Auftrag zur Verarbeitung personenbezogener Daten gemäß § 11 BDSG

Hiermit beauftrage/-n ich/wir die

Fa. **AnyDesk Software GmbH**, Friedrichstr. 9, 70176 Stuttgart

zur Datenverarbeitung gemäß unserer

„**Ergänzenden Bedingungen Auftragsdatenverarbeitung“**
(http://anydesk.de/agb#terms-data)

und der hier beiliegenden

Anlage zur beauftragten Datenverarbeitung.

Ich/wir nehme/-n zur Kenntnis, dass ein wirksamer Vertrag zwischen mir/uns und der Fa. **AnyDesk Software GmbH** nur unter diesen Bedingungen zustande kommt.

_____ Firma

_____ Straße und Hausnummer

_____ PLZ und Ort

_____ Ort, Datum

_____
rechtsverbindliche Unterschrift

_____
Name/-n in Druckbuchstaben

gegengezeichnet:

AnyDesk Software GmbH

_____
Ort, Datum

_____
rechtsverbindliche Unterschrift

Anlage zur Beauftragung der Datenverarbeitung

1. Allgemeines
Gegenstand, Umfang, Art und Zweck der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten durch AnyDesk für den Kunden ergeben sich aus den AGB von AnyDesk, den zugehörigen Leistungsbeschreibungen sowie den Ergänzenden Bedingungen zur Auftragsdatenverarbeitung.

In Ergänzung hierzu vereinbaren der Kunde und die Fa. AnyDesk GmbH (nachfolgend: „AnyDesk“) Folgendes:

2. Art der Daten
Gegenstand der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten können folgende Datenarten / -kategorien (Aufzählung / Beschreibung der Datenkategorien) sein:

- E-Mail Adresse
- IP-Adresse
- MAC-Adresse
- Personenbezogene Daten, die der Kunde bei seinen Nutzern im Rahmen seines Geschäftszwecks erhebt
- Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Vertragsabrechnungsdaten

3. Kreis der Betroffenen
Der Kreis der Betroffenen, deren Daten im Rahmen dieses Auftrags verwendet werden, kann folgende Personenkategorien umfassen:
- Jede Kategorie von Personen, die der Kunde im Rahmen seines Geschäftszwecks in der Software erfassen möchte;
- Mitarbeiter des Kunden;
- Kunden des Kunden

4. Standorte der Datenverarbeitung und Subunternehmer
Hetzner Online GmbH (Industriestr. 25, 91710 Gunzenhausen, Deutschland, Dedicated Hosting)

5. Datenschutzgerechte Verfahren zur Löschung/Vernichtung von personenbezogenen Daten
Soweit AnyDesk gesetzlich oder vertraglich zur Löschung/Vernichtung personenbezogener Daten verpflichtet ist, vereinbaren die Vertragsparteien als vertragskonforme Löschung / Vernichtung folgende Verfahren:

- Datenbank Secure DELETE
- Überschreiben eines Datenträgers mit Zufallsdaten vor Außerbetriebnahme

Defekte Datenträger oder Datenträger, bei denen eine Löschung technisch nicht bzw. nicht mehr möglich ist, müssen über den Kunden datenschutzgerecht entsorgt werden (dürfen insbesondere nicht über den Hausmüll, den Hersteller oder Dritte entsorgt werden); alternativ ist mit dem Kunden eine andere datenschutzgerechte Vorgehensweise zu vereinbaren.

6. Technisch-organisatorische Maßnahmen

6.1 Zutrittskontrolle
Ziel der Zutrittskontrolle ist es, dass Unbefugten der Zutritt zu solchen Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogener Daten verarbeitet oder genutzt werden.

Es existieren folgende Maßnahmen zur Zutrittskontrolle:
1) Festlegung von Sicherheitsbereichen
2) Realisierung eines wirksamen Zutrittsschutzes
3) Festlegung zutrittsberechtigter Personen
4) Verwaltung und Dokumentation von personengebundenen Zutrittsberechtigungen über den gesamten Lebenszyklus
5) Begleitung von Besuchern und Fremdpersonal
6) Überwachung der Räume außerhalb der Schließzeiten
7) Protokollierung des Zutritts

6.2 Zugangskontrolle
Ziel der Zugangskontrolle ist es, zu verhindern, daß Datenverarbeitungssysteme von Unbefugten genutzt werden, mit denen die Verarbeitung und Nutzung personenbezogener Daten durchgeführt werden.

