



# Norddeutscher Rundfunk Cloud-Dienstleistungen – Los 1 LEISTUNGSBESCHREIBUNG

Status: Version 02  
Stand: 16. Juni 2026

## Inhaltsverzeichnis

	Kapitel	Seite
<b>1</b>	<b>Einleitung</b> .....	<b>3</b>
1.1	Auftraggeber .....	3
1.2	Ausschreibungsgegenstand .....	3
<b>2</b>	<b>Leistungsanforderungen</b> .....	<b>4</b>
2.1	Allgemein .....	4
2.2	Anforderungen für alle Rollen .....	4
2.3	Einarbeitung .....	5
2.4	Konkrete Rollen und Anforderungen .....	6
2.4.1	Senior Cloud Consultant .....	6
2.4.2	Senior Cloud Architect.....	6
2.4.3	Cloud Engineer .....	8
2.4.4	Senior Cloud Engineer .....	9
2.4.5	Cloud Security Architect .....	10
2.4.6	Cloud FinOps Expert.....	12
2.4.7	Cloud GreenOps Expert.....	13
<b>3</b>	<b>Serviceanforderungen im Rahmen der Projekte</b> .....	<b>15</b>
3.1	Servicelevel/Servicezeiten .....	15
<b>4</b>	<b>Organisatorische Regeln</b> .....	<b>16</b>
4.1	Allgemein .....	16
4.2	Preisblatt.....	16

## 1 Einleitung

Auftraggeber ist der Norddeutsche Rundfunk (NDR). In diesem Dokument und im Kriterienkatalog wird dieser als AG und der Bieter als AN bezeichnet.

Die Vergabe der Leistungen erfolgt in einem europaweiten offenen Verfahren. Es findet eine Aufteilung der Ausschreibung in drei Losen statt.

Die Leistungsbeschreibung beschreibt die Anforderungen an Fachrollen, die für die Erbringung von Dienstleistungen in Projekten verantwortlich sind, die im Rahmen von Miniwettbewerben ausgeschrieben werden.

Dabei unterteilen sich die Lose in die folgenden Bereiche:

- ⇒ Los 1: Rollen für die Planung, Implementierung und den Service von Cloud-Infrastrukturen und Standardapplikationen
- ⇒ Los 2: Rollen für die Planung, Erstellung, Wartung, Implementierung und den Service von eigenen Cloud-Applikationen
- ⇒ Los 3: Rollen für die Planung, Erstellung, Wartung, Implementierung und den Service von eigenen AI-Applikationen und AI-Lösungen in der Cloud

Der AG beabsichtigt, je Los eine Rahmenvereinbarung mit maximal fünf AN und einer Laufzeit von 24 Monaten sowie einer Verlängerungsoption von zwei Mal 12 Monaten zu schließen. Der Abruf von Leistungen erfolgt während der Laufzeit in Miniwettbewerben.

Diese Leistungsbeschreibung beschreibt die Anforderungen an die Bieter im Los 1.

### 1.1 Auftraggeber

Auftraggeber (AG) ist die im Folgenden benannte Rundfunkanstalt:

Norddeutscher Rundfunk  
Rothenbaumchaussee 132  
20149 Hamburg

### 1.2 Ausschreibungsgegenstand

Der AG beabsichtigt, Services in eine Cloud zu verschieben bzw. neue Services direkt für die Cloud zu entwickeln. Dafür beabsichtigt der AG, bedarfsorientiert externe Unterstützungsleistungen in Anspruch zu nehmen. Es handelt sich hauptsächlich um beratende, designtechnische und konzeptionelle Leistungen für das Design und den Aufbau einer Cloud-Plattform und Cloud-Anwendungen basierend auf einem Multicloud-Ansatz, und weitere Leistungen, d. h. um Dienstleistungen, die nicht weisungsgebunden zu erbringen sind. Dies beinhaltet auch Programmierleistungen.

