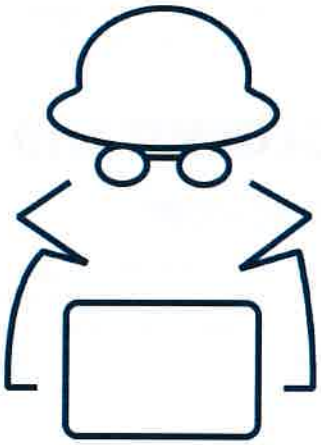
RELAX,
WE CARE



VERTRAG ZUR AUFTRAGSVERARBEITUNG PERSONENBEZOGENER DATEN IM RAHMEN VON SUPPORTLEISTUNGEN

Abgeschlossen zwischen den Parteien	
	NTS Netzwerk Telekom Service AG Parkring 4, 8074 Raaba-Grambach dataprivacy@nts.eu Fn173863g, LG f. ZRS Graz
„Verantwortlicher"	**„Auftragsverarbeiter"**

1. PRÄAMBEL

1. Der Auftragsverarbeiter führt im Auftrag des Verantwortlichen Wartungs- und/oder Pflegearbeiten an den IT-Systemen des AG durch. Der Umfang der beauftragten Wartungs- und/oder Pflegearbeiten richtet sich nach dem jeweiligen Hauptvertrag (Auftrag) und den Allgemeinen Supportbedingungen der NTS AG.
2. Da aufgrund der Natur der Systeme nicht ausgeschlossen werden kann, dass der Auftragsverarbeiter Zugriff auf personenbezogene Daten bekommt bzw. von solchen Daten Kenntnis erlangt, oder personenbezogene Daten verarbeitet, um die Wartung und Pflege von IT-Systemen durchzuführen oder durchführen zu können, wird nachfolgende Vereinbarung zur Auftragsverarbeitung von personenbezogenen Daten nach Art 28 Abs 3 Datenschutz-Grundverordnung (DSGVO) geschlossen.
3. Festgehalten wird, dass eine inhaltliche Bearbeitung oder Verarbeitung von personenbezogenen Daten regelmäßig nicht die Hauptintention der Parteien ist. Etwaige zufällig offengelegte oder offenbarte Daten mit Personenbezug werden von den Parteien nicht als Verarbeitung im Auftrag gesehen.

2. AUFTRAGSGEGENSTAND

2.1. IT INFRASTRUKTUR SUPPORT

Der Auftragsverarbeiter wird mit Wartungs- und/oder Pflegearbeiten der IT Infrastruktur Systeme des Verantwortlichen, nicht aber der Wartung und Pflege der personenbezogenen Daten selbst, beauftragt. Der Zweck dieser Arbeiten umfasst üblicherweise Installation, Hilfestellung im Betrieb, Fehlersuchen und Fehlerbehandlungen der betroffenen Systeme.

Im Zuge dieser beauftragten Arbeiten können Mitarbeiter der NTS AG Teile von personenbezogenen Daten einsehen, Loginformationen löschen, übermitteln oder vernichten.

Im Rahmen des Auftrages können Personendaten, Kontaktdaten, Netzwerk-Verkehrsdaten und andere personenbezogene Daten vom Verantwortlichen an den Auftragsverarbeiter weitergeleitet werden.

Kategorien betroffener Personen sind Mitarbeiter und Kunden des Verantwortlichen.

2.2. MANAGED MONITOR

Falls der Verantwortliche einen NTS Managed Monitor von NTS gekauft hat wird der Auftragsverarbeiter im Rahmen eines technischen Monitorings mit der Sammlung von technischen Daten beauftragt (Anzahl, Typ und Ort der IT-Infrastruktur-Systeme). Dazu zählt das Erstellen und Sammeln von System-Konfigurationsbackups und Sammeln von Betriebsdaten (Zustandsdaten aus IT Systemen, MAC, IP-Adressen, Traffic-Counter, etc.) der Systeme des Verantwortlichen. Die System-Konfigurationsbackups sind keine Backups von Datenbanken von personenbezogenen Daten, sondern Backups von technischen Konfigurationen der IT-Infrastruktur-Komponenten des Verantwortlichen.

Eine Verarbeitung von personenbezogenen Daten wird hier ausdrücklich nicht bezweckt, kann aber ein Zufallsergebnis sein. Insofern gelten die Bestimmungen dieses Vertrages nur soweit personenbezogene Daten davon betroffen sein können.

