Oracle Richtlinien für Cloud-Hosting und -Lieferung

Datum des Inkrafttretens: Februar 2026; Version 3.11

INHALTSVERZEICHNIS

Übersicht **4**

1. Oracle Richtlinie für Cloud-Sicherheit **5**

1.1 Oracle Information Security Practices – Allgemeines 5
1.2 Physische Schutzvorkehrungen 6
1.3 Systemzugriffskontrollen 6
1.4 Datenzugriffskontrolle 7
1.5 Benutzerverschlüsselung für externe Verbindungen 7
1.6 Eingabesteuerung 7
1.7 Daten- und Netzwerktrennung 7
1.8 Vertraulichkeit und Schulung 8
1.9 Management von Ressourcen 8
1.10 Interne Informationssicherheitsrichtlinien von Oracle 8
1.11 Interne Sicherheitsüberprüfungen und Durchsetzung 8
1.12 Externe Überprüfungen 8
1.13 Oracle Software Security Assurance 9
1.14 Sicherheitsprotokolle 9
1.15 Andere Verpflichtungen in Bezug auf Kundensicherheit 9

2. Oracle Richtlinie für Cloud Service-Kontinuität **10**

2.1 Hochverfügbarkeitsstrategie für Oracle Cloud Services 10
2.2 Backupstrategie für Oracle Cloud Services 10
2.3 Oracle Cloud Services Continuity Policy 10

3. Oracle Cloud Servicelevel-Vereinbarung **11**

3.1 Betriebszeiten 11
3.2 Serviceverfügbarkeit 11
3.2.1 Bewertung der Verfügbarkeit 11
3.2.2 Meldung der Verfügbarkeit 11
3.2.3 Servicegutschriften 11
3.3 Definition von „ungeplante Ausfallzeit“ (Nichtverfügbarkeit) 12
3.4 Überwachung 12
3.4.1 Überwachungs- und Testtools des Kunden 12

4. Oracle Richtlinie für Cloud-Change-Management **13**

4.1 Oracle Cloud Change Management und Wartung 13
4.1.1 Sicherheitswartung 13
4.1.2 Migration von Rechenzentren 14
4.1.3 Softwareupdates 14
4.1.4 End of Life 14

5. Oracle Richtlinie für Cloud-Support **14**

5.1 Bedingungen für Oracle Cloud Support 14
5.1.1 Supportvergütungen 14
5.1.2 Supportzeitraum 14
5.1.3 Technische Ansprechpartner 15
5.1.4 Oracle Cloud Support 15
5.2 Oracle Cloud-Kundensupportsysteme 15
5.2.1 Oracle Cloud-Kundensupportportal 15

5.2.2 Telefonische Liveunterstützung 16
5.3 Severity-Definitionen 16
5.3.1 Severity 1 (Kritischer Ausfall) 16
5.3.2 Severity 2 (Erhebliche Beeinträchtigung) 17
5.3.3 Severity 3 (Technisches Problem) 17
5.3.4 Severity 4 (Allgemeiner Hinweis) 17
5.4 Änderung der Service-Request-Severity 17
5.4.1 Anfänglicher Severity-Level 17
5.4.2 Herabstufung eines Service-Request-Levels 17
5.4.3 Hochstufung eines Service-Request-Levels 17
5.4.4 Einhaltung der Severity-Level-Definitionen 17
5.5 Service-Request-Eskalation 17
6. Oracle Richtlinie für Aussetzung und Beendigung von Cloud Services 18
6.1 Kündigung von Oracle Cloud Services 18
7. KI-Bestimmungen 19
8. Nutzung der Services 19

ÜBERSICHT

In diesen *Oracle Cloud Hosting and Delivery Policies* (Oracle Richtlinien für Cloud-Hosting und -Lieferung) (die „Delivery Policies“) werden die von Ihnen bestellten Oracle Cloud Services beschrieben. In diesen Delivery Policies wird unter Umständen auf andere Oracle Cloud-Richtliniendokumente Bezug genommen; jeder Verweis in diesen Delivery Policies oder in anderen Richtliniendokumenten auf „Kunde“ bezieht sich auf „Sie“, wie in Ihrem Auftrag definiert. Alle Zusagen in diesen Delivery Policies gelten für Produktions-Cloud Services, sofern nichts anderes angegeben ist.

Verweise in diesen Delivery Policies auf die „Rechenzentrumsregion“ eines Cloud Service bezeichnen (i) die geografische Region, die in Ihrem Auftrag für diese Services angeführt ist, oder, (ii) soweit zutreffend, das Land oder die umfassendere geografische Region, das bzw. die sich auf den Rechenzentrumsort bezieht, den Sie bei der Aktivierung der Instanz solcher Services ausgewählt haben. Für die Rechenzentrumsregion, die für Ihre bestellten Cloud Services gilt, gilt Folgendes:

- „Europa“ bezeichnet die Mitgliedsländer der Europäischen Union, das Vereinigte Königreich und die Schweiz zusammen; und
- „APAC“ bezeichnet den asiatisch-pazifischen Raum, mit Ausnahme von China, da Oracle keine Rechenzentren in China unterhält.
- „Nordamerika“ bezeichnet die geografischen Regionen der Vereinigten Staaten von Amerika und Kanadas, es sei denn, die Entität, die Cloud Services erwirbt, entscheidet sich für eine anfängliche Bereitstellung im Land Mexiko. In diesem Fall bezieht sich Nordamerika auf die geografischen Regionen der Vereinigten Staaten von Amerika, Kanadas und Mexikos.

Im Zusammenhang mit Ihren beauftragten Oracle Cloud Services werden Ihre Inhalte in der für diese Services geltenden Rechenzentrumsregion gespeichert. Zur Unterstützung der Datenredundanz steht es Oracle frei, Ihre Inhalte auf andere Standorte innerhalb der bezeichneten Rechenzentrumsregion zu replizieren. Die Begriffe, die in den vorliegenden Delivery Policies nicht anderweitig definiert werden, haben jeweils die im relevanten Oracle Vertrag, Ihrem Auftragsdokument oder in der relevanten Oracle Richtlinie festgelegten Bedeutungen. Die vorliegenden Delivery Policies werden zweimal im Jahr aktualisiert.

Ihr Auftrag oder die Leistungsbeschreibungen von Oracle (entsprechend den Definitionen in Ihrem Vertrag für Oracle Cloud Services, zu denen auch die Oracle Cloud Services Pillar-Dokumentation, die Service Descriptions sowie weitere Definitionen nach dem Oracle Cloud Services-Vertrag gehören) umfasst bzw. umfassen gegebenenfalls weitere Details oder Ausnahmen im Zusammenhang mit den spezifischen Oracle Cloud Services. Die Oracle Cloud Service Pillar-Dokumentation, die Service Descriptions und die Programmdokumentation für Oracle Cloud Services sind abrufbar unter https://www.oracle.com/contracts.

Sie stimmen zu, alle von Oracle angeforderten Maßnahmen zu ergreifen und Oracle andernfalls die vernünftigerweise erforderlichen Information und Zugriffsmöglichkeiten sowie die erforderliche Mitwirkung bereitzustellen, damit Oracle die Oracle Cloud Services implementieren und verwalten kann, einschließlich der Implementierung jedweder Änderungen an Oracle Cloud Service durch Oracle, wie im Abschnitt *Oracle Cloud Change Management Policy (Oracle Richtlinie für Cloud-Change-Management)* dargelegt.