Dabei plant der AG, die Clouds der folgenden Anbieter zu verwenden:

- ⇒ AWS
- ⇒ Azure
- ⇒ Google Cloud (GCP)
- ⇒ StackIT
- ⇒ ARD-Private-Cloud (basierend auf VMware-Tanzu)

## 2 Leistungsanforderungen

### 2.1 Allgemein

Die AN dieser Rahmenvereinbarung sind verpflichtet, dem AG auf dessen Anforderung mittels Durchführung von Miniwettbewerben auf hohem qualitativem Niveau geeignete, qualifizierte Personen oder Gewerke anzubieten. Da die im Einzelnen anfallenden konkreten Aufgaben bzw. Projekte noch nicht absehbar sind, wird das erwartete Qualitätsniveau im Folgenden für die benötigten Rollen beschrieben.

Die für die Leistungserbringung erforderlichen Mindestanforderungen, hinsichtlich Berufsausbildung und beruflicher Qualifikation der Ausübenden, sind in Kapitel 2 detailliert beschrieben. Die für die einzelnen Rollen ggf. geforderten persönlichen Zertifizierungen sollen sicherstellen, dass ausschließlich speziell geschultes und qualifiziertes Personal eingesetzt wird. Die Anforderungen können in den durchzuführenden Miniwettbewerben vom Auftraggeber nochmals konkretisiert werden.

Des Weiteren erwartet der AG, soweit ein regelmäßiger Austausch zwischen den eingesetzten Personen und dem AG zur Erbringung der jeweiligen Leistung erforderlich ist, den Einsatz kommunikationsfähiger Personen, welche über eine ausgeprägte Sozialkompetenz verfügen und sich über eine bestimmte Zeit und zu einem bestimmten Zweck in möglicherweise bereits laufende Projekte zügig einarbeiten können.

⇒ *Anforderungen:*

- 2.1-(1) [A] Der AN benennt für die Vertragslaufzeit des Rahmenvertrages einen verantwortlichen Ansprechpartner als Single Point of Contact (SPOC).
- 2.1-(2) [A] Die benötigte persönliche Hardware für die Leistungserbringung wird vom AN für seine Mitarbeiter gestellt. Der AG stellt Zugänge für den Remote-Zugriff bereit.
- 2.1-(3) [A] Die Projektsprache ist generell deutsch. Alle eingesetzten Mitarbeiter des AN verfügen über deutsche Sprachkenntnisse in Wort und Schrift auf dem Niveau C1. Einzelne Fachgespräche können auch in Englisch erfolgen.
- 2.1-(4) [A] Der AN ist verpflichtet, den AG regelmäßig über den Projektfortschritt zu informieren. Die genauen Informationszyklen werden im jeweiligen Miniwettbewerb festgelegt.
- 2.1-(5) [A] Nach Beendigung des jeweiligen Einsatzes übergibt der AN die Arbeitsergebnisse an den AG. Die genaue Ausgestaltung/Präzisierung der zu übergebenden Artefakte erfolgt im jeweiligen Miniwettbewerb.
- 2.1-(6) [A] Eigentum an allen Arbeitsergebnissen der im Rahmen der Projekte erstellten Quellcodes und Skripte erhält der AG.
- 2.1-(7) [A] Der AN erklärt sich generell bereit, im Rahmen von Projekten bei durch den AN entwickelten Produkten, die Produktverantwortung zu übernehmen. Die Ausgestaltung der genauen Anforderungen wird im Miniwettbewerb bekanntgegeben.
- 2.1-(8) [A] Der AN erklärt sich generell bereit, im Rahmen von Projekten die Verantwortung für Projektziele zu übernehmen. Die Ausgestaltung der genauen Anforderungen wird im Miniwettbewerb bekanntgegeben.

### 2.2 Anforderungen für alle Rollen

Von den Mitarbeitern des Auftragnehmers erwartet der Auftraggeber eine positive, wertschätzende und authentische Grundhaltung, die sich mit dem Werterahmen des Auftraggebers deckt. Darüber hinaus müssen die bereitgestellten Mitarbeiter über die Fähigkeit zur Selbstreflexion und Selbstwahrnehmung (z. B. Kritikfähigkeit, Ehrlichkeit, Resilienz

usw.) verfügen. Weiterhin haben die Mitarbeiter eine positive berufliche Einstellung bzw. Haltung, was sich beispielsweise in Motivation, Interesse, Engagement, Flexibilität, Belastbarkeit, Verantwortungsbereitschaft, Durchhaltevermögen und Zuverlässigkeit ausdrückt.

