistungen verantwortlich ist und Schulungen für Mitarbeitende gemäß den Sicherheitsrichtlinien von Zendesk entwickelt und durchführt.

Technische und organisatorische Schutzmaßnahmen von neteleven – Großunternehmen-Dienste

Die technischen und organisatorischen Maßnahmen zum Schutz von Servicedaten für Großunternehmensdienste sind in den Enterprise-Sicherheitsmaßnahmen von Neteleven enthalten. Neteleven behält sich das Recht vor, sein Schutzprogramm von Zeit zu Zeit zu aktualisieren; vorausgesetzt jedoch, dass keine Aktualisierung die allgemeinen Schutzmaßnahmen in diesem Anhang I wesentlich verringert.

- **Informationsschutzprogramm und Team:** Das Neteleven-Schutzprogramm umfasst dokumentierte Richtlinien und Standards für administrative, technische, physische und organisatorische Schutzmaßnahmen, die den Umgang mit Servicedaten in Übereinstimmung mit geltendem Recht regeln. Das Schutzprogramm ist darauf ausgelegt, die Vertraulichkeit und Integrität der Servicedaten zu schützen, entsprechend der Art, dem Umfang, dem Kontext und den Zwecken der Verarbeitung sowie den Risiken, die mit der Verarbeitung für die Betroffenen verbunden sind. Neteleven unterhält mit seinem Partner Zendesk ein weltweit tätiges Schutzteam, das rund um die Uhr am Telefon ist, um auf Schutzwarnungen und -events zu reagieren.
- **Schutz-Zertifizierungen:** Neteleven besitzt die Schutz-bezogenen Zertifizierungen von unabhängigen Drittprüfern: SOC 2 Typ II, ISO 27001:2013 oder ISO 27018:2014.
- **Physische Zugangskontrollen:** Neteleven ergreift angemessene Maßnahmen, wie Schutzpersonal und gesicherte Gebäude, um zu verhindern, dass unbefugte Personen physischen Zugang zu Servicedaten erhalten, und überprüft, ob Dritte, die Rechenzentren im Auftrag von Neteleven betreiben, solche Kontrollen einhalten.
- **Systemzugriffskontrollen:** Neteleven ergreift angemessene Maßnahmen, um zu verhindern, dass Servicedaten ohne Genehmigung verwendet werden. Diese Kontrollen variieren je nach Art der durchgeführten Verarbeitung und können unter anderem die Authentifizierung über Passwörter und/oder Zwei-Faktor-Authentifizierung, dokumentierte Autorisierungsprozesse, dokumentierte Change Management-Prozesse und/oder die Protokollierung des Zugriffs auf mehreren Ebenen umfassen.
- **Datenzugriffskontrollen:** Neteleven ergreift angemessene Maßnahmen, um sicherzustellen, dass Servicedaten nur für ordnungsgemäß autorisiertes Personal zugänglich und verwaltbar sind, der direkte Zugriff auf Datenbankabfragen

eingeschränkt ist und Anwendungszugriffsrechte eingerichtet und durchgesetzt werden, um sicherzustellen, dass Personen, die berechtigt sind, ein Datenverarbeitungssystem zu verwenden, nur Zugriff auf die Servicedaten haben, auf die sie Zugriffsrecht haben, und dass Servicedaten im Laufe der Verarbeitung nicht ohne Genehmigung gelesen, kopiert, geändert oder entfernt werden können.

- **Übertragungssteuerung:** Neteleven ergreift angemessene Maßnahmen, um sicherzustellen, dass überprüft und festgestellt werden kann, welche Entitäten über Datenübertragungseinrichtungen Servicedaten übertragen, sodass Servicedaten während der elektronischen Übertragung oder des Transports nicht unbefugt gelesen, kopiert, geändert oder entfernt werden können. Service-Daten werden bei der Übertragung verschlüsselt, wenn sie mit Neteleven-Benutzeroberflächen (UIs) und Anwendungsprogrammierschnittstellen (APIs) über den Industriestandard HTTPS/TLS (TLS 1.2 oder höher) kommunizieren.
- **Eingabesteuerungen:** Neteleven ergreift angemessene Maßnahmen, um die Möglichkeit zu bieten, zu prüfen und festzustellen, ob und von wem Dienstdaten in Datenverarbeitungssysteme eingegeben, geändert oder entfernt wurden, und dass jede Übertragung von Dienstdaten an einen externen Dienstanbieter über eine sichere Übertragung erfolgt.
- **Logische Trennung:** Daten aus verschiedenen Neteleven-Kundenumgebungen werden auf Systemen, die von Neteleven verwaltet werden, logisch getrennt, um sicherzustellen, dass Servicedaten, die von verschiedenen Controllern gesammelt werden, voneinander getrennt werden.
- **Keine Hintertüren:** Neteleven hat keine Hintertüren oder andere Methoden in die Dienste integriert, um es Regierungsbehörden zu ermöglichen, ihre Sicherheitsmaßnahmen zu umgehen, um Zugriff auf Dienstdaten zu erhalten.
- **Rechenzentrumsarchitektur und Schutz:** Neteleven hostet Servicedaten hauptsächlich in Rechenzentren, die als ISO 27001, PCI DSS Service Provider Level 1 und/oder SOC2 konform zertifiziert sind.
- **Netzwerkarchitektur und Schutz:** Neteleven-Systeme werden in Zonen gehostet, die ihrem Schutz entsprechen, je nach Funktion, Informationsklassifizierung und Risiko.
- **Testen, Überwachen und Protokollieren:** Jedes Jahr beauftragt Neteleven externe Schutzexperten, um einen umfassenden Penetrationstest über die Neteleven Production- und Unternehmensnetzwerke durchzuführen. Neteleven verwendet ein Security Incident Event Management (SIEM)-System.

- **Datenhosting-Standort:** Neteleven bietet Kunden die Möglichkeit zu wählen, wo Servicedaten gehostet werden, wenn ein Kunde das Add-On Standort des Rechenzentrums erwirbt.
- **Verfügbarkeit und Kontinuität:** Neteleven führt eine öffentlich zugängliche Status-Webseite, die Systemverfügbarkeitsdetails, geplante Wartungsarbeiten, die Historie von Service-Vorfällen und relevante Sicherheits-Events enthält.
- **Personenschutz:** Neteleven führt vor der Einstellung Hintergrundüberprüfungen aller Mitarbeiter durch
- **Regelmäßige Backups und Wiederherstellungsprozesse:** Neteleven führt regelmäßige Backups und Wiederherstellungen zur Datensicherheit und Verfügbarkeit durch.
- **Protokollierung und Monitoring:** es werden alle Zugriffe protokolliert und auf Unregelmäßigkeiten in engem zyklischem Abstand kontrolliert.
- **Patch- und Update-Management:**
  Neteleven verpflichtet sich, alle Systeme, die zur Verarbeitung personenbezogener Daten eingesetzt werden, regelmäßig mit Sicherheitsupdates und Patches zu versorgen. Kritische Sicherheitslücken werden unverzüglich nach Bekanntwerden geschlossen. Das Patch- und Update-Management ist dokumentiert und wird regelmäßig überprüft.