Oracle Cloud Services werden gemäß den Bestimmungen des Oracle Vertrags, Ihres Auftrags und den für diese Services geltenden Leistungsbeschreibungen bereitgestellt. Voraussetzung für die Erbringung der Oracle Cloud Services durch Oracle ist, dass Sie und Ihre Benutzer den in den genannten Dokumenten und den darin eingebundenen Richtlinien festgelegten Verpflichtungen und Verantwortlichkeiten nachkommen. Diese Delivery Policies und die Dokumente, auf die hierin verwiesen wird, können von Oracle nach eigenem Ermessen geändert werden. Änderungen der Richtlinien von Oracle führen jedoch nicht zu einer wesentlichen Verringerung des Umfangs der Leistung, der Funktionalität, der Sicherheit oder der Verfügbarkeit der Oracle Cloud Services, die während des Leistungszeitraums Ihres Auftrags bereitgestellt werden.

Oracle Cloud Services werden in Rechenzentren oder durch von Oracle beauftragte Drittdienstleister von Infrastrukturdiensten bereitgestellt, mit Ausnahme von Oracle Cloud at Customer Services. Oracle Cloud at Customer Services sind Public Cloud Services, die in Ihrem Rechenzentrum oder in einem von Ihnen beauftragten Rechenzentrum einer Drittpartei bereitgestellt werden. Sie können diese Services einzeln erwerben, oder sie können als zugrunde liegende Plattform für andere Oracle Cloud Services eingesetzt werden. Für Oracle Cloud at Customer Services liefert Oracle Ihrem Rechenzentrum bestimmte Hardwarekomponenten, einschließlich der Gateway-Ausrüstung, die Oracle für den Betrieb dieser Services benötigt. Sie sind dafür verantwortlich, für ausreichend Platz, Stromversorgung und Kühlung für die Bereitstellung der Oracle Hardware (einschließlich Gateway-Ausrüstung) zu sorgen, und eine angemessene Netzwerkverbindung für Oracle Cloud Operations sicherzustellen, um auf die Services zugreifen zu können. Es obliegt der alleinigen Verantwortung von Oracle, die Oracle Hardwarekomponenten (einschließlich Gateway-Ausrüstung) zu warten.

Diese Delivery Policies gelten nicht für Oracle BigMachines Express oder andere Oracle Cloud-Angebote, wie von Oracle in Ihrem Auftrag oder den anwendbaren Service Descriptions angegeben.

1. ORACLE RICHTLINIE FÜR CLOUD-SICHERHEIT

1.1 Oracle Information Security Practices – Allgemeines

Oracle hat für die Oracle Cloud Services Sicherheitskontrollen und -verfahren eingeführt, die dazu dienen, die Vertraulichkeit, Integrität und Verfügbarkeit Ihrer Inhalte, die von Oracle in Ihren Oracle Cloud Services gehostet werden, zu schützen und Ihre Inhalte vor unbefugten Verarbeitungsaktivitäten wie dem Verlust oder der unrechtmäßigen Vernichtung von Daten zu schützen. Oracle arbeitet kontinuierlich daran, diese Sicherheitskontrollen und -verfahren zu stärken und zu verbessern.

Oracle Cloud Services werden unter Verfahren betrieben, die den Kontrollmechanismen für die Informationssicherheit der Norm ISO/IEC 27002 entsprechen, aus denen eine umfassende Auswahl von Kontrollmechanismen angewendet wird. Oracle Cloud Services halten die Vorschriften der Regelwerke National Institute of Standards and Technology („NIST“) 800-53 und 800-171 ein.

Die Informationssicherheitsverfahren von Oracle Cloud definieren und regeln für Oracle Cloud Services und Ihre Nutzung dieser Oracle Cloud Services geltende Sicherheitsbereiche.

Oracle Personal (einschließlich Mitarbeiter, Auftragnehmer und vorübergehende Mitarbeiter) unterliegt den Informationssicherheitsverfahren von Oracle und allen anderen zusätzlichen Richtlinien, die ihre Beschäftigung oder die für Oracle von ihnen erbrachten Dienstleistungen regeln.

In Bezug auf Informationssicherheit verfolgt Oracle Cloud einen ganzheitlichen Ansatz und wendet eine mehrstufige Verteidigungsstrategie an. Dabei sollen die Sicherheitsverfahren für Netzwerke, Betriebssysteme, Datenbanken und Software einander mit starken internen Kontrollen, durch Governance und Beaufsichtigung ergänzen.

Bei denjenigen Oracle Cloud Services, die es Ihnen ermöglichen, Ihr Sicherheitsverhalten zu konfigurieren, sind Sie, sofern nicht anders angegeben, für die Konfiguration, den Betrieb, die Wartung und die Sicherung der Betriebssysteme und anderer zugehöriger Software dieser ausgewählten Oracle Cloud Services (einschließlich Ihrer Inhalte) verantwortlich, die nicht von Oracle bereitgestellt werden. Sie sind dafür verantwortlich, angemessene Vorkehrungen für Sicherheit, Schutz und Backup Ihrer Inhalte zu treffen, worunter auch die Anwendung von Verschlüsselungstechnologie zum Schutz Ihrer Inhalte vor unbefugtem Zugriff und die regelmäßige Archivierung Ihrer Inhalte fallen können.

1.2 Physische Schutzvorkehrungen

Oracle setzt Maßnahmen um, die verhindern sollen, dass unbefugte Personen Zugang zu von Oracle verwalteten Computeranlagen, auf denen Ihre Inhalte gehostet werden, erhalten, so wie den Einsatz von Sicherheitspersonal und Zugangsbeschränkungen für Gebäude sowie ausgewiesene Rechenzentrumsanlagen. Von Oracle verwaltete Bürostandorte und Cloud-Infrastruktureinrichtungen sind gesichert. Oracle verlangt zudem von seinen Lieferanten, Einrichtungen, die Ihre Inhalte hosten, auf ähnliche Weise zu sichern. Zu den üblichen Sicherheitsmaßnahmen, die zwischen Bürostandorten und den von Oracle verwalteten Nebenstandorten/Rechenzentren zum Einsatz kommen, gehören zurzeit beispielsweise folgende:

- Der physische Zugang erfordert eine Autorisierung und wird überwacht
- Alle Mitarbeiter, Unterauftragnehmer und autorisierten Besucher müssen am Standort deutlich sichtbar einen offiziellen Ausweis tragen
- Besucher müssen sich anmelden und müssen in Oracle Einrichtungen von Oracle Mitarbeitern begleitet werden
- Der Besitz von Schlüsseln/Zugangskarten sowie die Möglichkeit zum Betreten der Räumlichkeiten wird überwacht. Mitarbeiter, die Oracle verlassen, müssen ihre Schlüssel/Karten zurückgeben.

Dieser Abschnitt gilt nicht für Oracle Cloud at Customer Services. Sie müssen Ihre eigenen sicheren Computeranlagen für das Hosting und den Betrieb der Hardware bei Oracle Cloud at Customer Services (einschließlich der Gateway-Ausrüstung) sowie Netzwerkverbindungen bereitstellen, damit Oracle die Oracle Cloud at Customer Services bereitstellen kann.

1.3 Systemzugriffskontrollen

Oracle Richtlinien verlangen die Anwendung der Multifaktor-Authentifizierung (MFA), dokumentierte Autorisierungskontrollen und die Protokollierung des Zugriffs. Die Verwendung von MFA ist für alle Benutzer, die auf Oracle Cloud Services zugreifen, obligatorisch. Wenn die von Oracle bereitgestellte Option für MFA für einen Oracle Cloud Service verfügbar ist, müssen Sie diese aktivieren und durchsetzen. Wenn Sie einen externen Identitätsanbieter mit einem Oracle Cloud Service verwenden, müssen Sie ihn so konfigurieren, dass MFA für alle Benutzer erforderlich ist, die auf solche Cloud Services zugreifen. Sie sind allein verantwortlich für alle negativen Folgen für Sie oder Ihre Benutzer im Zusammenhang mit Ihren

Cloud Services, die durch die Verwendung der von Oracle bereitgestellten MFA-Option, sofern verfügbar, hätten vermieden werden können.