Der AG erwartet von den eingesetzten Mitarbeitern die folgenden Sozialkompetenzen:

- ⇒ Teamfähigkeit
- ⇒ Ein hohes Maß an Kommunikationsfähigkeit
- ⇒ Ein hohes Maß an Konfliktlösungskompetenz
- ⇒ Kundenorientierung
- ⇒ Sicheres Auftreten

Die folgenden Methodenkompetenzen werden von den eingesetzten Mitarbeitern erwartet:

- ⇒ Fähigkeit, Informationen zu beschaffen, zu strukturieren, zu bearbeiten, aufzubewahren und wieder zu verwenden, darzustellen, Ergebnisse von Verarbeitungsprozessen richtig zu interpretieren und in geeigneter Form zu präsentieren
- ⇒ Fähigkeit zur Anwendung von Problemlösungstechniken
- ⇒ Fähigkeit zur Gestaltung von Problemlösungsprozessen
- ⇒ Fähigkeit zur Selbstorganisation

Die eingesetzten Personen des AN müssen über die fachliche Fähigkeit verfügen, die beauftragte Leistung in hoher Qualität und in gegebener Zeit zu erbringen. Dafür werden unter anderem die folgenden allgemeinen fachlichen Fähigkeiten gefordert:

- ⇒ Gewährleistung von Prozessen zur Qualitätssicherung
- ⇒ Identifizierung und Bewertung von Risikoindikatoren
- ⇒ Lösung von akuten Problemen und Beseitigung von Hindernissen
- ⇒ Reporting und Dokumentation von Arbeitsergebnissen der Teams (Informationsfluss in/von anderen Teams)
- ⇒ Nutzung der vom Auftraggeber vorgegebenen Plattform für kollaboratives Arbeiten (überwiegend MS Teams, Jira, Confluence) zum Austausch von gemeinsamen Arbeitsdokumenten
- ⇒ Nutzung der vom AG vorgegebenen Tools für CI/CD-Pipelines (GitLab, OpenTofu, TerraForm etc.)
- ⇒ Verwendung aktueller Technologien
- ⇒ Erarbeiten von qualitativ hochwertigen Lösungen im Hinblick auf Wiederverwendbarkeit und Weiterentwicklungsmöglichkeit

### **2.3 Einarbeitung**

Die Anforderungen und Bedingungen für die Einarbeitung werden in den Miniwettbewerben festgelegt. Generell wird davon ausgegangen, dass eine Konstanz bei den eingesetzten Mitarbeitern gegeben ist.

Grundsätzlich wird der AG eine Einweisung in die aktuellen Konfigurationen und verwendeten Methoden vornehmen. Eine Einarbeitung in die o. g. verwendeten kollaborativen Plattformen und Tools obliegt dem AN. Bei Personalwechseln seitens des AN obliegt es dem AN, diese Informationen weiterzugeben. Personalwechsel sind vom AN gegenüber dem AG mit angemessener Frist anzukündigen und abzustimmen.

## 2.4 Konkrete Rollen und Anforderungen

### 2.4.1 Senior Cloud Consultant

Ein Senior Cloud Consultant ist ein Spezialist, der Unternehmen und Stakeholder dabei berät, Cloud-Technologien strategisch und effizient einzusetzen.

Der Senior Cloud Consultant muss den Auftraggeber strategisch und konzeptionell beim Aufbau von NDR-Cloud-Diensten beraten und insbesondere bei der Bewertung der Implementierung von Sicherheits- und Datenschutzmaßnahmen in den jeweiligen Public-Cloud-Umgebungen unterstützen. Dabei muss er das Spezialwissen des „Cloud Architect“, des „Cloud Engineer“ und des „Cloud Security“ nutzen und in die Beratungsinformation einfließen lassen. Zu seinen Aufgaben zählen insbesondere auch die Beratung und Unterstützung der Product Owner des Auftragsgebers bei der Erstellung von User Stories. Beratung und Unterstützung bei Konzeption und Aufbau eines Kostenmanagementsystems zur Überwachung und Optimierung der Ausgaben für Cloud-Ressourcen ist eine weitere wesentliche Aufgabe des Senior Cloud Consultants.

