GRASS-MERKUR
Leitlinie
Datenschutzinformationen zu Cloud Services

Versionierung	
Version:	v1.1.0
Stand:	20191016
Autor:	Dr. Oliver Kunert
Verteilerinformationen	
Vertraulichkeit:	offen
Verteiler:	GRASS MERKUR
Info:	GRASS-MERKUR, Kunden und Interessenten
Dokumentenstatus	
Status:	FREIGABE

1 Abstrakt

Dieses Dokument soll Kunden und Interessenten an Cloud-Services der GRASS-MERUR darüber informieren, welche Rahmenbedingungen, Regelungen und Verantwortlichkeiten zum Schutz personenbezogener Daten im Kontext der von GRASS-MERKUR betriebenen und den Kunden angebotenen Cloud-Services gelten.

GRASS-MERKUR
Leitlinie
Datenschutzinformationen zu Cloud Services

Inhaltsverzeichnis

2 Einleitung

Dieses Dokument ist an Kunden und Interessenten der Cloud-Services der GRASS-MERKUR gerichtet. Es beschreibt in Konformität mit einschlägigen gesetzlichen Vorgaben und internationalen Standards die Ausgestaltung der Regelungen zu Umgang mit personenbezogenen Daten bei der Bereitstellung, dem laufenden Betrieb und der Nutzung der Cloud-Services der GRASS-MERKUR. Dabei soll ein gemeinsames Verständnis geschaffen werden für

- die Funktion der Cloud-Services der GRASS-MERKUR
- die Rolle, die Kunden bei der Einrichtung, der Verwaltung und der laufenden Nutzung der Cloud-Services zukommt
- die geteilten Verantwortlichkeiten zwischen Kunden und GRASS-MERKUR
- die Grundsätze, die beim Schutz personenbezogener Daten gelten

Das Dokument beschreibt die Reaktion von GRASS-MERKUR auf die Anforderungen, welche von Zertifizierungsstellen an das Informationssicherheitsmanagement mit Fokus auf den Umgang mit personenbezogenen Daten gestellt werden.

3 Technische und organisatorische Grundlagen

Es existieren verschiedene Modelle der Bereitstellung von Cloud-Services. Alle zeichnen sich jedoch mindestens durch folgende sie von anderen Services abgrenzende Eigenschaften aus.

- Ressourcen-Pooling auf virtualisierter Infrastruktur
- Mandantentrennung
- Kundenzugriff über Netzwerke aus räumlicher Distanz
- Dynamik und Elastizität der Infrastruktur
- verbrauchsbezogene Abrechnung

Diese besonderen Eigenschaften der Cloud-Services erfordern eine andere und vor allem spezielle Sicht auf den Umgang mit personenbezogenen Daten.

3.1 Modellbeschreibung der Clouds-Services

GRASS-MERKUR legt in Bezug auf seine Cloud-Services folgendes Modell zugrunde. Zur Darstellung werden Sichten auf die Cloud der GRASS-MERKUR verwendet. Im Modell gelten zwei Sichten, die als

a) ***die*** Cloud und

b) ***in der*** Cloud

bezeichnet werden sollen.

Die Cloud umfasst die Leistungen, die von GRASS-MERKUR erbracht werden. Dazu zählen:

- Betrieb des Rechenzentrums
- Betrieb der Cloud-Infrastruktur (physische Server, Appliances, Ablaufumgebungen (Hypervisors), Speichersysteme, Netzwerk, Management-Systeme) als Kernelement der Cloud-Services
- Betrieb der Sicherheitsinfrastruktur

- Betrieb der Datensicherungs-Infrastruktur
- Betrieb der Kundenschnittstelle für die Zugriffsverwaltung zur GRASS-MERKUR-Cloud
- Betrieb der Systeme zum Nachweis der vertraglichen Leistungserfüllung, zum Monitoring und zum Ressourcenverbrauch (Accounting)

Als ***in der*** Cloud werden folgende Objekte und Verwaltungsaktivitäten angesehen:

- Kundenapplikationen und Middleware
- Kundengastsysteme
- Kundendaten
- Konfiguration der Zugriffsberechtigungen auf Kundensysteme und Anwendungen durch den Kunden
- Datenverschlüsselung
- Netzwerk- und Firewalls
- In die Verantwortung des Kunden fallen auch kundeneigene Client-Systeme, die sich mit der GRASS-MERKUR-Cloud verbinden.

3.2 Verantwortlichkeitsverteilung

Entsprechend dem dargestellten Modell kommen systembedingt auf Kunden und GRASS-MERKUR geteilte Verantwortlichkeiten zu. IT-Infrastruktur aus der GRASS-MERKUR-Cloud zu nutzen, bedeutet, dass sowohl dem Kunden als auch GRASS-MERKUR wichtige Rollen beim Betrieb und dem IT-Sicherheitsmanagement in ihrem jeweiligen Verantwortungsbereich zukommen. GRASS-MERKUR betreibt, verwaltet und überwacht die Komponenten von der Schicht des Host-Betriebssystems und der Virtualisierungsebene bis hinunter zum physischen Schutz der Einrichtungen, der technischen Gebäudeausrüstungen und des Rechenzentrums-Gebäudes selbst, in dem die Cloud-Services von GRASS-MERKUR betrieben werden. GRASS-MERKUR kennt jedoch nicht die Daten in den von Kunden verwalteten Systemen, die Konfigurationen der Kundensysteme und deren Zustand in der Cloud. GRASS-MERKUR nimmt darauf auch keinen Einfluss, außer dies ist in einem Servicevertrag ausdrücklich geregelt.

Der Kunde ist verantwortlich für die Verwaltung der Gast-Betriebssysteme (einschließlich Updates und Security Patches für das Gast-Betriebssystem), der Datenbanken, der Anwendungssoftware und ganz besonders der Daten in den Systemen, auch die ggf. gewollte oder verlangte Verschlüsselung der Inhalte in der Cloud. Der Kunde erhält von GRASS-MERKUR eine Zugangsberechtigung zur Verwaltungsumgebung der GRASS-MERKUR-Cloud. Über diesen Zugang verwaltet der Kunde nach seinem Ermessen und ohne Einfluss von GRASS-MERKUR Administrator- und Benutzerberechtigungen für die Services und Systeme, die der Kunde in der GRASS-MERKUR-Cloud nutzt.

Der Kunden verbindet sich entweder über eine direkte Leitung oder über das Internet mit der GRASS-MERKUR-Cloud und zu seinen Systemen. GRASS-MERKUR stellt dazu mit gängigen technischen Verfahren und Protokollen nutzbare Zugangspunkte zur Cloud bereit. GRASS-MERKUR unterstützt Kunden dabei, geeignete Lösungen für einem bedarfsgerechten Sicherheitsniveau entsprechende Verbindungen zur Cloud zu finden und einzurichten.

