Hinweis zur Auftragsdatenverarbeitung

Falls Sie im Rahmen der Nutzung dieser Plattform personenbezogene Daten verarbeiten wollen, müssen Sie gemäß den Regelungen des anwendbaren Rechts mit der T-Mobile Austria GmbH, Rennweg 97-99, A-1030 Wien, FN 171112k HG Wien, (nachfolgend „T-Mobile“ genannt) einen Vertrag über die Verarbeitung personenbezogener Daten (ADV) abschließen.
Ob die von Ihnen zu verarbeitenden Daten personenbezogene Daten sind, und ob die Regelungen in der beigefügten Vereinbarung die Anforderungen des für Sie geltenden Rechts erfüllen, müssen Sie selbst prüfen. T-Mobile bietet Ihnen gerne für diese Vereinbarung den hier beigefügten Vertrag über die Verarbeitung personenbezogener Daten an.
Bitte senden Sie den Vertrag unterschrieben an die folgende Adresse:

T-Mobile Austria GmbH
z.H. von der Rechtsabteilung (Datenschutz)
Rennweg 97-99
A-1030 Wien

Eine von T-Mobile unterschriebene Ausführung erhalten Sie für Ihre Unterlagen zurück.

Auftrag zur Verarbeitung personenbezogener Daten

Hiermit beauftrage ich die

T-Mobile Austria GmbH
Rennweg 97-99
A-1030 Wien, Austria,

zur Datenverarbeitung gemäß

- den „Ergänzenden Bedingungen Auftragsdatenverarbeitung für den Kunden-Support für Microsoft Online Dienste“ sowie
- den „Ergänzende Bedingungen Auftragsdatenverarbeitung für den Kunden-Support für Microsoft Online Dienste“.

Ich nehme einverständlich zur Kenntnis, dass ein wirksamer Vertrag zwischen mir und der T-Mobile nur unter diesen Bedingungen zustande kommt.

_____
Firma

_____
Straße und Hausnummer

_____
PLZ und Ort

_____
Ort, Datum

_____ _____
Unterschrift Name in Druckbuchstaben

Signiert von: Werner Norbert Kraus
Datum: 20.05.2020 11:53:04
www.handy-signatur.at
Dieses mit einer qualifizierten elektronischen Signatur versehene Dokument hat gemäß Art. 25 Abs. 2 der Verordnung (EU) Nr. 910/2014 vom 23. Juli 2014 ("eIDas-VO") die gleiche Rechtswirkung wie ein handschriftlich unterschriebenes Dokument.
Dieses Dokument ist digital signiert!
Prüfinformation:
Informationen zur Prüfung der elektronischen Signatur finden Sie unter:
www.handy-signatur.at
A-TRUST einfach sicher

_____

Dipl.Ing. Werner Kraus

Senior Vice President Business & Wholesale

T-Mobile Austria GmbH

Signiert von: Ania Tretbar-Bustorf
Datum: 28.05.2020 08:36:15
www.handy-signatur.at
Dieses mit einer qualifizierten elektronischen Signatur versehene Dokument hat gemäß Art. 25 Abs. 2 der Verordnung (EU) Nr. 910/2014 vom 23. Juli 2014 ("eIDas-VO") die gleiche Rechtswirkung wie ein handschriftlich unterschriebenes Dokument.
Dieses Dokument ist digital signiert!
Prüfinformation:
Informationen zur Prüfung der elektronischen Signatur finden Sie unter:
www.handy-signatur.at
A-TRUST einfach sicher

_____

Mag. Anja Tretbar-Bustorf

Vice President Legal, Regulatory & Interception

T-Mobile Austria GmbH

Ergänzende Bedingungen Auftragsdatenverarbeitung für den Kunden-Support für Microsoft Online Dienste

1. Allgemeines

Gegenstand der Vereinbarung ist die Vereinbarung der Rechte und Pflichten des Kunden und T-Mobile, sofern im Rahmen der Leistungserbringung (nach AGB und mitgeltenden Dokumenten) eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten (nachstehend „Daten" genannt) durch T-Mobile für den Kunden im Sinne des anwendbaren Datenschutzrechts 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.

Definitionen:
a) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)
b) Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten.
c) Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.
d) Datenverarbeiter ist jede natürliche oder juristische Person, welche die personenbezogenen Daten im Auftrag der verantwortlichen Stelle verarbeitet.
e) Dritter ist jede natürliche oder juristische Person, die nicht Betroffener, Datenverarbeiter oder verantwortliche Stelle ist.
f) Einwilligung ist jede freiwillige erteilte, spezifische und informierte, jederzeit widerrufbare Willenserklärung des Betroffenen

2. Verantwortung und Weisungsrechte des Kunden

2.1 Der Kunde als Auftraggeber und verantwortliche Stelle 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 verarbeiten lässt.