Jedweder Remotezugriff auf das Oracle Cloud Network durch Oracle Mitarbeiter, die Zugriff auf Ihre Inhalte haben, wird durch die Verwendung eines Virtual Private Network eingeschränkt, das MFA verwendet. Zusätzlich zur obligatorischen Verwendung eines Virtual Private Network führt Oracle, bevor Oracle Mitarbeiter Zugang zum Oracle Cloud Network erhalten, Gerätezustandsprüfungen durch und verfügt über Kontrollmechanismen wie Bastion Hosts. Oracle verbietet (sowohl durch Richtlinien als auch durch technische Kontrollen) die Verwendung von persönlichen Geräten für den Zugriff auf das Oracle Cloud Network und die Oracle Cloud Services.

1.4 Datenzugriffskontrolle

Bei von Oracle verwalteten Servicekomponenten ist der Zugriff von Oracle auf Ihre Inhalte auf autorisierte Mitarbeiter beschränkt.

In Bezug auf den Zugriff von Oracle Mitarbeitern auf die Oracle Cloud Services (einschließlich des Zugriffs auf Ihre in den Oracle Cloud Services befindlichen Inhalte) setzt Oracle funktionsbasierte Zugriffskontrolle („Role Based Access Controls, RBAC“) durch und wendet die Zugriffsverwaltungsprinzipien „Need-to-Know“ (Kenntnis nur, wenn nötig), „Least Privilege“ (geringstmögliche Berechtigung) und „Segregation of Duties“ (Funktionstrennung) an. Darüber hinaus bietet Oracle einen Mechanismus, mit dem Sie den Zugriff Ihrer Benutzer auf die Oracle Cloud Services und auf Ihre Inhalte steuern können.

1.5 Benutzerverschlüsselung für externe Verbindungen

Ihr Zugriff auf Oracle Cloud Services erfolgt über ein von Oracle zur Verfügung gestelltes sicheres Kommunikationsprotokoll. Wenn der Zugriff über eine Transport Layer Security-(TLS-)verschlüsselte Verbindung erfolgt, wird in Bezug auf die Verbindung eine Verschlüsselung von mindestens 128 Bit ausgehandelt. Die Länge des zur Erzeugung des Chiffrierschlüssels verwendeten Private Key beträgt mindestens 2048 Bit. TLS wird für alle von Oracle bereitgestellten webbasierten Anwendungen implementiert oder konfigurierbar gemacht. Es wird empfohlen, dass für die Verbindung zu den Cloud Services die neusten zur Verfügung stehenden Browser verwendet werden, die mit höheren Verschlüsselungsstärken kompatibel sind und über eine verbesserte Sicherheit verfügen. Die Liste der empfohlenen Browser für die jeweiligen Releases der Oracle Cloud Services wird über ein Portal, auf das Sie zugreifen können, oder in den entsprechenden Service Descriptions für die Oracle Cloud Services zur Verfügung gestellt. In manchen Fällen akzeptieren Drittanbieter-Websites, die Sie in die Oracle Cloud Services integrieren möchten, wie z. B. einen Dienst für soziale Medien, keine verschlüsselten Verbindungen. Bei Oracle Cloud Services, für die Oracle HTTP-Verbindungen mit der Drittanbieter-Website erlaubt, aktiviert Oracle diese HTTP-Verbindungen zusätzlich zu HTTPS-Verbindungen.

1.6 Eingabesteuerung

Die Quelle Ihrer Inhalte unterliegt Ihrer Kontrolle und Verantwortung, und die Integration Ihrer Inhalte in die Oracle Cloud Services wird von Ihnen verwaltet.

1.7 Daten- und Netzwerktrennung

Ihre Inhalte sind von den Inhalten anderer Kunden, die in den Oracle Cloud Services gehostet werden, logisch oder physisch getrennt. Alle Oracle Cloud-Netzwerke sind von den Unternehmensnetzwerken von Oracle getrennt.

1.8 Vertraulichkeit und Schulung

Oracle Mitarbeiter unterliegen Geheimhaltungsvereinbarungen und sind verpflichtet, bei ihrer Einstellung eine Schulung zum Thema Datenschutz zu absolvieren. Danach müssen alle Oracle Mitarbeiter in regelmäßigen Abständen Schulungen in Übereinstimmung mit den geltenden Richtlinien von Oracle zur Sensibilisierung für Sicherheit und Datenschutz absolvieren.

1.9 Management von Ressourcen

Oracle befolgt formelle Verfahren zur Nachverfolgung, Verwaltung, zum Schutz und zur Außerbetriebnahme von Vermögenswerten. Zu diesen Verantwortlichkeiten können die Überprüfung von Zugriffsanfragen und deren Genehmigung nur bei geschäftlicher Erfordernis sowie die Inventarisierung von Anlagen gehören.

Sie sind verantwortlich für die von Ihnen kontrollierten Ressourcen, die die Oracle Cloud Services nutzen oder in diese integriert sind, einschließlich der Bestimmung der geeigneten Informationsklassifizierung für Ihre Inhalte und der Frage, ob die von Oracle Cloud Services bereitgestellten dokumentierten Kontrollen für Ihre Inhalte geeignet sind.

1.10 Interne Informationssicherheitsrichtlinien von Oracle

Die Informationssicherheitsrichtlinien von Oracle Cloud definieren und regeln für Oracle Cloud Services und Ihre Nutzung der Oracle Cloud Services geltende Sicherheitsbereiche. Oracle Mitarbeiter unterliegen den Oracle Corporate Information Security Policies (Unternehmensrichtlinien für Informationssicherheit von Oracle) und allen anderen zusätzlichen Richtlinien, die ihre Beschäftigung oder die für Oracle von ihnen erbrachten Dienstleistungen regeln. Das Oracle Information Security Program (Informationssicherheitsprogramm, „ISP“) besteht aus dokumentierten Richtlinien, die Risikofaktoren, einschließlich Cyber- und Sicherheitsfaktoren, mit begleitenden abgeleiteten Verfahren, Standards und Richtlinien, die für die effektive Umsetzung der Richtlinie erforderlich sind, berücksichtigen. Oracle ISP soll die Vertraulichkeit, Integrität, Geheimhaltung, Kontinuität und Verfügbarkeit Ihrer Inhalte, die von Oracle in Ihren Oracle Cloud Services gehostet werden, durch effektive Sicherheitsmanagementpraktiken und -kontrollen gewährleisten. Oracle ISP wird jährlich durch das Oracle Security Oversight Committee überprüft und bei Bedarf aktualisiert.

1.11 Interne Sicherheitsüberprüfungen und Durchsetzung

Oracle setzt interne Prozesse ein, um regelmäßig die Wirksamkeit der in diesem Abschnitt beschriebenen technischen und organisatorischen Sicherheitsmaßnahmen zu testen, zu beurteilen, zu bewerten und aufrecht zu erhalten.