Beim Betrieb und der Nutzung der Cloud-Services fallen prinzipbedingt personenbezogene Daten an, die in folgende Kategorien fallen: Konfigurationseinstellungen, Logging-Informationen und Nutzungs- bzw. Verbrauchsdaten. Diese Daten fallen in den Verantwortungsbereich der GRASS-MERKUR. Sie werden benötigt zum Nachweis vertraglich zugesicherter Leistungen, zur Fakturierung der Services gegenüber Kunden, zur Leistungssteuerung und Optimierung der Cloud-Services sowie ggf. zur Störungs- und Problemanalyse.

4 Sicherheit im Umgang mit personenbezogenen Daten

4.1 Sicherheit von Kundendaten

Welche Konsequenzen entstehen aus dem Modell für die Sicherheit der Kundendaten?

Für die Betrachtung der Sicherheit personenbezogener Daten im Zusammenhang mit Cloud-Services wird wieder das oben beschrieben Modell herangezogen:

a) "Sicherheit ***der*** Cloud": Sicherheitsmaßahmen, für deren Umsetzung GRASS-MERKUR die Verantwortung trägt und

b) "Sicherheit ***in*** der Cloud": Sicherheitsmaßnahmen, die der Kunde in Bezug auf die Sicherheit seiner Systeme, Anwendungen und Daten verantwortet

GRASS-MRKUR gewährleistet die Sicherheit ***der*** Cloud. Kunden tragen die Verantwortung für die Sicherheit ***in*** der Cloud.

Kunden haben und behalten jederzeit die Kontrolle darüber, welche Sicherheitsmaßnahmen sie auswählen und umsetzen, um ihre eigenen Inhalte dem Schutzbedarf entsprechend auf Vertraulichkeit und Integrität und insgesamt konform zu den geltenden Gesetzen und Regularien und ggf. branchenüblichen Vorgaben abzusichern (Compliance). Das ist für die Kunden der GRASS-MRKUR-Cloud-Services genau so, als würden sie ihre eigenen Systeme in eigenen Räumlichkeiten betreiben.

Kunden der GRASS-MERKUR werden nicht darin eingeschränkt, ihre Sicherheitsarchitektur so zu gestalten, dass sie ihre Compliance-Vorgaben erfüllt. GRASS-MERKUR wird aktiv nach Lösungen suchen und unterstützt die Kunden bei der Umsetzung ggf. vorhandener spezieller Erfordernisse, z.B. für verfügbarkeitssteigernde Service-Architekturen, Netzwerkverbindungen und Datensicherungen, Zugriffskontrollmechanismen, intensivierte Überwachungen auf Systemebene und Verschlüsselung von Daten während des Transports und bei der Ablage.

4.2 Sicherheit der Cloud

GRASS-MERKUR ist dem oben beschriebenen Modell folgend für die Sicherheit der zugrunde liegenden Cloud-Umgebung verantwortlich. Die Cloud-Infrastruktur erfüllt die dem Stand der Technik entsprechenden Anforderungen an Flexibilität, Verfügbarkeit, Resilienz und Kundentrennung. Sie ist skalierbar und basiert auf betriebssicheren Plattformen und erprobten Betriebsverfahren. GRASS-MERKUR weiß nicht, welche Inhalte Kunden in der Cloud speichern und kann deshalb nicht beurteilen, ob darunter personenbezogene Daten sind. Das ist allein Sache der Kunden.

GRASS-MERKUR verwendet Zugangs- und Zugriffssteuerungssysteme, elektronische Überwachungs- und Alarmierungsanlagen auf dem Stand der Technik. Zugriffe werden nach dem Prinzip der geringsten Rechte und ausschließlich zum Zweck der Systemadministration gewährt.

GRASS-MERKUR betreibt seit 2012 durchgängig ein zertifiziertes Informations-Sicherheitsmanagement-System (ISMS), das dem Standard ISO/IEC 27001 in der jeweils aktuellen Fassung entspricht. Die Zertifizierung belegt, dass GRASS-MERKUR seine Services mit wirksamem Risiko-Management und auf hohem Sicherheitsniveau erbringt.

Eine umfassende Darstellung aller etablierten Sicherheitseinrichtungen und umgesetzten Sicherheitsmaßnahmen, welche die Cloud-Infrastruktur, Plattformen und Services betreffen, finden Kunden und Interessenten an Cloud-Services der GRASS-MERKUR in der Leitlinie „Sicherheit der Cloud-Services“.

GRASS-MERKUR bietet an, eine Auftragsverarbeitungsvereinbarung zu schließen. Kunden sollen damit ihren eigenen datenschutzrechtlichen Verpflichtungen nachkommen können.

4.3 Sicherheit in der Cloud

Kunden behalten bei Nutzung der GRASS-MERKUR-Cloud-Service die ausschließliche Kontrolle über ihre in die Cloud eingebrachten Inhalt. Die Kunden entscheiden darüber, welche Inhalte sie in der GRASS-MERKUR-Cloud speichern. Kunden bestimmen, wie sie ihre Umgebungen konfigurieren und ihre Inhalte schützen, ob sie ihre Inhalte während der Ablage in der GRASS-MERKUR-Cloud und beim Transfer in oder aus der Cloud verschlüsseln. Die Kunden regeln selbst, wer Zugang zu diesen Inhalten hat. Mit der vollständigen Kontrolle über die Inhalte behalten die Kunden auch die Verantwortung über deren Sicherheit innerhalb der Cloud.

Um Kunden beim Design, bei der Implementierung und beim Betrieb ihrer Systeme innerhalb der GRASS-MERKUR-Cloud zu unterstützen, bietet GRASS-MERKUR gängige Sicherheits-Features an. Kunden können aber auch ihre eigenen Sicherheitsmechanismen und Werkzeuge einsetzen.

Kunden sollten folgenden Maßnahmen ergreifen, um den Schutz ihrer Inhalte zu erhöhen:

- Netzwerktrennung, Verschlüsselung von Inhalten, Benutzung von SSL/TLS und eine auf den Schutzbedarf abgestimmte Systemarchitektur
- Redundanz-Modelle und Backup-Strategien mit dem Ziel, das Risiko der Nichtverfügbarkeit zu entschärfen.
- Zwang zur Nutzung starker Passwörter, abgestufte, rollenbasierte Benutzerberechtigungen nach dem „need-toKnow-Prinzip“

Über alle diese Funktionen behält der Kunde die Kontrolle. GRASS-MERKUR hat keinen Einblick in deren Einstellungen und Parametrierungen und greift nicht in deren Funktion ein.

Kunden dürfen und können zur Verifikation und zum Test der implementierten Sicherheitsfunktionen und Konfiguration der genutzten Cloud-Services Sicherheitsüberprüfungen durchführen. Dies muss jedoch in Abstimmung mit und nach Zustimmung durch GRASS-MERKUR erfolgen und muss auf die eigenen Systeme des Kunden beschränkt sein und soll rückwirkungsfrei auf die GRASS-MERKUR-Cloud, sowie die Systeme anderer Kunden in der GRASS-MERKUR-Cloud erfolgen.