Es existieren folgende Maßnahmen zur Zugangskontrolle:
1) Zugangsschutz (Authentisierung)
2) Einfache Authentisierung der Mitarbeiter (per Benutzername/Passwort) bei hohem Schutzniveau
3) Gesicherte Übertragung von Authentisierungsgeheimnissen (Credentials) im Netzwerk
4) Sperrung bei Fehlversuchen/Inaktivität und Prozess zur Rücksetzung gesperrter Zugangskennungen
5) Verbot Speicherfunktion für Passwörter und/oder Formulareingaben
6) Festlegung befugter Personen
7) Verwaltung und Dokumentation von personengebundenen Authentifizierungsmedien und Zugangsberechtigungen
8) Protokollierung des Zugangs
9) Automatische Zugangssperre
10) Manuelle Zugangssperre

6.3 Zugriffskontrolle
Die Maßnahmen zur Zugriffskontrolle müssen darauf gerichtet sein, daß nur auf die Daten zugegriffen werden kann, für die eine Zugriffsberechtigung besteht und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Es existieren folgende Maßnahmen zur Zugriffskontrolle:
1) Erstellen eines Berechtigungskonzepts
2) Umsetzen von Zugriffsbeschränkungen
3) Vergabe minimaler Berechtigungen
4) Verwaltung und Dokumentation von personengebundenen Zugriffsberechtigungen
5) Vermeidung der Konzentration von Funktionen
6) Protokollierung des Datenzugriffs

6.4 Weitergabekontrolle
Ziel der Weitergabekontrolle ist es, zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Es existieren folgende Maßnahmen zur Weitergabekontrolle:
1) Protokollierungen jeder Übermittlung oder einer repräsentativen Auswahl
2) Rechtmäßigkeit der Weitergabe ins Ausland
3) Sichere Datenübertragung zwischen Server und Client
4) Sicherung der Übertragung im Backend
5) Sicherung der Übertragung zu externen Systemen
6) Risikominimierung durch Netzseparierung
7) Implementation von Sicherheitsgateways an den Netzübergabepunkten
8) Beschreibung aller Schnittstellen und der übermittelten personenbezogenen Datenfelder
9) Maschine-Maschine Authentisierung
10) Sichere, verschlüsselte Ablage von Daten
11) Verhinderung von Zugriffen auf lokale Zwischenspeicher
12) Sichere Datenträgeraufbewahrung
13) Prozess zur Sammlung und Entsorgung
14) Datenschutzgerechtes Lösch-/ Zerstörungsverfahren

6.5 Eingabekontrolle
Ziel der Eingabekontrolle ist es, mit Hilfe geeigneter Maßnahmen sicherzustellen, daß nachträglich die näheren Umstände der Dateneingabe überprüft und festgestellt werden können.

Es existieren folgende Maßnahmen zur Eingabekontrolle:

Dokumentation der Eingabeberechtigungen

6.6 Auftragskontrolle
Ziel der Auftragskontrolle ist es, zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Kundes verarbeitet werden können.

Es existieren folgende Maßnahmen zur Auftragskontrolle:
1) Protokollierung der Auftragsausführung durch AnyDesk
2) Beschränkung der Auftragsausführung

6.7 Verfügbarkeitskontrolle
Ziel der Verfügbarkeitskontrolle ist es, zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Es existieren folgende Maßnahmen zur Verfügbarkeitskontrolle:
1) Backup-Konzept
2) Notfallplan
3) Aufbewahrung der Backups
4) Prüfung der Notfalleinrichtungen

6.8 Verwendungszweckkontrolle
Ziel der Verwendungszweckkontrolle ist es, zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Es existieren folgende Maßnahmen zur Verwendungszweckkontrolle:
1) Sparsamkeit bei der Datenerhebung
2) Getrennte Verarbeitung