## Hinweis zur Auftragsdatenverarbeitung

Falls Sie im Rahmen der Nutzung dieser Plattform personenbezogene Daten verarbeiten wollen, müssen Sie gemäß der Richtlinie 95/46/EG (EU-Datenschutz Richtlinie) und insbesondere § 11 Bundesdatenschutzgesetz (BDSG) mit der T-Systems International GmbH (nachfolgend „Telekom“ genannt) einen Vertrag über die Verarbeitung personenbezogener Daten (ADV) abschließen. Ob die von Ihnen zu verarbeitenden Daten personenbezogene Daten sind, müssen Sie selbst prüfen. Die Telekom bietet Ihnen gerne für diese Vereinbarung den hier beigefügten Vertrag über die Verarbeitung personenbezogener Daten an.
Sollten Sie besondere personenbezogene Daten oder andere sensible personenbezogene oder personenbeziehbare Daten (wie z.B. Personaldaten, Sozialdaten, Kontodaten und Kreditkarteninformationen, o.ä.) verarbeiten, empfehlen wir den Abschluss eines spezifischen ADVs.
Bitte senden Sie den Vertrag unterschrieben an die folgende Adresse:

T-Systems International GmbH
Service und Delivery Management VMware
Querstr. 1-11
04103 Leipzig

Eine Ausführung erhalten Sie durch die T-Systems International GmbH unterschrieben für Ihre Unterlagen zurück.

# Auftrag zur Verarbeitung personenbezogener Daten

Hiermit beauftrage ich die

T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt

zur Datenverarbeitung gemäß den „Ergänzenden Bedingungen Auftragsdatenverarbeitung - vCloud“ und der „Anlage Ergänzende Bedingungen Auftragsdatenverarbeitung - vCloud“.
Ich nehme einverständlich zur Kenntnis, dass ein wirksamer Vertrag zwischen mir und der T-Systems International GmbH nur unter diesen Bedingungen zustande kommt.

_____
Firma

_____
Straße und Hausnummer

_____
PLZ und Ort

_____
Ort, Datum

_____ _____
Unterschrift Name in Druckbuchstaben

_____
Ort, Datum (T-Systems International GmbH)

_____ _____
Unterschrift (T-Systems International GmbH) Name in Druckbuchstaben (T-Systems International GmbH)

# Ergänzende Bedingungen Auftragsdatenverarbeitung „vCloud“

1 Allgemeines

Gegenstand der Vereinbarung ist die Vereinbarung der Rechte und Pflichten des Kunden und der Telekom, sofern im Rahmen der Leistungserbringung (nach AGB und mitgeltenden Dokumenten) eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten (nachstehend „Daten“ genannt) durch die Telekom für den Kunden im Sinne der Richtlinie 95/46/EG (EU-Datenschutz Richtlinie) und insbesondere des § 11 Bundesdatenschutzgesetz (BDSG) als Auftragsverarbeiter erfolgt. Die Vereinbarung gilt entsprechend für die (Fern-) Prüfung und Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen, wenn dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

2 Verantwortung und Weisungsrechte des Kunden

2.1 Der Kunde als Auftraggeber ist für die Beurteilung der Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten sowie für die Wahrung der Rechte der Betroffenen verantwortlich. Der Kunde hat dafür Sorge zu tragen, dass die gesetzlich oder behördlich vorgeschriebenen Voraussetzungen geschaffen werden bzw. Anforderungen erfüllt werden, wie z.B. die Einhaltung von Löschfristen und zulässiger Speicherdauer, die Einholung von Einwilligungserklärungen, insb. sofern der Kunde besonders sensible Daten im Sinne des Art.8 der Richtlinie 95/46/EG verarbeiten lässt. Dies gilt auch für Anforderungen, z.B. an die Ausgestaltung der Auftragsverarbeitung, die daraus resultieren, dass der Kunden seinem lokalen Datenschutzrecht unterliegt.