Der Kunde ist im Sinne der einschlägigen Gesetze verantwortliche Stelle in Bezug auf die personenbezogenen Daten, für die der Kunde den Verarbeitungszweck bestimmt hat und bei denen er entschieden hat, wie sie verarbeitet werden.

Der Kunde ist Auftragsverarbeiter in Bezug auf solche personenbezogene Daten, bei denen er die personenbezogenen Daten lediglich im Auftrag und nach den Wünschen eines Dritten in der GRASS-MERKUR-Cloud verarbeitet (wobei der Dritte seinerseits verantwortliche Stelle sein kann oder aber eine andere Partei innerhalb einer Lieferkette).

GRASS-MERKUR bietet in dieser Hinsicht lediglich Infrastruktur-Services für Kunden an, die ihre Inhalte in die GRASS-MERKUR-Cloud hochladen und dort verarbeiten wollen. In diesem Zusammenhang hat GRASS-MERKUR keinen Einblick in oder Kenntnis davon, was Kunden auf das GRASS-MERKUR-Netzwerk hochladen, und auch nicht, ob der Inhalt personenbezogene Daten enthält oder nicht. GRASS-MERKUR-Kunden haben zudem die Möglichkeit, Verschlüsselung zu verwenden, um die Inhalte für GRASS-MERKUR unlesbar zu machen.

Die verantwortliche Stelle muss dafür Sorge tragen, dass technische und organisatorische Maßnahmen zum Schutz der personenbezogenen Daten gegen zufällige oder unrechtmäßige Zerstörung oder zufälligen Verlust, Veränderung, unberechtigte Offenlegung oder Zugriff getroffen werden. Erfolgt die Datenverarbeitung durch einen Auftragsverarbeiter im Auftrag der verantwortlichen Stelle, ist die verantwortliche Stelle auch dafür verantwortlich, einen Auftragsverarbeiter auszusuchen, der ausreichende technische und organisatorische Maßnahmen zum Schutz der durchzuführenden Datenverarbeitung zur Verfügung stellt.

4.4 Zugriffsanforderungen von staatlichen Sicherheitsbehörden und Strafverfolgungsbehörden

Üblicherweise wird eine staatliche Stelle, die Zugriff auf die Daten eines Unternehmens nehmen will, ihr Auskunftsverlangen direkt an dieses Unternehmen richten, anstatt sich an GRASS-MERKUR zur Herausgabe dieser Daten zu werden. Die Europäische Union (EU) hat Gesetze erlassen, wonach die öffentlichen Strafverfolgungsbehörden und nationale Sicherheitsbehörden zum Zugriff auf Informationen ermächtigt werden. Auch ausländische Strafverfolgungsbehörden können mit den lokalen Strafverfolgungsbehörden und nationalen Sicherheitsbehörden über Hilfeersuchen kooperieren, um Zugriff auf Informationen in Deutschland zu erhalten. In der Praxis wird eine staatliche Stelle nachweisen müssen, dass es einen stichhaltigen Grund für das Zugriffsverlangen auf die Inhalte gibt, und sie wird einen Gerichtsbeschluss oder Durchsuchungsbefehl erwirken müssen.

GRASS-MERKUR wird Kundeninhalte nicht offenlegen, außer dies ist erforderlich, um rechtlich bindenden Anordnungen, wie einer richterlichen Anordnung, nachzukommen. GRASS-MERKUR wird jedes Ersuchen zur Herausgabe von Kundeninhalten sorgfältig prüfen und auf Konformität zu geltendem Recht verifizieren. Ist GRASS-MERKUR demnach rechtlich abgesichert gezwungen, Kundeninhalte herauszugeben, werden Kunden vor der Herausgabe über das Ersuchen informiert, und den Kunden wird damit die Möglichkeit eingeräumt, sich juristisch gegen die Herausgabe zu wehren.

5 Datenschutzgrundsätze bei geteilter Verantwortlichkeit

In der folgenden Tabelle sind die wesentlichen datenschutzrechtlichen Prinzipien zusammengestellt, die Kunden und GRASS-MERKUR üblicherweise in diesem Zusammenhang berücksichtigen müssen. Im Hinblick auf die Tabelle geht GRASS-MERKUR davon aus, dass der Kunde verantwortliche Stelle ist.

Wie vorstehend bereits erwähnt, ist uns jedoch bewusst, dass es viele Situationen geben kann, in denen der Kunde selbst Auftragsverarbeiter ist. Auch auf diese Konstellation treffen die folgenden Ausführungen zu.

Die nachfolgend beschriebenen Datenschutzgrundsätze richten sich nach den Vorgaben und Rahmenregelungen der EU-Datenschutzgrundverordnung (nachfolgend als Richtlinie bezeichnet) und dem Standard ISO/IEC 27018 in der jeweils aktuellen Fassung:

Datenschutzgrundsatz	**Datenschutzrechtliche Bedeutung**
Kundenbezug	**Bezug zu GRASS-MERKUR**
Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz: Betroffene sollten korrekte und vollständige Informationen über die Identität der verantwortlichen Stelle, den Zweck der Verarbeitung und alle anderen Informationen, die für eine angemessene Datenverarbeitung erforderlich sind, erhalten.	
Der Kunde (oder dessen Kunde) entscheidet darüber, welche Informationen er erhebt und für welchen Zweck er diese Informationen verwendet. In vielen Fällen wird der Kunde eine direkte Beziehung zu den Betroffenen haben und somit in einer guten Ausgangslage sein, um direkt mit ihnen zu kommunizieren. Darüber hinaus sollte der Kunde über den Umfang jeder vorherigen Mitteilung an die Betroffenen	GRASS-MERKUR hat keine Kontrolle darüber, welche Art von Inhalten der Kunde in der GRASS-MERKUR-Cloud speichert und für welchen Zweck dies geschieht. GRASS-MERKUR hat keinen Einblick in die Inhalte (einschließlich der Frage, ob diese Inhalte personenbezogene Daten enthalten). GRASS-MERKUR hat keine Möglichkeit, Betroffene, deren personenbezogene Daten der Kunde auf der GRASS-MERKUR-Infrastruktur gespeichert hat, zu identifizieren oder zu kontaktieren. GRASS-MERKUR kann daher Betroffenen keine relevanten Informationen geben.