2.2 Der Kunde stellt T-Mobile in seinem Verantwortungsbereich von Ansprüchen Betroffener gegenüber T-Mobile 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 T-Mobile führen, sind entsprechend gesondert zu vergüten. Bei Weisungen, deren Umsetzung für T-Mobile nicht oder nur mit unverhältnismäßig hohem Mehraufwand möglich ist, kann T-Mobile den Vertrag kündigen. Zusätzliche Weisungen bedürfen der Schriftform.

2.6 Der Kunde muss T-Mobile hinsichtlich der Anforderungen des anwendbaren nationalen Rechts informieren, die T-Mobile bei der Verarbeitung seiner personenbezogenen Daten zu beachten hat.

3. Schutzpflichten von T-Mobile / Kontrollpflicht und –recht des Kunden

3.1 T-Mobile verarbeiten die Daten ausschließlich im Rahmen der getroffenen Vereinbarungen. T-Mobile verwendet die Daten für keine anderen Zwecke und ist insbesondere nicht berechtigt, die ihr überlassenen Daten an Dritte weiterzugeben. T-Mobile wird die zum Schutz der Daten erforderlichen, technischen und organisatorische Maßnahmen treffen, die in der Anlage zu den Ergänzenden Bedingungen Auftragsdatenverarbeitung beschrieben sind. Im Rahmen dieser Beschreibungen kann T-Mobile

die technischen und organisatorischen Maßnahmen nach eigenem pflichtgemäßem Ermessen der technischen und organisatorischen Weiterentwicklung anpassen.

3.2 T-Mobile 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 von T-Mobile sein. Der Kunde wird Einzelkontrollen mit einer angemessenen Frist ankündigen und bei deren Durchführung auf Geschäftsbetrieb und Betriebsablauf Rücksicht nehmen. Bei Mehraufwand für T-Mobile ist dieser durch den Kunden gesondert zu vergüten

4. Weitere Rechte und Pflichten des Kunden und T-Mobile

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. T-Mobile 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 T-Mobile 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 T-Mobile 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 T-Mobile oder deren Unterauftragnehmer alle personenbezogenen Daten datenschutzgerecht löschen. Sollte dies dem Kunden nicht möglich sein, wird er T-Mobile rechtzeitig schriftlich informieren. T-Mobile 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 T-Mobile weiter vorzuhaltenden Daten, von T-Mobile gelöscht. Das Herausgabeverlangen muss T-Mobile einen Monat vor Ablauf der Frist zugegangen sein. Die Herausgabe selbst kann auch nach Ablauf der Frist erfolgen

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

4.5 T-Mobile informiert den Kunden 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 T-Mobile hat einen fachkundigen und zuverlässigen betrieblichen Datenschutzbeauftragten bestellt, dem die erforderliche Zeit zur Erledigung seiner Aufgaben gewährt wird.

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

6.1 T-Mobile darf zur Erfüllung der hier beschriebenen Aufgaben Unterauftragnehmer einsetzen. Soweit die T-Mobile im Rahmen der Leistungserbringung Unterauftragnehmer einbindet, wird T-Mobile diese in der Anlage zu den Ergänzenden Bedingungen Auftragsdatenverarbeitung für den Kunden-Support für Microsoft Online Dienste angeben.

6.2 Bei einem Wechsel der Unterauftragnehmer wird T-Mobile die Zustimmung des Kunden entsprechend des Verfahrens zur Änderungen der Allgemeinen Geschäftsbedingungen (AGB), Leistungsbeschreibungen und Preise einholen.

6.3 T-Mobile wird mit Subunternehmern vertragliche Vereinbarungen treffen, die den vertraglichen Regelungen dieser Vereinbarung entsprechen.

7. Sonstiges

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

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

7.3 Der Kunde vereinbart mit Microsoft für die Nutzung der Microsoft Online Dienste das Microsoft Customer Agreement (MCA). Dabei werden auch eine Auftragsdatenverarbeitungsvereinbarung sowie die sog. EU Standardvertragsklausel über die Nutzung der Microsoft Online Dienste direkt mit Microsoft abgeschlossen.