Im Rahmen des Auftrages können Netzwerk-Verkehrsdaten und andere personenbezogene Daten (zB IP-/MAC-Adressen, Gerätenamen) vom Auftragsverarbeiter im Supportfall eingesehen werden. Dies sind flüchtige Informationen, die nicht langfristig gespeichert und nicht verknüpft werden.

Kategorien betroffener Personen sind Mitarbeiter des Verantwortlichen.

2.3. ANDERE SERVICES

Für Cloud-Dienste (z.B. Meraki Services, Advanced Malware Protection, Umbrella, CWS, ...), deren Betrieb der Auftragsverarbeiter unterstützt, oder bei der Fehlerbehebung hilft, muss der Verantwortliche

direkt einen Auftragsverarbeitungsvertrag mit dem Cloud-Betreiber schließen, der die Daten auf den Cloud-Systemen betrifft.

3. PFLICHTEN DES AUFTRAGSVERARBEITERS

Der Auftragsverarbeiter verpflichtet sich:

1. Personengezogene Daten nur nach Maßgabe der geltenden Datenschutzgesetze und in dem Umfang zu verarbeiten, wie dies notwendig ist, um seine Pflichten aus der AV zu erfüllen, und wie er vom Verantwortlichen angewiesen wurde (dies schließt gegebenenfalls Änderungen an geltenden Gesetzen und notwendige Änderungen an den internen Richtlinien und/oder Prozessen des Auftragsverarbeiters ein, die sich auf die Verarbeitung der Daten durch den Auftragsverarbeiter auswirken können);
2. den Verantwortlichen unverzüglich zu benachrichtigen, wenn er der Ansicht ist, dass die Anweisungen des Verantwortlichen gegen geltende Datenschutzgesetze verstoßen;
3. den Verantwortlichen umgehend über eine Anfrage, Beschwerde, Nachricht, ein Ersuchen oder eine sonstige Kommunikation zu informieren, die er von einer Aufsichtsbehörde, staatlichen Stelle oder von sonstigen Dritten bezüglich der Verarbeitung von personenbezogene Daten durch den Auftragsverarbeiter erhält. Der Auftragsverarbeiter unterstützt den Verantwortlichen in angemessener Weise, damit dieser auf solche Anfragen, Beschwerden, Nachrichten, Ersuchen oder eine sonstige Kommunikation in Einklang mit den geltenden Datenschutzgesetzen antworten kann. Es ist dem Auftragsverarbeiter untersagt, mit Dritten, die derartige Anfragen stellen, direkt zu kommunizieren, ausgenommen der Auftragsverarbeiter wäre gesetzlich dazu verpflichtet;
4. den Verantwortlichen zu unterstützen, indem er Informationen und Dokumente als Reaktion auf eine Anfrage eines Betroffenen insbesondere im Zusammenhang mit dem Recht auf Auskunft, Richtigstellung, Löschung und Übertragbarkeit von personenbezogenen Daten, zur Verfügung stellt, damit der Verantwortliche diese Anfragen innerhalb der in den Datenschutzgesetzen jeweils festgelegten gesetzlichen Fristen beantworten kann;
5. seine eigenen Verpflichtungen aus den geltenden Datenschutzgesetzen jederzeit zu erfüllen, darunter die Führung von Unterlagen über die Datenverarbeitung (Verzeichnis von Verarbeitungstätigkeiten), die Einholung behördlicher Genehmigungen, etc. soweit dies für die personenbezogenen Daten von Relevanz ist;
6. den Verantwortlichen zu unterstützen und jede Information zur Verfügung zu stellen, die der Verantwortliche zur Durchführung einer Datenschutz-Folgenabschätzung benötigt, sofern der Verantwortliche nicht selbst Zugang zu den entsprechenden Daten hat;
7. den Verantwortlichen so bald wie möglich schriftlich unter der auf dem Deckblatt angeführten Email-Adresse zu benachrichtigen, sofern ihm Folgendes zur Kenntnis gelangt ist („Data Breach"):
   - eine tatsächliche oder vermutete unbefugte oder unrechtmäßige Verarbeitung der personenbezogenen Daten,
   - ein zufälliger oder unrechtmäßiger Verlust, eine Beschädigung, Vernichtung oder Verfälschung der personenbezogenen Daten;
8. im Falle eines Data Breach im Sinne von Punkt 7 dem Verantwortlichen so bald wie möglich, jedoch spätestens innerhalb von 72 Stunden ab Kenntnis der Datenschutzverletzung, umfassende Informationen über den Data Breach zur Verfügung zu stellen, u.a. die Art der Datenschutzverletzung, die Art der betroffenen Daten, die Kategorien und die Anzahl der betroffenen Personen, die Kategorien und die Anzahl der betroffenen Datensätze, die möglichen Folgen der Datenschutzverletzung, die Maßnahmen, die ergriffen oder vorgeschlagen wurden, um die Datenschutzverletzung zu untersuchen und ihre Auswirkungen möglichst gering zu halten;
9. ein Protokoll über den Data Breach anzufertigen, einschließlich der Sachverhalte, Auswirkungen und ergriffenen Abhilfemaßnahmen. Darüber hinaus ist der Auftragsverarbeiter verpflichtet, zügig alle notwendigen Schritte zu unternehmen, um die personenbezogenen Daten wiederherzustellen und/oder zu rekonstruieren, die infolge der Datenschutzverletzung verloren gegangen sind,