Datenschutzgrundsatz	Datenschutzrechtliche Bedeutung
Kundenbezug	**Bezug zu GRASS-MERKUR**
informiert sein. Wenn der Kunde darüber entscheidet, ob und für welchen Zweck er personenbezogene Daten verarbeitet, muss der Kunde auch bedenken, ob er eines der Kriterien der Richtlinie erfüllt. Zu den Kriterien gehört beispielsweise, dass der Betroffene seine Einwilligung erklärt hat oder dass die Verarbeitung für die Durchführung eines Vertrags mit dem Betroffenen erforderlich ist.	GRASS-MERKUR erhebt und verarbeitet Daten, die im Rahmen der Nutzung der Cloud-Services durch Kunden anfallen (Logging-Daten), nur zum Zweck der Erfüllung von Verträgen, aus rechtlichen Verpflichtungen heraus und zum Nachweis seiner Leistungen (Accounting). Wie vorstehend dargelegt, hat GRASS-MERKUR keine Kontrolle darüber, welche Art von Inhalten der Kunde bei GRASS-MERKUR speichert (und auch nicht, ob diese Inhalte personenbezogene Daten umfassen). GRASS-MERKUR bestimmt nicht, welche Architektur der Kunde durch die Kombination der GRASS-MERKUR-Service-Angebote erstellt und ob diese für die konkreten Bedürfnisse des Kunden angemessen ist. GRASS-MERKUR ist nicht in den Entscheidungsprozess eingebunden, ob und für welchen Zweck die Daten verarbeitet werden. Dementsprechend ist GRASS-MERKUR nicht in der Lage, zu beurteilen, ob eine Ermächtigungsgrundlage für die Verarbeitung vorliegt.
Zweckbindung und Datenminimierung: Personenbezogen Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.	
Es ist Sache des Kunden, zu bestimmen, welche personenbezogenen Daten er erhebt und für welche Zwecke sie verwendet werden. Wenn er diese Entscheidung trifft, muss der Kunde sicherstellen, dass es einen bestimmten, genau festgelegten und rechtmäßigen Zweck gibt. Der Kunde entscheidet darüber, ob die Daten danach für andere Zwecke verarbeitet werden und kann abwägen, ob diese anderen Zwecke mit dem ursprünglichen Zweck vereinbar sind.	GRASS-MERKUR hat keine Kontrolle über den Zweck, zu dem der Kunde die Daten erhebt, verwendet und in der GRASS-MERKUR-Cloud speichert. GRASS-MERKUR erhebt und verarbeitet Daten, die im Rahmen der Nutzung der Cloud-Services durch Kunden anfallen (Konfigurationsdaten, Logging-Daten, Abrechnungsdaten), nur zum Zweck der Erfüllung von Verträgen, aus rechtlichen Verpflichtungen heraus und zum Nachweis seiner Leistungen (Accounting). GRASS-MERKUR reduziert die genannten Daten auf das notwendige Minimum zur Wahrnehmung seiner Aufgaben und zur Erfüllung des genannten Zwecks. Zugleich berücksichtigt GRASS-MERKUR die im Rahmen geltender Gesetze und rechtverbindlicher Vorgaben notwendigen Umfänge der pflichtgemäß zu erhebenden Daten und wägt deren Mindestumfang ab.
Rechte der Betroffenen: Betroffene müssen in der Lage sein, Zugriff auf ihre personenbezogenen Daten zu haben und die Berichtigung, Löschung oder Sperrung der personenbezogenen Daten zu erreichen, die anders als in Einklang mit der Richtlinie verarbeitet werden.	
Der Kunde behält die Kontrolle über die Inhalte, die er bei GRASS-MERKUR speichert, und kann daher darüber bestimmen, wie die Betroffenen auf ihre	Wie im Abschnitt 3.2 dargelegt, hat GRASS-MERKUR keine Kontrolle darüber, welche Art von Inhalten der Kunde in der GRASS-MERKUR-Cloud speichert und zu welchem Zweck dies geschieht. GRASS-MERKUR hat keinen Einblick in

Datenschutzgrundsatz	Datenschutzrechtliche Bedeutung
Kundenbezug	**Bezug zu GRASS-MERKUR**
personenbezogenen Daten, die in den Inhalten enthalten sind, zugreifen können. Ebenso ist der Kunde am besten in der Lage, Anfragen oder Beschwerden eines Betroffenen hinsichtlich der Zulässigkeit der Datenverarbeitung durch den Kunden zu beantworten.	diese Inhalte und kann deshalb nicht beurteilen, ob diese Daten Personenbezug haben. GRASS-MERKUR kann die Betroffenen, deren personenbezogene Daten der Kunde in der GRASS-MERKUR-Cloud gespeichert hat, nicht identifizieren und kann keinen Kontakt zu ihnen herstellen. GRASS-MERKUR kann daher den jeweiligen Betroffenen keine Informationen liefern. GRASS-MERKUR ist nicht in der Lage, Daten, die in der GRASS-MERKUR-Cloud gespeichert sind, mit einer bestimmten Person in Verbindung zu bringen. Diese Informationen liegen ausschließlich in der Kontrolle des Kunden. Daten, die im Rahmen der unter dem Grundsatz „Zweckbindung“ angegebenen wahrzunehmenden Pflichten anfallen, behandelt GRASS-MERKUR gemäß diesem Grundsatz.
Richtigkeit: Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.	
Der Kunde hat die Kontrolle über die personenbezogenen Daten, die er bei GRASS-MERKUR speichert. Er ist daher dafür verantwortlich, ihre Richtigkeit zu überprüfen und aufrecht zu erhalten (und kann sie gegebenenfalls aktualisieren und berichtigen). Darüber hinaus verantwortet der Kunde die Sicherheit ***in*** der Cloud, so dass der Kunde sicherstellen kann, dass er angemessene Maßnahmen zum Schutz der Daten vor Verfälschung implementiert hat.	GRASS-MERKUR hat keine Kontrolle darüber, welche Art von Inhalten der Kunde bei GRASS-MERKUR speichert. GRASS-MERKUR hat auch keinen Einblick in die Inhalte. GRASS-MERKUR gibt keine Daten im Auftrag des Kunden ein oder ändert sie in seinem Auftrag. GRASS-MERKUR kann daher weder die Richtigkeit der Daten überprüfen noch die Daten ggf. aktualisieren. GRASS-MERKUR stellt in der Cloud-Infrastruktur Mechanismen nah dem Stand der Technik zur Verfügung mit denen Kunden nach deren Einschätzung unrichtige Informationen berichtigt oder gelöscht werden können.
Datensicherheit: Die verantwortliche Stelle muss angemessene technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten vor zufälliger oder unberechtigter Zerstörung oder vor zufälligem Verlust, Veränderung, unberechtigter Offenlegung oder Zugriff treffen.	
Nur der Kunde ist in der Lage, festzustellen, ob eine bestimmte Sicherheitsarchitektur, die er geplant oder implementiert hat, angemessen ist, um eine bestimmte Art von Inhalten einschließlich personenbezogener Daten zu schützen. Kunden sind für die Sicherheit ***in*** der Cloud verantwortlich, einschließlich der Sicherheit ihrer Inhalte	GRASS-MERKUR ist dafür verantwortlich, die Sicherheit der zugrunde liegenden Cloud-Umgebung herzustellen. Eine umfassende Darstellung der Sicherheitsmaßnahmen der Cloud-Infrastruktur, Plattformen und Services von GRASS-MERKUR ist in der Leitlinie „Sicherheit der GRASS-MERKUR-Cloud“ beschrieben. GRASS-MERKUR zieht externe Auditoren hinzu, um die Wirksamkeit seiner Sicherheitsmaßnahmen, einschließlich