2.2 Der Kunde stellt die Telekom in seinem Verantwortungsbereich von Ansprüchen Betroffener gegenüber der Telekom frei.

2.3 Gegenstand, Dauer, Art und Zweck der ggf. erfolgenden Datenverarbeitung bestimmt der Kunde durch seine Produktwahl, dessen Leistungsinhalte sich aus den AGB und ggf. mit geltenden Dokumenten ergeben und hinsichtlich der datenschutzrechtlichen Anforderungen in der Anlage zu den Ergänzenden Bedingungen Auftragsdatenverarbeitung konkretisiert sind.

2.4 Im Rahmen der produktspezifischen Parameter bestimmt der Kunde Art und Umfang der Datenverarbeitung durch die Art der Nutzung des Produktes durch Auswahl der dort ggf. ermöglichten Varianten z.B. hinsichtlich des Umfangs und der Art der zu verarbeitenden Daten oder des Ortes der Datenverarbeitung.

2.5 Zusätzliche Weisungen des Kunden im Hinblick auf die Verarbeitung personenbezogener Daten, die über die vertraglich vereinbarten Leistungen und Produktparameter hinausgehen und zu einem Mehraufwand für die Telekom führen, sind entsprechend gesondert zu vergüten. Bei Weisungen, deren Umsetzung für die Telekom nicht oder nur mit unverhältnismäßig hohem Mehraufwand möglich ist, kann die Telekom den Vertrag kündigen. Zusätzliche Weisungen bedürfen der Schriftform.

3. Schutzpflichten der Telekom / Kontrollpflicht und –recht des Kunden

3.1 Die Telekom verarbeitet die Daten ausschließlich im Rahmen der getroffenen Vereinbarungen. Die Telekom verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, die ihr überlassenen Daten an Dritte weiterzugeben. Die Telekom wird die zum Schutz der Daten erforderlichen technischen und organisatorische Maßnahmen gem. Art. 17 der Richtlinie 95/46/EG treffen, die in der Anlage zu den Ergänzenden Bedingungen Auftragsdatenverarbeitung beschrieben sind. Im Rahmen dieser Beschreibungen kann die Telekom die technischen und organisatorischen Maßnahmen nach eigenem pflichtgemäßen Ermessen der technischen und organisatorischen Weiterentwicklung anpassen.

3.2 Die Telekom hält geeignete Testate bereit, mit denen der Kunde die Einhaltung der Vorschriften über den Datenschutz im Hinblick auf die ihn betreffende Datenverarbeitung kontrollieren kann. Sie werden dem Kunden auf Anfrage zur Verfügung gestellt und in regelmäßigen Abständen, mindestens alle 24 Monate, aktualisiert. In besonders zu begründenden Ausnahmefällen kann der Kunde eine Einzelkontrolle durchführen. Sie kann auf seine Kosten durch den Kunden selbst durchgeführt werden oder durch einen von ihm beauftragten Dritten. Der Dritte ist mit der Beauftragung nachweislich zur Wahrung der Vertraulichkeit zu verpflichten. Dritte im Sinne dieser Vereinbarung dürfen keine Vertreter von Wettbewerbern der Telekom sein. Der Kunde wird Einzelkontrollen mit einer angemessenen Frist ankündigen und bei deren Durchführung auf Geschäftsbetrieb und Betriebsablauf Rücksicht nehmen. Bei Mehraufwand für die Telekom ist dieser durch den Kunden gesondert zu vergüten

4 Weitere Rechte und Pflichten des Kunden und der Telekom

4.1 Der Kunde ist verantwortlich für die Einhaltung der Rechte der Betroffenen, wie Berichtigung, Löschung und Sperrung von Daten, die ihm gegenüber geltend gemacht werden können. Die Telekom gewährleistet durch die Nutzungsmöglichkeiten der Produktparameter, dass der Kunde den Rechten der Betroffenen nachkommen kann. Macht der Betroffene sein Recht auf Berichtigung, Löschung oder Sperrung seiner Daten gegenüber dem Kunden geltend und kann der Kunde dem nicht durch entsprechende Auswahl bestimmter Produktparameter nachkommen, wird die Telekom in Abstimmung mit dem Kunden die Berichtigung, Sperrung oder Löschung vornehmen, soweit ihr die Vornahme der Anpassungen rechtlich und tatsächlich möglich ist.