1.12 Externe Überprüfungen

Oracle kann unabhängige Überprüfungen der Oracle Cloud Services durch Dritte in den folgenden Bereichen durchführen (der Umfang solcher Überprüfungen kann je nach Service und Land variieren):

- SOC 1- (auf Grundlage von Statement on Standards for Attestation Engagements (SSAE) Nr. 18) bzw. SOC 2-Berichte (auf Grundlage von „Trust Services Criteria“ (Trust-Services-Kriterien)).
- Andere Sicherheitstests von unabhängigen Dritten zur Überprüfung der Effektivität von administrativen und technischen Kontrollen

Während des Leistungszeitraums können Sie die jeweils aktuellen SOC-Berichte über die Ihnen zur Verfügung stehenden Methoden (z. B. Selfservicekonsole oder Service Request (SR)) abrufen, soweit solche Berichte für die betreffenden Cloud Services gepflegt werden. Solche Berichte enthalten eine Überprüfung der vorhandenen Kontrollmechanismen und können aus SOC 1- und/oder SOC 2-Berichten bestehen. Sie stimmen zu, dass Sie die SOC-Berichte von Oracle und alle darin enthaltenen Informationen als vertrauliche Informationen von Oracle in Übereinstimmung mit den Geheimhaltungsbestimmungen Ihres Vertrags schützen werden. Ferner bestätigen Sie und stimmen zu, dass (1) Sie die SOC-Berichte nur zur Beurteilung der Sicherheitskontrollen von Oracle für die gegenständlichen Cloud Services verwenden, (2) die SOC-Berichte ohne Gewährleistung ausgegeben werden und (3) Oracle sämtliche Rechte an den SOC-Berichten behält.

1.13 Oracle Software Security Assurance

Mit Oracle Software Security Assurance (OSSA) sorgt Oracle für Sicherheit bei der Konzipierung, Entwicklung, Erprobung und Wartung seiner Produkte, unabhängig davon, ob sie von Kunden vor Ort genutzt oder über die Oracle Cloud bereitgestellt werden. Eine Beschreibung des OSSA-Programms kann hier abgerufen werden: https://www.oracle.com/corporate/security-practices/assurance/.

1.14 Sicherheitsprotokolle

Oracle protokolliert bestimmte sicherheitsrelevante Aktivitäten auf Betriebssystemen, Anwendungen, Datenbanken und Netzwerkgeräten. Die Systeme sind so konfiguriert, dass sie standardmäßige Sicherheitsaktivitäten, Zugriffe auf Informationen oder Programme, Systemereignisse wie Warnungen, Konsolenmeldungen und Systemfehler protokollieren.

Oracle prüft die Protokolle zur Untersuchung von Sicherheitsereignissen und für forensische Zwecke. Erkannte außergewöhnliche Aktivitäten fließen in das Verfahren für das Management von Sicherheitsereignisse ein. Sicherheitsprotokolle werden im Security Information and Event Management-System (oder einem ähnlichen System) in einem nativen, unveränderten Format gespeichert und in Übereinstimmung mit den internen Richtlinien von Oracle aufbewahrt. Sicherheitsprotokolle werden mindestens 1 Jahr lang online aufbewahrt. Diese Protokolle werden von Oracle aufbewahrt und für unsere internen Sicherheitsoperationen verwendet.

1.15 Andere Verpflichtungen in Bezug auf Kundensicherheit

Sie sind für Folgendes verantwortlich:

- Die Implementierung Ihres eigenen umfassenden Systems aus Sicherheits-, Betriebsrichtlinien, -standards und -verfahren
- Die Durchführung von Integritäts- und Sicherheitsprüfungen, wie das Scannen nach Schwachstellen, Viren, Malware und sonstigen Schädlichkeitsanzeigen in (i) Ihren Daten und Dateien, bevor diese in die Oracle Cloud Services importiert oder hochgeladen werden, (ii) Ihren Inhalten für Oracle Cloud Services, die Ihnen die Konfiguration Ihres Sicherheitsverhaltens ermöglichen; und (iii) Ihren Anpassungen und Integrationen
- Die Aufrechterhaltung von vom Kunden verwalteten Accounts in Übereinstimmung mit Ihren Richtlinien und bewährten Sicherheitsverfahren
- Für Oracle Cloud at Customer Services sind Sie außerdem für Folgendes verantwortlich:

- Angemessene physische und Netzwerksicherheit
- Sicherheitskontrollen und Netzwerküberwachung zur Verringerung des Risikos von Ereignissen, die eine Bedrohung für die Datenvertraulichkeit, -verfügbarkeit oder -integrität darstellen könnten.

2. ORACLE RICHTLINIE FÜR CLOUD SERVICE-KONTINUITÄT

2.1 Hochverfügbarkeitsstrategie für Oracle Cloud Services

Oracle stellt die Oracle Cloud Services auf einer resilienten Computing-Infrastruktur bereit, die darauf ausgelegt ist, die Verfügbarkeit und Kontinuität der Services im Falle eines Vorfalls, der die Services betrifft, aufrechtzuerhalten. Die von Oracle für das Hosting der Oracle Cloud Services beauftragten Rechenzentren verfügen über redundante Komponenten und eine redundante Stromversorgung mit Backupgeneratoren, und Oracle kann Redundanz in einer oder mehreren Layers, einschließlich Netzwerkinfrastruktur, Programmserver, Datenbankserver und/oder Speicher, integrieren.

2.2 Backupstrategie für Oracle Cloud Services

Oracle erstellt in regelmäßigen Abständen Backups Ihrer Inhalte in Ihrer Instanz der Oracle Cloud Services zur alleinigen Verwendung durch Oracle, um den Datenverlust im Falle eines Vorfalls zu minimieren. Backups werden am primären Standort der Erbringung der Oracle Cloud Services gespeichert und können zu Aufbewahrungszwecken auch an einem anderen Standort gespeichert werden. Backups werden normalerweise für einen Zeitraum von mindestens 60 Tagen ab dem Datum der Erstellung des Backups online oder offline aufbewahrt. In der Regel aktualisiert Oracle Ihre Daten in Ihrem Auftrag nicht, fügt sie nicht ein, löscht sie nicht und stellt sie nicht wieder her. In Ausnahmefällen und unter der Voraussetzung einer schriftlichen Genehmigung kann Oracle Sie allerdings bei der Wiederherstellung von Daten, die Sie aufgrund eigenen Verschuldens verloren haben, unterstützen.

Bei Oracle Cloud Services, die es Ihnen ermöglichen, Backups in Übereinstimmung mit Ihren eigenen Richtlinien zu konfigurieren, sind Sie für die Durchführung von Backups und Wiederherstellungen Ihrer Inhalte verantwortlich. Darüber hinaus wird Ihnen empfohlen, einen Geschäftskontinuitätsplan zu entwickeln, um die Kontinuität Ihres eigenen Betriebs im Falle eines Notfalls sicherzustellen.

2.3 Oracle Cloud Services Continuity Policy

Oracle wird stets einen Plan für die internen Abläufe von Oracle aufrechterhalten, der darauf abzielt, Unterbrechungen der Services im Falle von Katastrophen, Störungen oder höherer Gewalt möglichst gering zu halten („BC-Plan“ (Business Continuity Plan, Geschäftskontinuitätsplan)).

Im BC-Plan sind Prozesse, Verfahren und Kontrollen festgelegt, dokumentiert und implementiert, um sicherzustellen, dass die Oracle Geschäftsprozesse, die Oracle Cloud Services unterstützen, im Falle der Anwendung des BC-Plans nicht eingeschränkt werden. Der Zweck des BC-Plans besteht darin, die Ausfallsicherheit der internen Abläufe von Oracle zugunsten der Kontinuität der Oracle Cloud Services unabhängig von der jeweiligen Ursache sicherzustellen.