beschädigt, vernichtet oder verfälscht wurden, und zwar so, als würde es sich um die eigenen Daten des Auftragsverarbeiters handeln, und den Verantwortlichen in Bezug auf diese Datenschutzverletzung angemessen zu unterstützen;

10. bei Beendigung der Auftragsverarbeitung aus welchem Grund auch immer oder bei Ablauf des Hauptvertrags, ohne Zusatzkosten und nach Wahl des Verantwortlichen, alle vorhandenen personenbezogenen Daten zu vernichten oder diese in einem branchenüblichen Format ggf. zusammen mit allen Kopien an den Verantwortlichen zurückzugeben. Sofern der Verantwortliche wünscht, dass der Auftragsverarbeiter alle personenbezogenen Daten vernichtet, weist der Auftragsverarbeiter diese Vernichtung gegenüber dem Verantwortlichen nach, sofern nicht geltende Gesetze, die Löschung, aller oder Teile der übertragenen Daten, verhindern.

4. SUB-AUFTRAGSVERARBEITUNG

1. Der Auftragsverarbeiter greift im Fall von Supportleistungen nach Notwendigkeit auf Leistungen der jeweiligen Produkt-Hersteller und Partnerunternehmen zurück (siehe Anhang 2). Von der in der Liste angeführten Sub-Unternehmer werden nur jene involviert, die zur Erbringung der Servicleistungen notwendig sind. Der Verantwortliche erteilt seine ausdrückliche Zustimmung, zur Unterbeauftragung dieser Sub-Auftragsverarbeiter.

2. Der Auftragsverarbeiter trägt dafür Sorge, dass jeder Sub-Auftragsverarbeiter mindestens denselben Verpflichtungen unterliegt, wie sie nach Maßgabe dieses Vertrages für den Auftragsverarbeiter gelten. Auf Verlangen legt der Auftragsverarbeiter dem Verantwortlichen eine Kopie der schriftlichen Vereinbarung mit dem Sub-Auftragsverarbeiter vor.

3. Der Verantwortliche erteilt seine Zustimmung zur Unterbeauftragung von weiteren Sub-Auftragsverarbeitern, die mindestens denselben Verpflichtungen unterworfen werden, wie sie nach Maßgabe dieses Vertrages für den Auftragsverarbeiter gelten, sofern das für die Erbringung dieser oder der Hauptvereinbarung notwendig sein sollte.

4. Auf Wunsch wird der Auftragsverarbeiter den Verantwortlichen über eine Änderung der Sub-Auftragsverarbeiter vorab in Kenntnis setzen. Dazu wird ein Email-Notification Service eingerichtet, das der Verantwortliche über ein Email an subprocessors@nts.eu mit dem Betreff „Subscribe" für die jeweilige Absendeadresse aktivieren kann.

5. Im Fall der Aufnahme eines neuen Sub-Auftragsverarbeiters kann der Verantwortliche dieser Änderung widersprechen, sofern der Verantwortliche Produkte im Leistungsbereich des neu aufzunehmenden Sub-Auftragsverarbeiters im Einsatz hat bzw dafür aufgrund eines Hauptvertrages auf NTS Supportleistungen zurückgreifen möchte und der Widerspruch aus Gründen von

   5.1. Objektiv begründeten Bedenken in Hinsicht auf den zu wahrenden Datenschutz (zB zu erwartende Datenschutzverletzungen durch den Sub-Auftragnehmer, nicht ausreichende technische und organisatorische Maßnahmen)