4.2. Nicht mehr benötigte Unterlagen mit personenbezogenen Daten und Dateien, mit Ausnahme der aufgrund gesetzlicher Verpflichtung durch die Telekom weiter vorzuhaltenden Daten, werden entsprechend der vertraglichen Vereinbarung datenschutzgerecht vernichtet. Gleiches gilt für Test- und Ausschussmaterial. Soweit sich Speichermedien im Verfügungsbereich des Kunden befinden, wird der Kunde vor deren Übergabe an die Telekom oder deren Unterauftragnehmer alle personenbezogenen Daten datenschutzgerecht löschen. Sollte dies dem Kunden nicht möglich sein, wird er die Telekom rechtzeitig schriftlich informieren. Die Telekom ist dann berechtigt personenbezogene Daten im Auftrag des Kunden zu löschen. Soweit nicht ausdrücklich vereinbart, wird der Aufwand der

Löschung gesondert vergütet.

4.3 Der Kunde kann jederzeit während des Bestehens des Vertragsverhältnisses oder bis zu drei Monaten danach schriftlich die Daten, die nicht gemäß Ziffer 4.2 gelöscht sind, herausverlangen. Nach Ablauf dieser Fristen werden die übrigen Daten, mit Ausnahme der aufgrund gesetzlicher Verpflichtung der Telekom weiter vorzuhaltenden Daten, von der Telekom gelöscht. Das Herausgabeverlangen muss der Telekom einen Monat vor Ablauf der Frist zugegangen sein. Die Herausgabe selbst kann auch nach Ablauf der Frist erfolgen

4.4 Die Telekom wird den Kunden informieren, wenn die Datenverarbeitung nach Ansicht der Telekom gegen datenschutzrechtliche Vorschriften verstößt. Die Telekom ist berechtigt, die Durchführung der entsprechenden Datenverarbeitung solange auszusetzen, bis sie durch den Kunden bestätigt oder geändert wird.

4.5 Die Telekom informiert den Kunde über Fälle von schwerwiegenden Betriebsstörungen, bei Datenschutzverletzungen, bei Verstößen gegen die in dieser Vereinbarung getroffenen Festlegungen oder anderen wesentlichen Unregelmäßigkeiten bei der Verarbeitung der Daten des Kunden.

4.6 Die Telekom hat einen fachkundigen und zuverlässigen betrieblichen Datenschutzbeauftragten bestellt, dem die erforderliche Zeit zur Erledigung seiner Aufgaben gewährt wird. Der Datenschutzbeauftragte nimmt die Aufgaben gem. § 4g Bundesdatenschutzgesetz (BDSG) wahr.

4.7 Ist der Kunde gegenüber einer staatlichen Stelle oder einer Person verpflichtet, Auskünfte über die Verarbeitung von Daten zu geben, so wird die Telekom den Kunde darin unterstützen, diese Auskünfte zu erteilen. Soweit nicht ausdrücklich anders vereinbart, ist der Aufwand der Unterstützungsleistungen der Telekom gesondert zu vergüten.

## 5. Prüfung, Wartung, Fernzugriff

5.1 Sofern bei Prüfungs- und Wartungsarbeiten von automatisierten Verfahren oder von Datenverarbeitungsanlagen - auch solchen im Wege des Fernzugriffs – ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann, wird die Telekom nur in dem Umfang – auch in zeitlicher Hinsicht – von dem Zugriff Gebrauch machen, der für die ordnungsgemäße Durchführung der beauftragten Wartungs- und Prüfungsarbeiten unerlässlich notwendig ist.

5.2 Die Mitarbeiter der Telekom verwenden angemessene Identifizierungs- und Verschlüsselungsverfahren. Soweit nicht ausdrücklich anders vereinbart, ist für etwaig notwendige Datensicherungsmaßnahmen jede Partei in ihrem jeweiligen Verantwortungsbereichen verantwortlich.