3. ORACLE CLOUD SERVICELEVEL-VEREINBARUNG

3.1 Betriebszeiten

Die Oracle Cloud Services sind so konzipiert, dass sie rund um die Uhr an 7 Tagen die Woche und 365 Tagen im Jahr verfügbar sind, außer während Wartungsperioden, Technologieupgrades und wie anderweitig im Oracle Vertrag, Ihrem Auftrag und dieser *Oracle Cloud Servicelevel-Vereinbarung* festgelegt.

3.2 Serviceverfügbarkeit

Ab Aktivierung Ihres Oracle Cloud Service durch Oracle bemüht sich Oracle um die Erfüllung der Zielvorgabe für das Serviceverfügbarkeitsniveau oder für die Servicebetriebszeit von 99,9 %. Dies ist in Übereinstimmung mit der Oracle Cloud Service Pillar-Dokumentation für den entsprechenden Oracle Cloud Service (oder der Zielvorgabe für das Serviceverfügbarkeitsniveau oder für die Servicebetriebszeit, die von Oracle für den Cloud Service in einer solchen Dokumentation festgelegt wurde).

3.2.1 Bewertung der Verfügbarkeit

Nach jedem Ende eines Kalendermonats des relevanten Leistungszeitraums misst Oracle das Serviceverfügbarkeitsniveau oder die Servicebetriebszeit des jeweils unmittelbar vorhergehenden Monats; dazu wird die Differenz zwischen der Gesamtzahl der Minuten im monatlichen Messungszeitraum und den etwaigen ungeplanten Ausfallzeiten (wie unten definiert) durch die Gesamtzahl der Minuten des Messungszeitraums dividiert und das Ergebnis mit 100 multipliziert, um so einen Prozentsatz zu berechnen.

$$\left(\frac{Number\ of\ minutes\ in\ the\ month - Number\ of\ minutes\ of\ unplanned\ downtime}{Number\ of\ minutes\ in\ the\ month}\right) * 100$$

Anzahl der Minuten in einem 30-Tage-Monat = 30 Tage * 24 Stunden am Tag * 60 Minuten in der Stunde

Anzahl der ungeplanten Minuten im Monat = Minuten ungeplanter Ausfallzeiten, wie im Abschnitt „*Definition von „ungeplante Ausfallzeit““* unten definiert.

Beispiel: Der Juni hat 30 Tage = 30*24*60 = 43.200 Minuten im Monat

Treten im Monat Juni 90 Minuten ungeplanter Ausfallzeit auf, lautet die Gleichung:

$$((43{,}200 - 90)/43.200) * 100 = 99{,}8\ \%\ \text{Servicelevel-Verfügbarkeit}$$

3.2.2 Meldung der Verfügbarkeit

Oracle stellt Ihnen Metriken zum Serviceverfügbarkeitsniveau für die Oracle Cloud Services zur Verfügung, die Sie im Rahmen Ihres Auftrags erworben haben, und zwar entweder in Form eines Selbstbedienungsdienstes oder über einen Service Request, den Sie bei Oracle einreichen, um die Metriken anzufordern.

3.2.3 Servicegutschriften

Sie können Servicegutschriften erhalten, falls das Serviceverfügbarkeitsniveau oder die Servicebetriebszeit für Oracle Cloud Services, die Sie im Rahmen Ihres Auftrags erworben haben, unter der definierten Zielvorgabe für das Serviceverfügbarkeitsniveau oder für die Servicebetriebszeit liegt, die für solche Services gilt. Servicegutschriften sind in der Oracle Cloud Service Pillar-Dokumentation oder in den Service Descriptions definiert, die für Ihre erworbenen Oracle Cloud Services gelten. Ungeachtet der

Bestimmungen dieses Abschnitts können Sie, wenn Ihr Auftrag mit Oracle oder die Leistungsbeschreibungen, die für Ihren Auftrag für einen bestimmten Oracle Cloud Service gelten, das Recht auf einen höheren Betrag an Servicegutschriften vorsieht, die Servicegutschriften gemäß der Bestimmung erhalten, die den höchsten Betrag an Servicegutschriften für Sie vorsieht, aber Sie können die Servicegutschriften nicht gemäß mehrerer Bestimmungen für dasselbe Ereignis erhalten.

3.3 Definition von „ungeplante Ausfallzeit“ (Nichtverfügbarkeit)

Oracle Cloud Services werden in resilienten Rechenzentren mit einer resilienten Infrastruktur, redundanten Netzwerkverbindungen und Stromversorgungen in den einzelnen Hostingeinrichtungen bereitgestellt.

„Ungeplante Ausfallzeit“ bezeichnet jede Zeit, in der ein Problem mit den betreffenden Oracle Cloud Services Ihre Konnektivität mit Ihrer Produktionsinstanz dieser Cloud Services verhindert. Ungeplante Ausfallzeit beinhaltet keine Zeit, während der die Oracle Cloud Services oder Komponenten der Oracle Cloud Services nicht verfügbar sind aufgrund von: (i) planmäßigen Wartungszeiträumen, (ii) Umständen/Infrastruktur, die sich der Kontrolle durch Oracle entziehen, sowie Ereignissen höherer Gewalt, (iii) Handlungen oder Unterlassungen von Ihnen, Ihren Benutzern oder einem Dritten (außer Vertretern und Auftragnehmern, die Oracle mit der Unterstützung der Services beauftragt hat) oder (iv) einer zulässigen Aussetzung durch Oracle.

In Bezug auf Oracle Cloud at Customer Services gehören zu den ungeplanten Ausfallzeiten auch keine Ausfallzeiten oder andere Nichtverfügbarkeiten (i) Ihres Rechenzentrums (z. B. aufgrund von Wartungsarbeiten) oder (ii) außerhalb der in Ihrem Auftrag festgelegten Vor-Ort-Zeiten für Oracle Cloud Operations-Mitarbeiter in Ihrem Rechenzentrum.

3.4 Überwachung

Oracle nutzt eine Reihe verschiedener Softwaretools zur Überwachung der Verfügbarkeit und Leistung der Cloud Services und des Betriebs der Infrastruktur- und Netzwerkkomponenten (wie CPU, Arbeitsspeicher, Speicher, Datenbank und sonstige Komponenten). Oracle generiert Warnmeldungen im Zusammenhang mit Abweichungen von festgelegten Schwellenwerten, und Oracle Mitarbeiter untersuchen und beheben alle identifizierten zugrunde liegenden Probleme. Oracle überwacht oder meldet keine nicht von Oracle verwalteten Komponenten, die von Ihnen in den Oracle Cloud Services verwendet werden, wie nicht von Oracle stammende Anwendungen.

3.4.1 Überwachungs- und Testtools des Kunden

Oracle gestattet Ihnen die Durchführung begrenzter Funktionstests für Oracle Cloud Services in Ihrer Testinstanz. Spezifische Regeln für das Testen finden Sie in den Oracle Corporate Security Practices (Oracle Unternehmenssicherheitsverfahren), die unter https://www.oracle.com/corporate/security-practices/ abrufbar sind.

Oracle führt regelmäßig Penetrations- und Schwachstellentests sowie Sicherheitsbewertungen für die Oracle Cloud Infrastruktur, Plattformen und Anwendungen durch, um die Sicherheit der Oracle Cloud Services insgesamt zu überprüfen und zu verbessern. Die Oracle Cloud Services-Programmdokumentation beschreibt, wann und wie Sie Komponenten, die Sie in Oracle Cloud Services verwalten oder erstellen, bewerten oder testen dürfen, einschließlich nicht von Oracle stammenden Anwendungen, nicht von Oracle stammenden Datenbanken, andere anwendbare nicht von Oracle stammende Software, Code oder die Verwendung von Data-Scraping-Tools.