Datenschutzgrundsatz	Datenschutzrechtliche Bedeutung
Kundenbezug	**Bezug zu GRASS-MERKUR**
(und der darin enthaltenen personenbezogenen Daten) und der Implementierung einer angemessenen Architektur bei der Nutzung der GRASS-MERKUR-Cloud-Services. Insbesondere sind Kunden verantwortlich für die ordnungsgemäße Konfiguration der GRASS-MERKUR-Services, Benutzung der zur Verfügung stehenden Kontrollmechanismen und Ergreifung von Maßnahmen, die sie für notwendig erachten, um angemessene Sicherheitsvorkehrungen und Datensicherungen ihrer personenbezogenen Daten aufrecht zu erhalten (z.B. durch Nutzung von Verschlüsselungstechnologie, um personenbezogene Daten vor unberechtigtem Zugriff zu schützen, sowie regelmäßige Archivierung).	der Sicherheit des Rechenzentrums, aus denen GRASS-MERKUR seine Services erbringt, überprüfen zu lassen.
Aufbewahrung der Daten und Speicherbegrenzung: Personenbezogene Daten sollen (in identifizierbarer Form) nicht länger aufbewahrt werden, als dies für den Zweck, für den sie erhoben oder verarbeitet wurden, erforderlich ist. Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist;	
Es ist Sache des Kunden darüber zu entscheiden, für welche Zwecke die in der GRASS-MERKUR-Cloud gespeicherten personenbezogenen Daten verwendet werden und wie lange eine Speicherung dieser Daten dementsprechend notwendig ist. Der Kunde kann die personenbezogenen Daten löschen oder anonymisieren, wenn sie nicht länger benötigt werden.	GRASS-MERKUR hat keinen Einblick, ob gespeicherte Daten personenbezogenen Daten beinhalten oder für welche Zwecke der Kunde die von ihm in der Cloud gespeicherten Daten verarbeitet. Entsprechend kann GRASS-MERKUR nicht darüber entscheiden, für wie lange eine Datenspeicherung erforderlich ist, um diese Zwecke zu erreichen. Wenn ein Kunde Inhalte in der GRASS-MERKUR-Cloud löscht, werden sie unlesbar oder unbrauchbar gemacht und die zu Grunde liegenden Speichereinheiten in der GRASS-MERKUR-Cloud, die zur Speicherung der Inhalte verwendet wurden, werden gesäubert, bevor sie wieder vergeben und überschrieben werden. Die GRASS-MERKUR-Prozesse sehen auch sichere Stilllegungsprozesse und Vernichtungsprozesse vor, die durchgeführt werden, bevor Speichermedien, die zur Erbringung der GRASS-MERKUR-Services verwendet wurden, entsorgt werden. Als Teil dieses Prozesses werden Speichermedien entmagnetisiert oder gelöscht und physisch zerstört oder nach dem Stand der Technik unbrauchbar gemacht. Die Aufbewahrung der personenbezogenen Daten, die im Rahmen der auftragsgemäßen Leistungserfüllung anfallen, wird auf das gesetzlich erforderliche und zweckerfüllend

Datenschutzgrundsatz	Datenschutzrechtliche Bedeutung
Kundenbezug	**Bezug zu GRASS-MERKUR**
	notwendige Maß begrenzt. Anschließend werden die Daten unwiederbringlich gelöscht. Auskünfte zur tatsächlichen Aufbewahrungsdauer einzelner Daten erteilt GRASS-MERKUR auf Anfrage.
Weitergabe und Übermittlung: Personenbezogene Daten sollen nicht in Drittländer (außerhalb der Europäischen Union) übermittelt werden, es sei denn, dass in diesem Land oder Gebiet ein angemessenes Schutzniveau für die Rechte und Freiheiten der Betroffenen in Bezug auf die Verarbeitung der personenbezogenen Daten sichergestellt ist. Eine Liste der Länder wird von der Europäischen Kommission im Amtsblatt und auf Ihrer Webseite veröffentlicht.	
Die Cloud-Services der GRASS-MERKUR werden in Deutschland am Standort Hannover erbracht.	GRASS-MERKUR überträgt Kundeninhalte nicht außerhalb seines in Deutschland befindlichen Rechenzentrums, es sei denn, dies ist aufgrund eines Gesetzes oder einer gültigen und bindenden staatlichen Anordnung erforderlich.
Integrität und Vertraulichkeit: Personenbezogene Daten müssen durch geeignete technische und organisatorische Maßnahmen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.	
Der Kunde hat die Kontrolle über die personenbezogenen Daten, die er in der GRASS-MERKUR-Cloud speichert. Er ist daher dafür verantwortlich, ihre Richtigkeit zu überprüfen und aufrecht zu erhalten (und kann sie gegebenenfalls aktualisieren und berichtigen). Darüber hinaus verantwortet der Kunde die Sicherheit ***in*** der Cloud, so dass der Kunde sicherstellen kann, dass er angemessene Maßnahmen zum Schutz der Daten vor Verfälschung implementiert hat.	GRASS-MERKUR hat keine Kontrolle über die in die GRASS-MERKUR-Cloud durch Kunden eingebrachten und verarbeiteten Daten und kann deshalb die Integrität und Vertraulichkeit nicht beeinflussen. GRASS-MERKUR betreibt eine sichere Cloud-Umgebung nach dem Stand der Technik als verantwortungsvoller und umsichtiger Dienstleister in Kenntnis und unter Verwendung der einschlägigen technischen Mittel, um dem Kunden zur Wahrnehmung der diesem Grundsatz entsprechenden Verantwortung zu verhelfen. Die von GRASS-MERKUR im Rahmen der Nutzung der Cloud-Services durch Kunden anfallenden Daten (Konfigurationsdaten, Logging-Daten, Abrechnungsdaten) schützt GRASS-MERKUR so, dass Integrität und Vertraulichkeit gewahrt bleiben.
Rechenschaftspflicht: Der Verantwortliche ist für die Einhaltung der in dieser Tabelle genannten Grundsätze verantwortlich und muss dessen Einhaltung nachweisen können	
Der Kunde ist sich bei Nutzung der GRASS-MERKUR-Cloud-Services bewusst, dass die ihm zukommende und in dieser Tabelle aufgeführte Verantwortung ausschließlich von ihm getragen wird und verhält sich danach.	GRASS-MERKUR erkennt die in dieser Tabelle aufgeführten Grundsätze an und handelt danach. GRASS-MERKUR wird die Kunden der Cloud-Services hinsichtlich der Umsetzung der ihnen zukommenden Verantwortung mit der Bereitstellung dem jeweiligen Stand der Technik entsprechenden Lösungen und durch Beratung unterstützen.

6 Datenschutzregelungen

6.1 Geographische Lokation der Datenablage

Die IT-Systeme, welche die GRASS-MERKUR-Cloud-Services bereitstellen, befinden sich in Deutschland am Standort Hannover. Sämtliche von Kunden in die GRASS-MERKUR-Cloud eingebrachten Inhalte werden an diesem Standort abgelegt.