5.3 Prüfungs- und Wartungsarbeiten, auch solche im Weg des Fernzugriffs, werden dokumentiert und protokolliert.

## 6. Datenverarbeitung im Ausland

6.1 Die Telekom wird die vertraglichen Leistungen dieser Vereinbarung in Deutschland bzw. von den mit dem Kunden vereinbarten Leistungsstandorten aus erbringen. Wenn die Telekom die geschuldeten Leistungen ganz oder teilweise von einem anderen Standort im Ausland erbringen möchte, wird die Telekom die Zustimmung des Kunden entsprechend des Verfahrens zur „Änderungen der Allgemeinen Geschäftsbedingungen (AGB), Leistungsbeschreibungen und Preise“ in den AGB vCloud Kapitel 11 einholen.

6.2 Der Kunde wird seine Zustimmung zur Verlagerung der Leistungserbringung ins Ausland nicht unbillig verweigern. Die konkreten Orte der Leistungserbringung (Lokation) werden Seitens Telekom dokumentiert und auf Verlangen des Kunden nachgewiesen.

6.3 Sofern die Datenverarbeitung nach dieser Vereinbarung und den gesetzlichen Vorgaben zur Verarbeitung personenbezogener Daten im Auftrag bzw. zur Übermittlung personenbezogener Daten in das Ausland zulässig außerhalb Deutschlands erbracht werden darf, wird die Telekom für die Einhaltung und Umsetzung der gesetzlichen Erfordernisse bei grenzüberschreitendem Datenverkehr Sorge tragen

6.4 Die Telekom wird im Falle einer Übermittlung personenbezogener Daten im Wege der Unterbeauftragung in sog. Offshore-Länder außerhalb der Europäischen Union (EU) oder des Europäischen Wirtschaftsraums (EWR) die gesetzlichen Vorgaben für grenzüberschreitende Übermittlungen beachten und insbesondere ein angemessenes Datenschutzniveau sicherstellen. Soweit hierzu ein Vertrag nach Maßgabe der jeweils gültigen EU-Standardvertragsklauseln für ein Controller-Processor-Verhältnis mit dem außerhalb der EU oder des EWR ansässigen Subunternehmer zugrunde gelegt wird, werden die EU-Standardvertragsklauseln im Namen und im Auftrag des Auftraggebers abgeschlossen. **Die Vertretungsvollmacht hierfür wird hiermit erteilt.** Soweit für den Abschluss der EU-Standardvertragsklauseln die Information oder Zustimmung der nationalen Datenschutzbehörde erforderlich ist, hat der Kunde dafür Sorge zu tragen, dass die gesetzlich oder behördlich vorgeschriebenen Voraussetzungen geschaffen werden bzw. erfüllt werden.

## 7. Unterauftragnehmer

7.1 Die Telekom darf zur Erfüllung der hier beschriebenen Aufgaben Unterauftragnehmer einsetzen. Soweit die Telekom im Rahmen der Leistungserbringung Unterauftragnehmer einbindet, wird die Telekom diese in der Anlage zu den Ergänzenden Bedingungen Auftragsdatenverarbeitung - vCloud angeben.

7.2 Bei einem Wechsel der Unterauftragnehmer wird die Telekom die Zustimmung des Kunden entsprechend des Verfahrens zur „Änderungen der Allgemeinen Geschäftsbedingungen (AGB), Leistungsbeschreibungen und Preise“ in den AGB vCloud Kapitel 11 einholen.

7.3 Die Telekom wird mit Subunternehmern vertragliche Vereinbarungen treffen, die den vertraglichen Regelungen dieser Vereinbarung entsprechen. Die Telekom wird in ihrem Verantwortungsbereich bei der Beauftragung von Subunternehmern im Ausland etwaige gesetzliche Vorgaben für die Verarbeitung personenbezogener Daten im Auftrag bzw. für die Übermittlung personenbezogener Daten in das Ausland sowie die Ziffern 6.1 bis 6.3 beachten.