Oracle behält sich das Recht vor, den Zugriff auf Tools oder Technologien zurückzuziehen oder zu deaktivieren, die gegen die Richtlinien in diesem Abschnitt oder die entsprechende Oracle Cloud Services-Programmdokumentation verstoßen, ohne jegliche Haftung Ihnen gegenüber.

4. ORACLE RICHTLINIE FÜR CLOUD-CHANGE-MANAGEMENT

4.1 Oracle Cloud Change Management und Wartung

Oracle nimmt Änderungen an der Cloud-Hardwareinfrastruktur, der Betriebssoftware, der Produktsoftware und unterstützender Anwendungssoftware, die von Oracle als Bestandteil der Oracle Cloud Services zur Verfügung gestellt werden, vor, um so für die operative Stabilität, Verfügbarkeit, Sicherheit, Leistung und Aktualität der Oracle Cloud Services zu sorgen. Oracle hält sich dabei an formale Change-Management-Verfahren, in deren Rahmen die Änderungen vor ihrer Anwendung im Service geprüft, getestet und genehmigt werden.

Zu Änderungen im Rahmen von Change-Management-Verfahren gehören beispielsweise System- und Servicewartungsaktivitäten, Upgrades und Updates und kundenspezifische Änderungen. Oracle Cloud Services Change-Management-Verfahren dienen der Minimierung von Serviceunterbrechungen während der Implementierung von Änderungen.

Oracle plant bestimmte Wartungszeiträume für Änderungen ein, bei denen der Oracle Cloud Service während des Wartungszeitraums möglicherweise nicht verfügbar ist. Oracle bemüht sich darum, dass Change-Management-Verfahren während der geplanten Wartungszeiträume (die Oracle im Voraus ankündigt) durchgeführt werden und berücksichtigt gleichzeitig Zeiträume mit geringem Datenverkehr sowie geografische Anforderungen.

Oracle informiert Sie im Voraus über Änderungen am Zeitplan für Wartungszeiträume. Bei kundenspezifischen Änderungen und Upgrades stimmt Oracle die Wartungszeiträume, soweit möglich, mit Ihnen ab.

Bei Änderungen, die voraussichtlich zu einer Serviceunterbrechung führen, zählt die Dauer der geplanten Wartungszeiträume nicht zur Berechnung der Minuten ungeplanter Ausfallzeiten im monatlichen Messzeitraum für das Serviceverfügbarkeitsniveau (siehe *Oracle Cloud Servicelevel-Vereinbarung* oben). Oracle bemüht sich auf wirtschaftlich zumutbare Weise, die Nutzung der geplanten Wartung sowie die Dauer von zu Serviceunterbrechungen führenden Wartungszeiträumen zu minimieren.

Bei Oracle Cloud Services, die es Ihnen ermöglichen, Wartungsaktivitäten durchzuführen, sind Sie für die Konfiguration und Wartung der Betriebssysteme und anderer zugehöriger Software verantwortlich.

4.1.1 Sicherheitswartung

Gegebenenfalls muss Oracle außerhalb der planmäßigen Wartungszeiträume zusätzliche Sicherheitswartungen durchführen, um eine dringliche Situation (z. B. eine Sicherheitsschwachstelle) der Oracle Cloud Services oder Oracle Infrastruktur zu beheben, die nur in Form eines Notfalleinsatzes behoben werden kann. Oracle bemüht sich, zusätzliche Sicherheitswartungen, die eine Unterbrechung der Services außerhalb der geplanten Wartungszeiträume erfordern, auf ein Mindestmaß zu beschränken und wird diese Wartungen, soweit dies zumutbar ist, 24 Stunden im Voraus ankündigen.

4.1.2 Migration von Rechenzentren

Oracle ist berechtigt, Ihre Oracle Cloud Services, die in von Oracle beauftragten Rechenzentren bereitgestellt werden, zwischen Rechenzentren in derselben Rechenzentrumsregion zu migrieren, wie von Oracle als notwendig erachtet. Oracle informiert Sie mindestens 30 Tage im Voraus über Rechenzentrumsmigrationen; sofern eine solche Verpflichtung zur Vorankündigung nicht für Disaster-Recovery-Szenarien oder die Sicherstellung der Servicekontinuität gilt, wie, sofern zutreffend, in der einschlägigen Oracle Cloud Services Pillar-Dokumentation näher beschrieben.

4.1.3 Softwareupdates

Oracle stellt Oracle Cloud Services auf Basis eines Modells mit kontinuierlichen Updates bereit und unterstützt nur die Softwareversionen, die Oracle als unterstützte Releases für solche Oracle Cloud Services bezeichnet. Sie müssen stets dafür sorgen, dass Ihre Cloud Services unterstützte Releases verwenden, und alle erforderlichen Maßnahmen ergreifen, um die Aktualität der Version zu gewährleisten. Sie bestätigen, dass das Versäumnis, das Update vor dem Ende des Supports für das anwendbare Release abzuschließen, dazu führen kann, dass Oracle das Update automatisch durchführt oder den Zugriff auf die betroffenen Oracle Cloud Services aussetzt. Die Verpflichtungen von Oracle im Rahmen dieser Delivery Policies (einschließlich der *Oracle Cloud Service Continuity Policy (Oracle Richtlinie für Cloud Service-Kontinuität),* der *Oracle Cloud Servicelevel-Vereinbarung* und der *Oracle Cloud Support Policy (Oracle Richtlinie für Cloud-Support)*) gelten nur, wenn Sie unterstützte Releases verwenden. Oracle trägt keine Verantwortung für Probleme der Oracle Cloud Services bezüglich Leistung, Funktionalität, Verfügbarkeit oder Sicherheit, die sich aus der Ausführung früherer Versionen ergeben.

4.1.4 End of Life

Soweit dies vernünftigerweise praktikabel ist, kündigt Oracle mindestens 12 Monate im Voraus an, wenn das End of Life (EOL) für einen Oracle Cloud Service geplant ist und er eingestellt wird. Oracle Cloud Services mit geplantem EOL sind nicht mehr allgemein verfügbar, werden nicht unterstützt und erhalten keine technische Unterstützung oder Updates, wie z. B. Sicherheitspatches, Programmfehlerkorrekturen oder Complianceaktualisierungen, und fallen nicht unter die SLA-Abdeckung. Wenn ein Oracle Cloud Service das EOL erreicht, kann Oracle einen Nachfolgerservice für den Oracle Cloud Service benennen und von Ihnen eine Umstellung auf einen solchen Service verlangen.

5. ORACLE RICHTLINIE FÜR CLOUD-SUPPORT

Der in dieser *Oracle Cloud Support Policy* (Oracle Richtlinie für Cloud-Support) beschriebene Support gilt nur für Oracle Cloud Services und wird von Oracle im Rahmen der Oracle Cloud Services bereitgestellt, die unter Ihrem Auftrag bestellt wurden. Oracle kann zusätzliche Vergütungen anbieten, und Sie können gegen Zahlung zusätzlicher Vergütungen zusätzliche Unterstützungsserviceangebote von Oracle für die Oracle Cloud Services bestellen.

5.1 Bedingungen für Oracle Cloud Support

5.1.1 Supportvergütungen

Die von Ihnen gemäß Ihrem Auftrag gezahlte Vergütung für Oracle Cloud Services beinhaltet den in dieser *Oracle Cloud Support Policy* (Oracle Richtlinie für Cloud-Support) beschriebenen Support. Zusätzliche Vergütungen gelten für zusätzliche von Ihnen erworbene Oracle Support Services-Angebote.