⇒ *Anforderungen an den Senior Cloud Consultant:*

- ⇒ Vertiefte Kenntnisse im Bereich „Multicloud-Strategien und -Architekturen“: Breites Überblickswissen über mindestens die Public-Cloud-Plattformen (AWS, Azure, GCP), idealerweise auch STACKIT, vertieftes Wissen in mindestens einer Public-Cloud-Plattform (AWS, Azure, GCP).
- ⇒ Vertiefte Kenntnisse in technischem Cloud-Überblickswissen (Terraform/OpenTofu, Landingzones, Container, Netzwerk, CI/CD, 6Rs, Migration)
- ⇒ Vertiefte Kenntnisse mit cloud-bezogenen Projektaktivitäten
- ⇒ Vertiefte Kenntnisse in Cloud-Plattformen (Architektur, Betrieb, Monitoring, Plattform Engineering)
- ⇒ Vertiefte Kenntnisse in Praktiken wie DevOps, DevSecOps, SRE
- ⇒ Vertiefte Kenntnisse in Beratungskompetenz und Stakeholdermanagement: Fähigkeit zur Zusammenarbeit mit verschiedenen Interessengruppen auf allen Hierarchieebenen, Vermittlung zwischen technischen Experten und nicht-technischen Stakeholdern.
- ⇒ Vertiefte Kenntnisse in DevOps & IaC: Grundlegendes Verständnis der DevOps-Prinzipien und Erfahrung mit Infrastructure-as-Code
- ⇒ Vertiefte Kenntnisse in Sicherheits- und Compliance-Anforderungen, Cloud-Sicherheitskonzepten sowie von branchenspezifischen Compliance-Vorgaben (z. B. DSGVO, ISO 27001) und deren Umsetzung in der Cloud
- ⇒ Kenntnisse und Erfahrungen im Projektmanagement und in der Agilen Produktentwicklung
- ⇒ Die benötigten Kenntnisse und Fähigkeiten werden typischerweise nach einer Berufserfahrung in den einzelnen Bereichen von mindestens 4 Jahren erworben.

2.4.1-(1) [A] Der AN verfügt mindestens über einen Mitarbeiter, der die Anforderungen an einen Senior Cloud Consultant erfüllt und für Projekte im Rahmen des Rahmenvertrages generell zur Verfügung steht.

2.4.1-(2) [I] Bitte geben Sie an, wie viele Mitarbeiter die Rolle „Senior Cloud Consultant“ in Ihrem Unternehmen erfüllen und einnehmen.

### 2.4.2 Senior Cloud Architect

Ein Senior Cloud Architect ist eine Fachkraft, die Cloud-Infrastrukturen und -Lösungen konzipiert, plant und überblickt, um die Ziele zu erfüllen. Er wählt die passenden Cloud-

Plattformen und -Technologien aus und stellt sicher, dass die Architekturen skalierbar, sicher und effizient sind.

Der Senior Cloud Architect berät und unterstützt den Auftraggeber umfassend, um eine robuste und effiziente Cloud-Strategie zu etablieren und weiterzuentwickeln. Seine Hauptaufgaben umfassen die Befähigung der Teams des Auftraggebers, damit diese eigenständig sichere und effiziente Cloud-Architekturen entwickeln können. Des Weiteren ist er maßgeblich am Aufbau von Landing Zones beteiligt und sorgt für die konsequente Umsetzung aller Sicherheits- und Compliance-Anforderungen.