## 8. Sonstiges

8.1 Die Unwirksamkeit einer Bestimmung dieser Vereinbarung berührt die Gültigkeit der übrigen Bestimmungen nicht. Sollte sich eine Bestimmung als unwirksam erweisen, wird Telekom diese durch eine neue ersetzen, die dem von Kunde und Telekom Gewollten am nächsten kommt.

8.2 Im Fall von Widersprüchen von Regelungen dieser Vereinbarung und Regelungen aus sonstigen Vereinbarungen geht diese Vereinbarung und die Anlage Ergänzende Bedingungen Auftragsdatenverarbeitung vor.

# Anlage zu Ergänzende Bedingungen Auftragsdatenverarbeitung „vCloud“

**1 Allgemeines**

1.1 Der Kunde und Telekom haben die Geltung der Ergänzenden Bedingungen Auftragsdatenverarbeitung „vCloud“ vereinbart.

1.2 Konkretisierend zu den AGB, zugehörigen Leistungsbeschreibungen oder sonstigen Dokumenten und den Ergänzenden Bedingungen Auftragsdatenverarbeitung „vCloud“ vereinbaren die Vertragsparteien nachfolgendes.

**2. Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten**

2.1 Gegenstand, Umfang, Art und Zweck der Erhebung, Verarbeitung und / oder Nutzung personenbezogener Daten durch die Telekom für den Kunden ergeben sich aus den AGB bzw. Leistungsvereinbarungen sowie aus den spezifischen Produktparametern und ihrer Nutzung durch den Kunden.

2.2 Art der Daten

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

- Name
- Anschrift
- Vertragsstammdaten(Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)
- Vertragsabrechnungs- und Zahlungsdaten
- Zugangsdaten
- Verbrauchsdaten
- Protokollierungsdaten
- Personenbeziehbare oder personenbezogene Protokolldaten (Benutzernamen, IP-Adressen etc.)
- Kontaktdaten (z.B. Telefon, E-Mail)

2.3 Kreis der Betroffenen

Der Kreis der Betroffenen, deren Daten im Rahmen dieses Auftrags verwendet werden, kann folgende Personenkategorien umfassen:

- Kunden
- Ansprechpartner/Business-Partner
- Mitarbeiterdaten

**3. Standorte der Datenverarbeitung und Subunternehmer**

3.1 Leistungserbringer, (Land, Adresse, Kurzbeschreibung der Leistung)

| Name Leistungserbringer | Land | Adresse | Kurzbeschreibung der Leistung |
|---|---|---|---|
| EMC Deutschland GmbH | Deutschland | Am Kronberger Hang 2a, 65824 Schwalbach | Third Level Support |
| Hewlett-Packard GmbH | Deutschland | Herrenberger Straße 140, 71034 Böblingen | Third Level Support |
| IBM Deutschland GmbH | Deutschland | IBM-Allee 1, 71139 Ehningen | Third Level Support |
| Novell Ireland Software Limited | Irland | Corrig Road, Sandyford Business Parz, Dublin 18 | Third Level Support |
| Red Hat Ltd. | Irland | 6700 Cork Airport Business Park, Kinsale Road, Cork | Third Level Support |
| Symantec LTD | Irland | Sandyford Business Parz, Dublin 18 | Third Level Support |
| VMware International Limited | Irland | Parnell House, Barrack Square, Ballincollig, Country Cork | Third Level Support |
| T-Systems Slovakia s.r.o. | Slowakische Republik | Zriedlova 13, 04001, Kosice | First and Second Level Support, Operation |
| IT Services Hungary Szolgáltató Kft. | Ungarn | Csapó utca 28, 4028, Debrecen | First Level Support |

**5. Technisch-organisatorsiche Maßnahmen**

5.1 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) Verwaltung und Dokumentation von personengebundenen Zutrittsberechtigungen über den gesamten Lebenszyklus
3) Begleitung von Besuchern und Fremdpersonal
4) Überwachung der Räume außerhalb der Betriebszeiten
5) Protokollierung des Zutritts zu den datenverarbeitenden IT-Systemen