5.1.2 Supportzeitraum

Oracle Cloud Support ist ab dem Startdatum der Oracle Cloud Services verfügbar und endet nach Ablauf oder Kündigung der Services (der „Supportzeitraum“). Oracle ist nicht verpflichtet, den in dieser Oracle

Cloud Support Policy (Oracle Richtlinie für Cloud-Support) beschriebenen Support über das Ende des Supportzeitraums hinaus bereitzustellen.

5.1.3 Technische Ansprechpartner

Ihre technischen Ansprechpartner sind die einzige Verbindung zwischen Ihnen und Oracle in Bezug auf Oracle Support für Oracle Cloud Services. Diese technischen Ansprechpartner müssen mindestens eine Grundlagenschulung für den Service und bei Bedarf eine ergänzende Schulung erhalten haben, die für die jeweilige Rolle oder Implementierungsphase, die spezielle Service-/Produktnutzung und die Migration geeignet ist. Ihre technischen Ansprechpartner müssen sich mit den Oracle Cloud Services auskennen, um Oracle bei der Lösung von Systemproblemen und der Analyse und Bearbeitung von Service Requests zu unterstützen. Bei Einreichung eines Service Requests muss Ihr technischer Ansprechpartner über Grundkenntnisse über das vorliegende Problem verfügen und in der Lage sein, das Problem zu reproduzieren, um Oracle bei der Diagnose und Kategorisierung des Problems zu unterstützen. Um Unterbrechungen bei den Oracle Support für Oracle Cloud Services zu vermeiden, müssen Sie Oracle benachrichtigen, sobald die Verantwortlichkeiten eines technischen Ansprechpartners auf eine andere Person übertragen werden.

5.1.4 Oracle Cloud Support

Oracle Support für Oracle Cloud Services umfasst Folgendes:

- Diagnose von Problemen oder Vorfällen mit Oracle Cloud Services
- Wirtschaftlich zumutbare Anstrengungen, gemeldete und nachprüfbare Fehler in den Oracle Cloud Services zu beheben, so dass diese Oracle Cloud Services in allen wesentlichen Aspekten wie in den zugehörigen Leistungsbeschreibungen beschrieben funktionieren
- Support im Rahmen von in der *Oracle Cloud Change Management Policy (Oracle Richtlinie für Cloud-Change-Management)* definierten Change-Management-Aktivitäten.
- Unterstützung bei technischen Service Requests rund um die Uhr
- Rund um die Uhr und 365 Tage im Jahr Zugang zum Oracle Cloud-Kundensupportportal und telefonische Liveunterstützung zur Erfassung von Service Requests
- Zugang zu Community-Foren
- Nicht-technischer Kundenservice während der normalen Geschäftszeiten von Oracle (von 08:00 Uhr bis 17:00 Uhr Ortszeit).

5.2 Oracle Cloud-Kundensupportsysteme

5.2.1 Oracle Cloud-Kundensupportportal

Oracle bietet Support für den Oracle Cloud Service, den Sie gemäß einem Auftrag über das für diesen Oracle Cloud Service angegebene Cloud-Kundensupportportal (Supportportal) erworben haben. Obwohl der Oracle Cloud Support und die Portale (einschließlich eines beliebigen Teils der Services, die sie bereitstellen) einen Teil Ihres Auftrags umfassen, handelt es sich hierbei nicht um ein Oracle Cloud Service-Angebot, und sie können global bereitgestellt werden, wobei der Zugriff darauf den Nutzungsbedingungen unterliegt, die auf den jeweiligen Websites der Portale veröffentlicht werden und Änderungen unterliegen können. Insoweit solche Portale Ihnen das Hochladen von Informationen gestatten, sind Sie verantwortlich sicherzustellen, dass Sie und Ihre Benutzer keine amtlichen Identifikationsnummern und keine Gesundheits-, Finanz-, Zahlungskartendaten, kontrollierte nicht als geheim eingestufte Informationen oder

andere sensible personenbezogene Daten in solchen Portalen veröffentlichen, sofern dies nicht ausdrücklich gemäß den Bestimmungen des Supportportals oder Ihres anwendbaren Cloud Services-Auftrags gestattet ist. Der Zugang zum Supportportal ist Ihren ausgewiesenen technischen Ansprechpartnern und anderen autorisierten Benutzern der Oracle Cloud Services vorbehalten. Sofern zutreffend, bietet das Supportportal Ihren technischen Ansprechpartnern Support-Details, damit diese auf den Oracle Support für Oracle Cloud Services zurückgreifen können. Benachrichtigungen und Hinweise des Supports in Bezug auf Ihre Service Requests werden im Supportportal veröffentlicht.

5.2.2 Telefonische Liveunterstützung

Ihre technischen Ansprechpartner können die telefonische Liveunterstützung mithilfe der Telefonnummern und Kontaktinformationen nutzen, die auf der Supportwebsite von Oracle unter https://www.oracle.com/support/contact.html zu finden sind.

5.3 Severity-Definitionen

Service Requests für Oracle Cloud Services können von Ihrem technischen Ansprechpartner über das Supportportal eingereicht werden. Der Severity-Level eines Service Requests wird auf der Grundlage der von Ihnen gemachten Angaben zugewiesen und basiert auf den folgenden Severity-Definitionen:

5.3.1 Severity 1 (Kritischer Ausfall)

Ihre produktionsbezogene Nutzung der Oracle Cloud Services wird ausgesetzt oder so stark beeinträchtigt, dass Sie die Arbeit nicht auf zumutbare Weise fortsetzen können. Ihnen entsteht ein vollständiger Serviceverlust. Der beeinträchtigte Betrieb ist geschäftsgefährdend und die Situation als Notfall einzustufen. Ein Service Request mit Severity 1 weist eines oder mehrere der folgenden Merkmale auf:

- Beschädigte Daten
- Eine kritische dokumentierte Funktion ist nicht verfügbar
- Der Service hängt auf unbestimmte Zeit, was zu inakzeptablen oder zeitlich unbegrenzten Verzögerungen bei Ressourcen oder Reaktionen führt
- Der Service stürzt ab und stürzt nach Neustartversuchen wiederholt ab
- Sicherheitsvorfall mit dem Potenzial, die Vertraulichkeit, Integrität oder Verfügbarkeit des Service zu beeinträchtigen

Oracle wird zumutbare Anstrengungen unternehmen, auf Service Requests mit Severity 1 innerhalb von fünfzehn (15) Minuten zu reagieren. Während des Zeitraums, in dem Oracle an der Bearbeitung eines Service Requests mit Severity 1 arbeitet, erklären Sie sich bereit, Ihren technischen Ansprechpartner rund um die Uhr zur Verfügung zu stellen. Oracle wird rund um die Uhr an 7 Tagen die Woche arbeiten, bis ein Service Request mit Severity 1 behoben ist, eine angemessene Abhilfe geschaffen wurde, ein genehmigter Maßnahmenplan vorliegt oder der Ansprechpartner des Kunden nicht mehr rund um die Uhr erreichbar ist. Sie müssen Oracle während dieses 24x7-Zeitraums einen technischen Ansprechpartner nennen, der bei der Datenerfassung, bei Tests und der Anwendung von Fehlerkorrekturen unterstützt. Sie sind gehalten, diese Severity-Einstufung nach reiflicher Prüfung vorzuschlagen, damit Situationen mit echter Severity 1 die erforderlichen Ressourcen von Oracle zugewiesen werden können.

5.3.2 Severity 2 (Erhebliche Beeinträchtigung)

Ihnen entsteht ein schwerwiegender Serviceverlust. Wichtige Funktionen der Oracle Cloud Services stehen nicht zur Verfügung, und es gibt keinen annehmbaren Workaround; der Betrieb kann jedoch eingeschränkt fortgesetzt werden.