Anlage zu Ergänzende Bedingungen Auftragsdatenverarbeitung

für den Kunden-Support für Microsoft Online Dienste

1 Allgemeines

1.1 Der Kunde und T-Mobile haben die Geltung der Ergänzenden Bedingungen Auftragsdatenverarbeitung vereinbart.
1.2 Konkretisierend zu den AGB, zugehörigen Leistungsbeschreibungen oder sonstigen Dokumenten und den Ergänzenden Bedingungen Auftragsdatenverarbeitung 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 T-Mobile 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
- Zugangsdaten
- Verbrauchsdaten
- 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
- Mitarbeiter

3 Standorte der Datenverarbeitung und Subunternehmer

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

Name Leistungserbringer	Land	Adresse	Kurzbeschreibung der Leistung
Deutsche Telekom AG	DE	Friedrich-Ebert-Allee 140, 53113 Bonn	Plattformbetreiber Cloud Marketplace
STRATO AG	DE	Pascalstrasse 10, 10587 Berlin	1st und 2nd Level Kunden-Support

4 Datenschutzgerechte Verfahren zur Löschung/ Vernichtung von personenbezogenen Daten

Soweit T-Mobile gesetzlich oder vertraglich zur Löschung/ Vernichtung personenbezogener Daten verpflichtet ist, vereinbaren die Vertragsparteien als vertragskonforme Löschung/ Vernichtung folgende Verfahren:
4.1. Löschung von Festplatten, USB-Sticks, wieder-beschreibbare Datenträger

- Datenträger werden gemäß den durch die Beschaffungs- und Entsorgungsprozesse bereitgestellten Verfahren ausgetauscht oder vernichtet.
- Bei der Entsorgung der Datenträger wird die Informationsschutzrichtlinie bzw. der Kundenauftrag beachtet.
- Die Löschung oder die Vernichtung von Datenträgern wird protokolliert.

Zudem sind die folgenden Punkte zu beachten:

- Eine Datenlöschung umfasst immer auch ein eventuell vorhandenes Backup.
- Die Datenlöschung muss protokolliert werden.

4.2 Löschung von Dateien auf Festplatten, USB-Sticks oder sonstigen wieder beschreibbaren Datenträgern
Unter Anwendung einer der in Punkt 4.1 als geeignet aufgeführten Methoden werden die jeweiligen Datenträger vollständig gelöscht. Sollen jedoch nur einzelne Dateien, datenschutzgerecht gelöscht werden, muss eine Software verwendet werden, welche die zu löschende Datei überschreibt und nicht nur den Verzeichniseintrag löscht.
Nicht geeignet sind folgende Methoden:

- Löschung mittels der Lösch-Taste (Delete-Funktion)
- Verschieben der Datei in den Papierkorb
- Umbenennen der Datei

5 Technisch-organisatorische 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) Realisierung des Zutrittschutzes
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 Betriebszeiten
7) Protokollierung des Zutritts

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) Einfache Authentisierung der Mitarbeiter (per Benutzername/Passwort) bei hohem Schutzniveau
3) Gesicherte Übertragung von Authentisierungsgeheimnissen (Credentials) im Netzwerk
4) Verbot Speicherfunktion für Passwörter und/ oder Formulareingaben
5) Festlegung befugter Personen
6) Verwaltung und Dokumentation personengebundenen Authentifizierungsmedien
7) Protokollierung des Zugangs
8) 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 Zugriffskontrolle:
1) Erstellen eines Berechtigungskonzepts
2) Umsetzen von Zugriffsbeschränkungen
3) Vergabe minimaler Berechtigungen
4) Personengebundene Zugriffberechtigungen werden verwaltet und dokumentiert
5) Vermeidung der Konzentration von Funktionen
6) 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
4) Sicherung der Übertragung zu externen Systemen
5) Risikominimierung durch Netzseparierung
6) Sicherheitsgateways an den Netzübergabepunkten
7) Härtung der Backendsysteme
8) Beschreibung aller Schnittstellen und der übermittelten personenbezogenen Datenfelder
9) Jede Maschine die in das IV-Verfahren einbezogen ist, besitzt eine eineindeutige Kennung/Passwort
10) Zugriff auf lokale Zwischenspeicher, zu Zwecken bzw. mit Anwendungen, die der Auftraggeber nicht freigegeben hat, ist technisch unterbunden Gesicherte Speicherung auf mobilen Datenträgern
11) Datenschutzgerechtes Lösch- und Zerstörungsverfahren

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) Dokumentation der Eingabeberechtigungen
2) 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 existiert folgende Maßnahme zur Auftragskontrolle:
1) Weisungserteilung und -entgegennahme
2) Regelungen/Beschränkungen zur Auftragsausführung
3) Protokollierung der Auftragsausführung durch den Auftragnehmer

5.7 Verfügbarkeitskontrolle
Ziel der Verfügbarkeitskontrolle ist es, zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.
Es existiert folgende Maßnahme zur Verfügbarkeitskontrolle:
1) Backup-Konzept
2) Notfallplan
3) Aufbewahrung des Backups
4) Prüfung der Notfalleinrichtungen

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 Verwendungszweck-kontrolle:
1) Sparsamkeit bei der Datenerhebung
2) Getrennte Verarbeitung und/oder Lagerung von Daten mit unterschiedlichen Vertragszwecken.