5.2 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) Starke Authentisierung bei höchstem Schutzniveau
3) Einfache Authentisierung der Mitarbeiter (per Benutzername/Passwort) bei hohem Schutzniveau
4) Gesicherte Übertragung von Authentisierungsgeheimnissen (Credentials) im Netzwerk
5)Personen mit Zugangsberechtigung werden explizit bestimmt und auf ein Minimum beschränkt
6) Personengebunden Authentifizierungsmedien werden dokumentiert und verwaltet
7) Protokollierung der erfolgreichen und abgewiesenen Zugangsversuche
8) Festlegung befugter Personen
9) Automatische und manuelle Zugangssperre bei Verlassen des Arbeitsplatzes

5.3 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 Zutrittskontrolle:

1) Erstellen eines Berechtigungskonzepts
2) Umsetzen von Zugriffsbeschränkungen
3) Vergabe minimaler Berechtigungen
4) Personengebundene Zugriffberechtigungen werden verwaltet und dokumentiert
5) Protokollierung des Datenzugriffs

5.4 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) Sichere Datenübertragung zwischen Server und Client
3) Sicherung der Übertragung im Backend
5) Sicherheitsgateways an den Netzübergabepunkten
6) Löschung voreingestellter Dienstkonten/Passwörter und nicht benötigter Dienste
7) Beschreibung aller Schnittstellen und der übermittelten personenbezogenen Datenfelder
8) Jede Maschine die in das IV-Verfahren einbezogen ist, besitzt eine eineindeutige Kennung/Passwort
9) Die Datenspeicherung erfolgt ausschließlich auf der Plattform und den Backup-System
10) Die vollständige, datenschutzgerechte und dauerhafte Löschung von Daten bzw. Datenträgern mit Kundendaten des Auftraggebers wird protokolliert

5. 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:

1) Protokollierung der Dateneingaben

5.6 Auftragskontrolle

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

Es existieren folgende Maßnahmen zur Auftragskontrolle:

1) Regelungen/Beschränkungen zur Auftragsausführung

5.7 Verfügbarkeitskontrolle

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

Die Maßnahmen zur Verfügbarkeitskontrolle sind in der „Leistungsbeschreibung Dynamic Services for Infrastructure with VMware vCloud Datacenter Services (DSI vCloud)“ in den Abschnitten (Datenspeicherung, Backup und Wiederherstellung von VMs, Disaster Recovery)
geregelt.

5.8 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 und/oder Lagerung von Daten mit unterschiedlichen Vertragszwecken.

**6. Genehmigte Subunternehmer**
**Name, Adresse Hauptsitz und ggf. abweichender hier relevanter Nebensitz**

| Name Subunternehmer | Adresse Hauptsitz/ ggf. Nebensitz | |
|---|---|---|
| EMC Deutschland GmbH | Deutschland | Am Kronberger Hang 2a, 65824 Schwalbach |
| Hewlett-Packard GmbH | Deutschland | Herrenberger Straße 140, 71034 Böblingen |
| IBM Deutschland GmbH | Deutschland | IBM-Allee 1, 71139 |

| | | | |
|---|---|---|---|
| | | Ehningen | |
| Novell Ireland Software Limited | Irland | Corrig Road, Sandyford Business Parz, Dublin 18 | |
| Red Hat Ltd. | Irland | 6700 Cork Airport Business Park, Kinsale Road, Cork | |
| Symantec LTD | Irland | Sandyford Business Parz, Dublin 18 | Third Level Support |
| VMware International Limited | Irland | Parnell House, Barrack Square, Ballincollig, Country Cork | Third Level Support |
| T-Systems Slovakia s.r.o. | Slowakische Republik | Zriedlova 13, 04001, Kosice | |
| IT Services Hungary Szolgáltató Kft. | Ungarn | Csapó utca 28, 4028, Debrecen | |