Kunden, die zusätzlich dazu eine räumlich entfernte Ablage Ihrer Inhalte wünschen (Spiegelung, Duplikation) können diesen Service auf Nachfrage erhalten. Der Ablageort der gespiegelten Inhalte ist dann ebenfalls in der Bundesrepublik Deutschland.

6.2 Kontrolle des Kunden über seine Inhalte auf dem Weg von und zur GRASS-MERKUR-Cloud

Es liegt in der Verantwortung des Kunden, mittels geeigneter Mechanismen und technischer Einrichtungen dafür Sorge zu tragen, dass während der Übertragung von Daten vor und zur GRASS-MERKUR-Cloud der Datentransfer abgesichert entsprechend dem Schutzbedarf der Kundeninhalte erfolgt. Das betrifft z.B. den Schutz vor Verfälschung, Sicherstellung der Vollständigkeit, Schutz vor Verlust während der Übertragung und Sicherstellung, dass die übertragenen Inhalte das beabsichtigte Ziel erreichen.

GRASS-MERKUR stellt technisch marktübliche Verfahren, Protokolle und Systeme an der Kundenschnittstelle dafür bereit und unterstützt die Kunden bei deren Einrichtung und Nutzung.

6.3 Rückgabe und Vernichtung von Kundeninhalten

Von Kunden in die GRASS-MERKUR-Cloud eingebrachte Inhalte werden an den Kunden nach Vertragsbeendigung vollständig zurückgegeben oder an einen anderen Dienstleister im Auftrag des Kunden weitergegeben. Die Durchführung dessen obliegt dem Kunden. GRASS-MERKUR stellt gängige technische Verfahren dazu bereit. Anschließend kann der Kunde seine Inhalte und von ihm genutzte Systeme in der GRASS-MERKUR-Cloud einschließlich eventuell vorhandener Datensicherungen unwiederbringlich löschen oder GRASS-MERKUR damit beauftragen. Im Zusammenhang mit der Nutzung der Cloud-Services angefallene Konfigurationsdaten, Logging-Daten und Verbrauchsdaten werden von GRASS-MERKUR nach Ablauf verpflichtender Aufbewahrungsfristen unwiederbringlich gelöscht. Zur Vernichtung der Daten und Kundeninhalte werden marktübliche und anerkannte Verfahren nach dem Stand der Technik eingesetzt, welche die Unwiederbringlichkeit sicherstellen. Dazu gehören Überschreiben, Entmagnetisierung oder Zerstörung von Datenträgern. GRASS-MERKUR kann damit auch nachweislich kompetente und vertrauenswürdige Dienstleister beauftragen.

6.4 Zugriff auf schon zuvor genutzte Speicherbereiche

GRASS-MERKUR stellt sicher, dass der Wiederverwendung zugeführte, zuvor durch andere Kunden oder für eigene Zwecke genutzte Speicherbreiche, so hinterlassen werden, dass die vorhergehende Verwendung und vormals gespeicherte Inhalte nicht ersichtlich sind.

6.5 Sichere Vernichtung bzw. Wiederverwendung von Systemen

GRASS-MERKUR stellt durch geeignete technische und organisatorische Maßnahmen sicher, dass zur

Wiederverwendung oder zur Entsorgung vorgesehene Geräte noch in der Verantwortung von GRASS-MERKUR so behandelt werden, dass keine Rückschlüsse auf die vorhergehende Verwendung, bzw. auf die vormals darauf abgelegten Daten gezogen werden können.

6.6 Papierausdrucke von personenbezogenen Daten

GRASS-MERKUR erstellt keine Papierausdrucke von personenbezogenen Daten, die in den eigenen Verantwortungsbereich fallen (Konfigurationsdaten, Logging-Daten, Abrechnungsdaten, → ***die*** Cloud)

6.7 Datensicherung (Information Backup)

GRASS-MERKUR bietet Datensicherungslösungen für Kunden an, welche Services in der GRASS-MERKUR-Cloud nutzen. Diese Datensicherungen konfiguriert und steuert der Kunde selbst. Der Kunde wählt aus, welche System und Daten in die Sicherungen einbezogen werden und wählt das geeignete Sicherungsregime (Häufigkeit der Sicherungen und Aufbewahrungsdauer) selbst aus. Auch die bedarfsweise notwendigen Rücksicherungen führt der Kunde selbst aus. Ablageort der Sicherungsmedien ist ausschließlich innerhalb des GRASS-MERKUR-Rechenzentrums, in dem die Cloud-Services erbracht werden, jedoch in einem separaten Brandabschnitt. Eine Auslagerung findet nicht statt. Sollten unter den vom Kunden zu sichernden Daten personenbezogene Informationen sein, so hat GRASS-MERKUR davon keine Kenntnis. Der Kunde allein ist dafür verantwortlich, auch bei Datensicherungen das notwendige Sicherheitsniveau einzuhalten. GRASS-MERKUR stellt innerhalb seiner Cloud Schutzmaßnahmen (Verschlüsselung und Zugriffsbeschränkungen) zur Nutzung durch den Kunden zur Verfügung. Bei deren Einrichtung leistet GRASS-MERKUR Hilfestellung.

GRASS-MERKUR überwacht und überprüft die Funktionsfähigkeit der Datensicherungslösungen laufend.

Durch Kunden für deren Datensicherungen benutzte Speicherbereiche und Medien werden vor einer Wiederverwendung so behandelt, dass eine Wiederherstellung der vorher darauf gespeicherten Daten nicht möglich ist.

6.8 Überwachung und Dokumentation von Datenrücksicherungen

Die Ausführung von Datenrücksicherungen (Restore) durch Kunden wird revisionssicher dokumentiert. Ein Kunde kann die Protokollierung für die seine Systeme und Daten betreffenden Rücksicherungen einsehen.

6.9 Event-Logging und Monitoring

Zu seinen Cloud-Services bietet GRASS-MERKUR den Kunden Möglichkeiten der Einrichtung einer Überwachung (Monitoring). Die Parametrierung der Überwachung übernimmt der Kunde selbst im Rahmen der durch die Cloud-Infrastruktur gebotenen Möglichkeiten. Speizelle Kundenanforderungen wird GRASS-MERKUR auf Umsetzungsfähigkeit prüfen und dem Kunden ggf. dabei behilflich sein. Durch die Überwachung festgestellte Abweichungen vom Normalzustand können als Events (Alarme) signalisiert werden. Kunden können das Monitoring auch verwenden, um Datenschutzverletzungen zu detektieren. Die sachgerechte Konfiguration und geeignete Verwendung obliegt jedoch vollständig dem Kunden. GRASS-MERKUR kennt die Systeme und Daten der Kunden in der Cloud nicht und kann deshalb die Wirksamkeit der Überwachung in Bezug auf die Kundendaten und Eignung der Parametrierung zur Feststellung von Datenschutzpannen nicht beurteilen.