5.3.3 Severity 3 (Technisches Problem)

Ihnen entsteht ein geringer Serviceverlust. Die Beeinträchtigung stellt eine Unannehmlichkeit dar, die möglicherweise einen Workaround erfordert, um die Funktionalität wiederherzustellen.

5.3.4 Severity 4 (Allgemeiner Hinweis)

Sie fordern Informationen, eine Verbesserung oder Dokumentation zur Klärung bezüglich der Oracle Cloud Services an, doch die Ausführung des Service ist nicht beeinträchtigt. Ihnen entsteht kein Serviceverlust.

5.4 Änderung der Service-Request-Severity

5.4.1 Anfänglicher Severity-Level

Zum Zeitpunkt der Erstellung des Service Requests wird Oracle einen anfänglichen Severity-Level des Service Requests auf der Grundlage der obigen Severity-Definitionen und/oder Ihrer Eingaben aufzeichnen. Oracle konzentriert sich nach Erstellung eines Service Requests zunächst auf die Lösung des dem Service Request zugrundeliegenden Problems. Der Severity-Level eines Service Requests kann wie nachstehend beschrieben angepasst werden.

5.4.2 Herabstufung eines Service-Request-Levels

Wenn der anfänglich zugewiesene Severity-Level des Problems aufgrund der aktuellen Beeinträchtigung der Abläufe der jeweiligen Oracle Cloud Services nicht länger gerechtfertigt ist, wird der anfängliche Severity-Level auf den Severity-Level herabgestuft, der der aktuellen Beeinträchtigung am ehesten gerecht wird.

5.4.3 Hochstufung eines Service-Request-Levels

Wenn im Laufe der Service Request-Bearbeitung eine Hochstufung des anfänglich zugewiesenen Severity-Levels des Problems aufgrund der aktuellen Beeinträchtigung der Produktionsabläufe der jeweiligen Oracle Cloud Services gerechtfertigt ist, wird der anfängliche Severity-Level auf den Severity-Level hochgestuft, der der aktuellen Beeinträchtigung am ehesten gerecht wird.

5.4.4 Einhaltung der Severity-Level-Definitionen

Sie stellen sicher, dass Zuweisung und Anpassung von Severity-Levels je nach aktueller Beeinträchtigung der Produktionsabläufe der jeweiligen Oracle Cloud Services auf korrekten Angaben basieren.

5.5 Service-Request-Eskalation

Bezüglich von Ihnen eskalierter Service Requests wird der Oracle Support-Analytiker den Oracle Service-Request-Eskalationsmanager einsetzen, der für das Eskalationsmanagement verantwortlich ist. Der Oracle Eskalationsmanager für Service Requests wird mit Ihnen zusammen an der Erstellung eines Maßnahmenplans arbeiten und angemessene Oracle Ressourcen zuweisen. Wenn das dem Service Request zugrundeliegende Problem nicht gelöst werden kann, können Sie sich an den Oracle Service Request-Eskalationsmanager wenden, damit dieser den Service Request prüft und bei Bedarf eine Eskalation auf

den nächsten Level innerhalb von Oracle anfordert. Um die erfolgreiche Bearbeitung eines eskalierten Service Requests zu unterstützen, müssen Sie Ansprechpartner aus Ihrem Unternehmen nennen, die auf einer Ebene tätig sind, die der Ebene entspricht, auf die der Service Request innerhalb von Oracle eskaliert wurde.

6. ORACLE RICHTLINIE FÜR AUSSETZUNG UND BEENDIGUNG VON CLOUD SERVICES

6.1 Kündigung von Oracle Cloud Services

Für einen Zeitraum von 60 Tagen nach dem Ende des Servicezeitraums für die Oracle Cloud Services oder, soweit zutreffend, für einen Zeitraum von 60 Tagen nach Ihrer Kündigung von Cloud Services, die Sie im Rahmen eines Pay-as-you-go-Modells in Anspruch nehmen, wird Oracle Ihre Inhalte, die sich in den Oracle Cloud Services befinden, über sichere Protokolle und in einem strukturierten, maschinenlesbaren Format zur Verfügung stellen oder das Servicesystem zum Zweck der Datenabfrage durch Sie zugänglich halten. Am Ende des Leistungszeitraums läuft Ihr Recht zur Nutzung dieser Services ab, außer insoweit diese anderweitig gemäß den Bestimmungen des Oracle Vertrags, Ihres Auftrags und den auf Ihre Oracle Cloud Services anwendbare Leistungsbeschreibung zulässig ist.

Für kostenlose Test- und Pilotservices von Oracle Cloud Services stellt Oracle Ihre Inhalte für einen Zeitraum von 30 Tagen nach Ende des Test- oder Pilotservice zur Verfügung. Während dieses Abrufzeitraums gilt die
Oracle Cloud Servicelevel-Vereinbarung nicht und das Servicesystem darf nicht für Produktionsaktivitäten verwendet werden. Nach diesem Abrufzeitraum ist Oracle nicht verpflichtet, Ihre Inhalte weiter aufzubewahren.

Falls Sie Unterstützung von Oracle benötigen, um Zugriff auf Ihre Inhalte oder Kopien Ihrer Inhalte zu erhalten, müssen Sie einen Service Request im entsprechenden Supportportal erstellen.

Der Abruf von Daten und die damit verbundene Unterstützung durch Oracle gelten nicht für Oracle Cloud Services, auf denen Ihre Inhalte nicht gespeichert sind. Sie sind dafür verantwortlich sicherzustellen, dass, falls diese separaten Oracle Cloud Services für die Speicherung der Daten von separaten Oracle Cloud Services (z. B. Storage Cloud Service oder Database Cloud Services) abhängig sind, diese separaten Oracle Cloud Services eine gültige Laufzeit bis zum Ende des beendeten Oracle Cloud Service aufweisen, um das Abrufen von Daten zu ermöglichen oder um anderweitige geeignete Maßnahmen zum Sichern oder anderweitigen separaten Speichern Ihrer Inhalte zu ergreifen, während die Oracle Cloud Services-Produktionsumgebung vor dem Ende des Leistungszeitraums noch aktiv ist.

Nach Ablauf des Abrufzeitraums löscht Oracle Ihre Inhalte aus den Oracle Cloud Services (sofern nicht anderweitig durch anwendbares Recht vorgeschrieben).

Für Oracle Cloud at Customer Services müssen Sie Oracle unter Berücksichtigung der bei angemessener Nutzung gewöhnlichen Abnutzung alle Hardwarekomponenten mit Bezug zu Oracle Cloud at Customer Services (einschließlich der Gateway-Ausrüstung) im gleichen einwandfreien Zustand zur Verfügung stellen, in dem sie sich zu Beginn der Oracle Cloud at Customer Services befanden.

7. KI-BESTIMMUNGEN

Die Bestimmungen für künstliche Intelligenz von Oracle, die online unter https://oracle.com/contracts abrufbar sind, gelten für die KI-Funktionalität (wie in diesen Bestimmungen definiert) in Ihren bestellten Cloud Services.

8. NUTZUNG DER SERVICES

Sie sind verantwortlich dafür sicherzustellen, dass der Zugang zu den erworbenen Oracle Cloud Services und deren Nutzung sowie der Nutzen aus diesen Cloud Services nur für und durch die Benutzer in den Ländern gemäß der Oracle Global Trade Compliance-Richtlinie möglich ist, wie unter https://www.oracle.com/corporate/security-practices/corporate/governance/global-trade-compliance.html beschrieben.