   5.2. Objektiv begründeten Bedenken in Hinsicht auf sonstige zu befürchtende Rechtsverletzungen durch den Sub-Auftragnehmer

   5.3. Sonstigen objektiv begründeten Bedenken, die in den Geschäftsinteressen des Verantwortlichen oder in den berechtigten Interessen der Betroffenen liegen (zB aufgrund von objektiv nachvollziehbaren Fakten befürchtete Offenlegung von Geschäftsgeheimnissen an den Mitbewerb oder Dritte)

   erfolgt. Im Fall des Widerspruchs nimmt der Verantwortliche zur Kenntnis, dass Support- und Unterstützungsleistungen nicht in dem Umfang erfolgen können, wie sie unter Hinzuziehung des Sub-Auftragsverarbeiters möglich wäre.

6. Eine Liste der aktuell beauftragten Sub-Auftragsverarbeiter ist unter www.nts.eu/gdpr-subprocessors abrufbar.

5. TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

1. Der Auftragsverarbeiter verpflichtet sich, die notwendigen technischen und organisatorischen Maßnahmen zu ergreifen, um die Einhaltung der geltenden Datenschutzgesetze und dieser AV sicherzustellen. Eine Übersicht über die zum Zeitpunkt der Unterzeichnung dieser AV umgesetzten Maßnahmen ist in Anhang 1 enthalten.
2. Der Auftragsverarbeiter ist verpflichtet, den Verantwortlichen umgehend schriftlich über wesentliche Änderungen bei den technischen oder organisatorischen Maßnahmen in Kenntnis zu setzen.

6. AUDIT

1. Der Auftragsverarbeiter gestattet dem Verantwortlichen oder einem externen Prüfer, der nach Anweisung des Verantwortlichen handelt, Prüfungen, Untersuchungen und Einsichtnahmen in Bezug auf Datenschutz und/oder Datensicherheit („Audit") durchzuführen, um die Datenschutz- und Datensicherheitsverfahren des Auftragsverarbeiters sowie der autorisierten Sub-Auftragsverarbeiter bei der Verarbeitung von personenbezogenen Daten auf Grundlage dieser AV zu prüfen, soweit dadurch keine Geheimhaltungsinteressen des Auftragsverarbeiters oder seiner Mitarbeiter und Kunden verletzt werden.
2. Der Verantwortliche wird den Auftragsverarbeiter vier Wochen im Voraus über Datum und Uhrzeit der Prüfung in Kenntnis setzen. Das Recht des Verantwortlichen, weitere Prüfungen durchzuführen, falls der Auftragsverarbeiter seine Datenschutzpflichten verletzt, bleibt hiervon unberührt.
3. Der Verantwortliche trägt alle mit dem Audit verbundenen Kosten.

7. VERTRAULICHKEIT DER DATEN

1. Der Auftragsverarbeiter unternimmt alle angemessenen Schritte, um die Zuverlässigkeit von Mitarbeitern (einschließlich Sub-Auftragsverarbeiter), die möglicherweise Zugriff auf personenbezogene Daten haben oder befugt sind, diese zu verarbeiten, sicherzustellen und zu gewährleisten, dass diese Mitarbeiter (einschließlich Sub-Auftragsverarbeiter) sich vertraglich zur Erfüllung entsprechender Geheimhaltungspflichten verpflichten oder gesetzlich zur Geheimhaltung verpflichtet sind. Der Auftragsverarbeiter stellt sicher, dass diese Geheimhaltungspflicht über die Beendigung von Beschäftigungsverträgen, Dienstleistungsverträgen oder der Beendigung dieser AV hinaus fort gilt.

8. BEENDIGUNG

1. Im Falle einer Beendigung des Hauptvertrages, bleibt die vorliegende AV solange bestehen, als der Auftragsverarbeiter personenbezogene Daten für den Verantwortlichen verarbeitet. Nach Beendigung der AV bleiben die Klauseln zur Geheimhaltung (Kapitel 7) weiterhin in Geltung.
2. Soweit der Verantwortliche und der Auftragsverarbeiter zusätzliche Vereinbarungen geschlossen haben, die in Konflikt mit dieser AV stehen, sind die Regelungen dieser AV in Bezug auf die Verarbeitung personenbezogener Daten maßgeblich.