Die Logging-Informationen, die GRASS-MERKUR im Rahmen seiner Verantwortung zum Betrieb der Cloud-Infrastruktur erzeugt, können personenbezogene Daten enthalten. Die Logging-Informationen sind durch

Zugriffsbeschränkungen geschützt, nur einem kleinen Personenkreis von GRASS-MERKUR zugänglich und grundsätzlich nicht durch Kunden einsehbar. Auf Anforderung kann GRASS-MERKUR die Daten für Kunden einsehbar machen. Einsehbar sind dann jedoch nur die den jeweiligen Kunden betreffenden Logging-Daten.

GRASS-MERKUR wird diese Informationen nur im Rahmen der Erfüllung der vertraglich geschuldeten Leistungen, zu Abrechnungszwecken oder zur Fehlerdiagnose und Entstörung einsetzen und nicht an Dritte weitergeben.

Nach dem Ende des Bedarfs, diese Informationen vorzuhalten wird GRASS-MERKUR die Logging-Informationen unwiederbringlich löschen, bzw. sicher überschrieben.

6.10 Schutz von Datenträgern, die das Rechenzentrum erreichen oder verlassen

Für den Umgang mit Datenträgern, die Kunden im Zuge der Nutzung der GRASS-MERKUR-Cloud-Services in das Rechenzentrum der GRASS-MERKUR einbringen bzw. verlassen, ist allein der Kunde zuständig.

Sollte GRASS-MERKUR mit dem Beschreiben, der Annahme bzw. dem Versand von Datenträgern durch Kunden beauftragt werden, wird GRASS-MERKUR die Datenträger mit einem gängigen zum Zeitpunkt des Beschreibens der Datenträger allgemein als sicher geltenden Verfahren verschlüsseln. Datenträger, die das Rechenzentrum von GRASS-MERKUR erreichen oder verlassen, werden registriert mit Typ des Datenträgers, (Serien-)Nummer des Datenträgers, Kunde, Datum, Uhrzeit, übergebender Person, annehmender Person und Quelle bzw. Ziel des Datenträgertransports.

6.11 Unverschlüsselte transportable Speichermedien und Geräte

Speichermedien und Geräte mit Speichermedien, die nicht mit einem als sicher anzunehmenden Verfahren verschlüsselt sind, sollen nur dann zum Einsatz kommen, wenn dies absolut unvermeidbar ist. Über den Einsatz solcher Objekte führt GRASS-MERKUR Protokoll.

6.12 Verschlüsselung über öffentliche Netze übertragener personenbezogener Daten

Es liegt in der Verantwortung des Kunden, zu entscheiden, ob und welche Art der Verschlüsselung des Transports seiner Daten in und aus der GRASS-MERKUR-Cloud zum Einsatz kommt. GRASS-MERKUR bietet hierzu Unterstützung an und stellt an der Kundenschnittstelle technische Möglichkeiten zur Verschlüsselung bereit.

Die in der Verantwortung von GRASS-MERKUR stehenden personenbezogenen Daten ***der*** Cloud (siehe Kapitel 3.2) wird GRASS-MERKUR nur verschlüsselt über öffentlich Netze übertragen.

6.13 Sichere Vernichtung von Ausdrucken

Entsprechend der Regelung in Kapitel 6.5 sind Papierausdrucke personenbezogener Daten untersagt. Andere Papierausdrucke werden entsprechend der von GRASS-MERKUR nach seiner Sicherheitspolicy vorgenommenen Vertraulichkeitseinstufung behandelt.

6.14 Benutzermanagement und Verwaltung von Benutzerkennungen

Die Systeme und Services der GRASS-MERKUR-Cloud sind mit einem auf allgemein anerkanntem Sicherheitsniveau und nach dem Stand der Technik ausgelegten Benutzermanagement ausgestattet, das die Vergabe abgestufter Benutzerberechtigungen erlaubt.

Die Vergabe und Zuordnung von Benutzerkennungen von Kundensystemen in der Cloud ist in der Verantwortung des Kunden. Kunden werden administrative Rechten an den von ihnen genutzten Cloud-Systemen eingeräumt, so dass die Kunden ihren Nutzern nach Bedarf selbstständig Zugriffsrechte zuweisen und entziehen können. Die Passwortverwaltung für Benutzer liegt in der Verantwortung der Kunden. Die Verantwortlichkeit liegt auch für die Fälle beim Kunden, wenn Passworte zu einem oder mehreren seiner Benutzerkonten ausgespäht wurden oder bekannt wurden und Benutzerkonten bzw. Kundeninhalte dadurch eventuell kompromittiert worden sind.

Administratoren von GRASS-MERKUR, die mit der Verwaltung der Cloud befasst sind, verfügen über jeweils eine eigene Benutzerkennung und sind gehalten, administrative Tätigkeiten unter ihrer eigenen Benutzerkennung durchzuführen.

6.15 Vergabe eindeutiger Benutzerkennungen

Die Vergabe und Zuordnung von Benutzerkennungen von Kundensystemen in der Cloud ist in der Verantwortung des Kunden. Die GRASS-MERKUR-Cloud stellt ein umfangreich konfigurierbares Berechtigungs-Management zur Verfügung, damit Kunden eindeutige Benutzerkennungen zu jeder handelnden Person vergeben können.

Jedem Mitarbeiter von GRASS-MERKUR, der mit der Administration der Cloud-Services beschäftigt ist, wird eine eindeutige Benutzerkennung zugeteilt, welche diese Person für alle Tätigkeiten zu verwenden hat.

Deaktivierte oder abgelaufene Benutzerkennungen, die GRASS-MERKUR-Mitarbeitern oder Kunden zugewiesen worden sind, werden nicht wiederverwendet.

6.16 Liste autorisierter Benutzer

Die Vergabe und Zuordnung von Benutzerkennungen von Kundensystemen in der Cloud ist in der Verantwortung des Kunden.

GRASS-MERKUR führt eine Dokumentation über die Administratoren, die zur Verwaltung der GRASS-MERKUR-Cloud berechtigt sind.

6.17 Trennung von Entwicklungs-, Test- und Produktions-umgebungen

GRASS-MERKUR unterhält neben der Produktionsumgebung der Cloud-Services, auf der die Kunden ihre Inhalte ablegen, weitere Umgebungen. Personenbezogene Daten auf diesen Umgebungen werden mit demselben Sicherheitsniveau und denselben Sicherheitsmaßnahmen behandelt wie die Daten der Produktionsumgebung.

6.18 Dokumentation der Freigabe personenbezogener Daten

GRASS-MERKUR wird die im Kontext der Cloud-Services anfallenden personenbezogenen Daten nicht

ohne Veranlassung im Rahmen der normalen Cloud-Service-Leistungen herausgeben, sondern

a) nur unter den im Kapitel 4 angegebenen gesetzlichen Pflichten den staatlichen Stellen übergeben.

b) auf Anforderung von Kunden, nach Nachweis der Autorisierung der anfordernden Stelle/Person des Kunden Einsicht gewähren. Die Einsichtgewährung erstreckt sich nur auf Daten, die in Bezug zu dem anfordernden Kunden stehen, nicht auf Daten von GRASS-MERKUR oder anderer Kunden.

Zu jeder Herausgabe und Einsichtgewährung, wird GRASS-MERKUR folgendes in eigenen Unterlagen dokumentieren: Datenkategorie, Datenquelle, Umfang der Daten, den Empfänger der Daten und den Zeitpunkt der Herausgabe.

6.19 Externe Dienstleister der GRASS-MERKUR (Cloud-Partner)

GRASS-MERKUR kann externe Subunternehmer (Cloud-Partner) beauftragen, die GRASS-MERKUR bei der Erbringung der Services unterstützen. Die Cloud-Partner erlangen keinen Zugriff auf Kundeninhalte. Darüber hinaus setzt GRASS-MERKUR nur solche Cloud-Partner ein, denen vertraut wird, führt eine Risikobetrachtung durch und setzt angemessene vertragliche Schutzmaßnahmen ein, die überwacht wird, um zu gewährleisten, dass die geforderten Standards aufrecht erhalten bleiben.

GRASS-MERKUR wird Interessenten an den Cloud-Services der GRASS-MERKUR die Namen die Cloud-Partner vor Abschluss eines Vertrages mit diesem Interessenten benennen.

Änderungen bei Cloud-Partnern wird GRASS-MERKUR den Kunden kommunizieren.

6.20 Dienstleister des Kunden

Wie bereits oben in diesem Dokument angemerkt, ist die GRASS-MERKUR-Umgebung auch mit anderen Services verbunden, die direkt durch Dritte erbracht werden (z.B. Internetdienstanbieter). Diese Dritten bleiben für ihr eigenes System verantwortlich, einschließlich der Sicherheit, und GRASS-MERKUR ist nicht für die Aktivitäten dieser Dritten verantwortlich.

6.21 Informations-Sicherheits-Vorfalls-Management (Incident)

GRASS-MERKUR betreibt im Rahmen des Informations-Sicherheits-Management-Systems (ISMS) einen standardkonformen Incident-Management-Prozess, der auch auf die Cloud-Services der GRASS-MERKUR angewendet wird. Bei jedem als sicherheitsrelevant eingestuften Incident wird in diesem Prozess zusätzlich geprüft, ob es hierbei zu einer Datenschutzverletzung gekommen ist. Falls die Bestätigung dazu vorliegt, wird weiter verfahren wie in Abschnitt 6.22 beschrieben.

6.22 Umgang mit Datenschutzverletzungen

Da die Kunden bei der Nutzung von GRASS-MERKUR die Verwaltung von und die Kontrolle über personenbezogene Daten behalten, bleiben die Kunden verantwortlich dafür, ihre eigene Umgebung auf Datenschutzverletzungen hin zu überwachen und die Aufsichtsbehörden und die betroffenen Personen nach Maßgabe der anwendbaren Gesetze hierüber zu informieren. Nur der Kunde hat die Möglichkeit, dieser Verantwortung nachzukommen. Kunden kontrollieren ihre eigenen Zugriffsschlüssel und bestimmen, wer berechtigt ist, auf ihren GRASS-MERKUR-Account zuzugreifen. Unter diesen Umständen hat GRASS-MERKUR keinen Einblick in die Zugriffsschlüssel oder darin, wer und wer nicht berechtigt ist, sich in einen Account einzu-

loggen. Daher ist der Kunde dafür verantwortlich, die Nutzung, den Missbrauch, die Vergabe oder den Verlust von Zugriffsschlüsseln zu überwachen.

GRASS-MERKUR wird den Kunden unverzüglich benachrichtigen, wenn GRASS-MERKUR tatsächliche Kenntnis einer bestätigten Datenschutzverletzung zu den personenbezogenen Daten ***der*** Cloud hat. In diesen Fällen wird zur Erfüllung gesetzlicher Pflichten zugleich auch die für GRASS-MERKUR zuständige Niedersächsische Landesdatenschutzbehörde informiert.

Die Information wird enthalten:

- Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten
- Name und Kontaktdaten einer Anlaufstelle für weitere Informationen
- Beschreibung der wahrscheinlichen Folgen
- Beschreibung der bereits ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung oder zur Abmilderung möglicher nachteiliger Auswirkungen

Kunden werden auch informiert, falls GRASS-MERKUR die bestätigte Kenntnis darüber hat, dass unerlaubte Zugriffe auf Systeme der Kunden erfolgten, Datenverlust oder Datenveränderungen an Kundensystemen ***in*** der Cloud stattgefunden haben.

7 Schlussbemerkungen

GRASS-MERKUR lässt sein Informations-Sicherheits-Management-System (ISMS) und seine Cloud-Services jährlich durch eine externe, unabhängige Organisation untersuchen und zertifizieren. Die zur Prüfung herangezogenen Standards sind ISO/IEC 27001, ISO/IEC 27017 und ISO/IEC 27018 in der jeweils aktuellen Fassung. GRASS-MERKUR erbringt mit der Vorlage der Zertifikate den Beweis und dokumentiert den unbedingten Willen, Kunden gegenüber höchste Ansprüche an Sicherheit seiner IT-Services und den Datenschutz erfüllen zu wollen. Zugleich schafft GRASS-MERKUR damit Transparenz für seine Services und seine Leistungserstellung.
Für GRASS-MERKUR haben die drei Dimensionen der IT-Sicherheit (Verfügbarkeit, Vertraulichkeit und Integrität) immer höchste Priorität. GRASS-MERKUR erbringt Services für anspruchsvolle Kunden, die ihrerseits hohe Ansprüche erfüllen wollen oder müssen.

Kunden, die sich über die ihnen obliegenden datenschutzrechtlichen Verpflichtungen Gedanken machen, sollten zunächst sicherstellen, dass sie die anwendbaren Anforderungen identifizieren und verstehen und bei Bedarf sachkundigen Rat suchen. GRASS-MERKUR wird Kunden bei der Erfüllung dieser Anforderung im Zuge der Nutzung seiner Cloud-Services beraten und unterstützen.

8 Mitgeltende Dokumente

- Leitlinie Sicherheit der GRASS-MERKUR-Cloud

9 Revision

Die Historie wird nach unten fortgeschrieben.

GRASS-MERKUR
Leitlinie
Datenschutzinformationen zu Cloud-Services

Version	Stand	Autor	Änderungen
v0.1.0	20180105	Dr. Oliver Kunert	initiale Version, Entwurf
v1.0.0	20190712	Jochen Kaiser	Freigabeversion
v1.1.0	20191016	Dr. Oliver Kunert	- Umformulierung im Kapitel 5 Datenschutzgrundsätze, Unterabschnitt Vertraulichkeit und Integrität - Anpassung: ISO/IEC 270.. in der jeweils aktuellen Fassung statt Jahreszahl