9. ALLGEMEINE BESTIMMUNGEN

1. Es gilt österreichisches Recht unter Ausschluss der Kollisionsnormen (IPRG) und des UN-Kaufrechts (CISG).
2. Ausschließlicher Gerichtsstand für alle Streitigkeiten aus diesem Vertrag ist Graz. Jede Partei stimmt zu, auf Einwände gegen das zuständige Gericht zu verzichten, sei es auf Grundlage der örtlichen Zuständigkeit oder des ungeeigneten Gerichtstands.
3. Falls einzelne Regelungen dieser AV unwirksam sind, bleiben die restlichen Regelungen der AV davon unberührt und in vollem Umfang in Kraft.
4. Änderungen oder Ergänzungen dieser Auftragsvereinbarung bedürfen der Schriftform. Dies gilt auch für ein Abgehen von dieser Formvereinbarung.

Grambach am 7. Mai 2018

Verantwortlicher	**, als**	**NTS Netzwerk Telekom Service AG, als Auftragsverarbeiter**
Unterschrift:		Unterschrift:
Name:		Name: DI. Hermann Koller
Funktion		Funktion

NTS NETZWERK TELEKOM SERVICE AG
Parkring 4, 8074 Raaba-Grambach
T +43 316 405 455 – 0 F – 56
FN 173863g, Landesgericht f. ZRS Graz

ANHANG 1 – TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

Als IT Infrastruktur Experte hat NTS umfassende technische und organisatorische Maßnahmen zum Schutz von Mitarbeiter und Kundendaten implementiert. Über die existierende Zertifizierung nach ISO 27001 und regelmäßige Schulungen aller Mitarbeiter wird die Vertraulichkeit, Integrität und Verfügbarkeit von personenbezogenen Daten unternehmensweit sichergestellt.

1. VERTRAULICHKEIT

Zutrittskontrolle
Es wird kein unbefugter Zutritt zu Datenverarbeitungsanlagen zugelassen. Die relevanten Systeme sind durch Chipkartenzugänge, Schlüssel, Alarmanlagen geschützt, sowie durch Videoanlagen überwacht.

Zugangskontrolle
Es ist keine unbefugte Systembenutzung möglich, da die Systeme durch sichere Kennwörter geschützt sind. Die Kennwörter unterliegen einer klaren Policy und müssen industriegültige Komplexität aufweisen. Die beteiligten Systeme verfügen über automatische Sperrmechanismen. Der Zugriff in das NTS Netz ist durch Zwei-Faktor-Authentifizierung oder gleichwertige Mechanismen abgesichert.
Laut aufrechten Mitarbeiterrichtlinien, im Rahmen der ISO 27001 Zertifizierung, dürfen keine Kundendaten auf den Benutzerendgeräten dauerhaft abgelegt werden. Die Kundendaten werden nur auf den dafür vorgesehenen Systemen abgelegt. Als zusätzliche Maßnahme (Defense in Depth) müssen alle Benutzerendgeräte die Verschlüsselung der Datenträger aktiviert haben.

Zugriffskontrolle
Die Daten auf den Systemen können nicht unbefugt gelesen, kopiert, verändert oder entfernt werden, da hier bedarfsgerechte Zugriffsrechte dazu gegeben sein müssen. Diese Zugriffe werden protokolliert.

Trennungskontrolle
Daten die zu unterschiedlichen Zwecken erhoben wurden, werden nicht zusammengeführt oder verknüpft.

Weitergabekontrolle
Bei elektronischer Übertragung von sensiblen Daten soll kein unbefugtes Lesen, Kopieren und Entfernen möglich sein. Die NTS AG stellt Plattformen zur Verfügung, womit die Daten des Verantwortlichen beim Transport über öffentliche Netze verschlüsselt übertragen werden können. (z.B. Sichere Übertragung auf die File-Share Plattform der NTS AG) Weiters können administrative Zugriffe via Virtual Private Networks zum Netzwerk des Verantwortlichen genutzt werden.

2. INTEGRITÄT

Bei der elektronischen Übertragung von sensiblen Daten kann der Verantwortliche verlangen, dass Verschlüsselungstechnologien eingesetzt werden, um eine Veränderung der Daten beim Transport zu verhindern (siehe 1 - Weitergabekontrolle).

Eingabekontrolle
Zugriffe auf die relevanten Systeme werden kontrolliert und Veränderungen der Daten werden protokolliert.

3. VERFÜGBARKEIT UND BELASTBARKEIT

Die NTS AG verfügt über Business Continuity Pläne, die im Rahmen der ISO 27001 Zertifizierung stetigen Reviews und kontinuierlichen Verbesserungen unterliegt.
NTS AG setzt anti-Malware Software ein, um das Risiko eines Verlustes von Daten gering zu halten.

4. VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

Durch das Infomrationssystem Management System der NTS AG (zertifiziert nach ISO 27001) ist gewährleistet, dass eine gültige Informationssystem Policy besteht. Das gesamte ISMS wird regelmäßig überprüft, bewertet und evaluiert.
Weiters ist ein Datenschutz-Management System etabliert, das auch regelmäßig überprüft, bewertet und evaluiert wird.
In diesen Systemen ist sichergestellt, dass es klare Sicherheitsrollen und Verantwortlichkeiten gibt.
Die NTS AG unterzieht sich regelmäßig und freiwillig internen und externen Audits, um mögliche Schwachstellen in Prozessen und Systemen früh zu erkennen und darauf reagieren zu können.
Incident Handling Prozesse stellen sicher, dass bei sicherheitsrelevanten Vorfällen, schnell und effizient Bedrohungen erkannt, eingedämmt und auch wieder eliminiert werden.

ANHANG 2 – LISTE DER SUBUNTERNEHMER

1. SCHWESTERUNTERNEHMEN DER NTS NETZWERK TELEKOM SERVICE AG:

1. **NTS Netzwerk Telekom Service AG**, Parkring 4, 8074 Grambach, Österreich
2. **NTS Deutschland GmbH**, Bahnhofplatz 3, 88045 Friedrichshafen, Deutschland
3. **NTS Italy, GmbH. – s.r.l.**, Schlachthofstraße, 30, 39100 Bozen, Italien
4. **NTS Schweiz GmbH**, Zinggenstraße 3, 9443 Widnau, Schweiz

   Eine Übermittlung erfolgt im Rahmen von technischen Unterstützungsleistungen auf Grundlage des Angemessenheitsbeschlusses der Europäischen Kommission (Beschluss der Europäischen Kommission 2000/518/EC)
5. **NTS Managed Service GmbH**, Parkring 4, 8074 Grambach, Österreich
6. **NTS North America Corp.** Goldberg & Company, LLC 25B Vreeland Road, Suite 211. Florham Park, NJ 07932, USA

   Eine Übermittlung erfolgt im Rahmen von technischen Unterstützungsleistungen auf Grundlage der „Model Contract Clauses" (Beschluss der Europäischen Kommission 2010/87/EU)

2. TECHNISCHE PARTNER

Soweit Support zu Produkten der nachfolgenden Firmen angefragt wird, kann eine Datenübermittlung im Rahmen von Support Cases (zB Logfiles, gemeinsame remote Sessions auf den Kundensystemen) in Länder außerhalb der EU erfolgen. Wo erforderlich, wird der Datenschutz über die von der EU vorgegebenen Instrumente auf Drittstaaten ausgedehnt.

2.1. PARTNER IN DER EU

1. **NTW Software GmbH**, Grabenweg 68, A-6020 Innsbruck

2.2. SICHERSTELLUNG DES DATENSCHUTZNIVEAUS ÜBER MODEL CONTRACT CLAUSES

Eine Übermittlung in Drittstaaten erfolgt im Rahmen von Support Cases oder sonstigen technischen Unterstützungsleistungen auf Grundlage der „Model Contract Clauses" (Beschluss der Europäischen Kommission 2010/87/EU):

1. **Cisco Systems, Inc.,** 170 West Tasman Drive, San Jose, CA 95134, USA
2. **Citrix Systems, Inc.,** 851 Cypress Creek Road, Fort Lauderdale, FL 33309, USA
3. **NetApp, Inc.**, 1395 Crossman Ave, Sunnyvale, CA 94089, USA
4. **Dell EMC Inc.**, 176 South Street, Hopkinton, MA 01748, USA
5. **Palo Alto Networks Inc.,** 3000 Tannery Way, Santa Clara, CA 95054, USA

2.3. SICHERSTELLUNG DES DATENSCHUTZNIVEAUS ÜBER EU-US PRIVACY SHIELD

Eine Übermittlung in Drittstaaten erfolgt im Rahmen von Support Cases oder sonstigen technischen Unterstützungsleistungen auf Grundlage von „Privacy Shield"(Beschluss der Europäischen Kommission (2016/1250/EU)

1. **Microsoft Corporation**, One Microsoft Way, Redmond, WA 98052-6399, USA
2. **Splunk Inc.,** 270 Brannan Street, San Francisco, CA 94107