Ziel ist es, eine solide Grundlage zu schaffen, die eine sichere und effiziente Migration sowie den reibungslosen Betrieb von Anwendungen in der ARD/NDR Cloud-Plattform ermöglicht. Einen hohen Stellenwert nimmt auch der Wissenstransfer und das Enablement ein: Durch gezielte Schulungen, Workshops und die Erstellung umfassender Dokumentationen teilt der Senior Cloud Architect sein Fachwissen, um ein breiteres Verständnis und verbesserte Fähigkeiten im Umgang mit Cloud-Technologien innerhalb des Unternehmens zu fördern.

⇒ *Anforderungen an den Senior Cloud Architect:*

- ⇒ Tiefes Verständnis der Architekturprinzipien und Dienste der jeweils verantworteten Public-Cloud-Plattform (AWS, Azure, GCP, STACKIT)
- ⇒ Vertiefte Kenntnisse in der Erstellung von Cloud-Architekturen
- ⇒ Vertiefte Kenntnisse in Aufbau und Betrieb von Landing Zones: Design und Implementierung von Landing Zones für Public-Cloud-Plattformen, einschließlich Automatisierung und Governance, Konfiguration von Policies, Netzwerken, IAM
- ⇒ Vertiefte Kenntnisse in Platform Engineering und Automatisierung: Expertise in Infrastructure-as-Code (IaC)-Tools, Erfahrung im Aufbau von Self-Service-Plattformen für Entwicklerteams, Automatisierung von Infrastruktur- und Plattformbereitstellungen
- ⇒ Vertiefte Kenntnisse in Cloud-Sicherheitsarchitektur: Fundierte Kenntnisse in Cloud-Sicherheitspraktiken, Verständnis von regulatorischen Anforderungen (z. B. DSGVO, ISO 27001) und deren Implementierung
- ⇒ Vertiefte Kenntnisse in Netzwerkdesign und -integration: Expertenwissen in der Konzeption und Konfiguration von Cloud-Netzwerken (z. B. VPC, Subnetze, VPN, Peering, Load Balancing)
- ⇒ Vertiefte Kenntnisse in Governance und Compliance: Kenntnisse in der Automatisierung von Compliance-Prüfungen und der Überwachung von Richtlinien eingehalten
- ⇒ Vertiefte Kenntnisse in Cloud-Kostenmanagement und Optimierung: Erfahrung in der Analyse und Optimierung von Cloud-Kosten, Kenntnisse in der Nutzung von Tools der verantworteten Cloud Plattform
- ⇒ Vertiefte Kenntnisse in Monitoring, Logging und Performance Management: Kenntnisse in der Nutzung von Monitoring- und Logging-Tools der verantworteten Cloud-Plattform, Fähigkeit, Performance-Daten zu analysieren und Optimierungspotenziale zu identifizieren.
- ⇒ Vertiefte Kenntnisse in Identifizierung und Behebung von Sicherheitslücken in Cloud-Umgebungen
- ⇒ Vertiefte Kenntnisse in fachlicher Führung und Kommunikation: Fähigkeit, technische Konzepte klar an Stakeholder zu kommunizieren, Erfahrung in der Zusammenarbeit mit verschiedenen Rollen, Übernahme von technischer Verantwortung und Anleitung von Teams.

⇒ Die benötigten Kenntnisse und Fähigkeiten werden typischerweise nach einer Berufserfahrung in den einzelnen Bereichen von mindestens 4 Jahren erworben.

2.4.2-(1) [A] Der AN verfügt mindestens über einen Mitarbeiter, der die Anforderungen an einen Senior Cloud Architect erfüllt und für Projekte im Rahmen des Rahmenvertrages generell zur Verfügung steht.

2.4.2-(2) [I] Bitte geben Sie an, wie viele Mitarbeiter die Rolle „Senior Cloud Architect“ in Ihrem Unternehmen erfüllen und einnehmen.

### 2.4.3 Cloud Engineer

Ein Cloud Engineer ist ein IT-Spezialist, der Cloud-Infrastrukturen implementiert und verwaltet. Dies beinhaltet die Migration von Anwendungen und Daten in die Cloud sowie die Gewährleistung von Sicherheit, Leistung und Kosteneffizienz. Er arbeitet eng mit anderen IT-Teams zusammen, um skalierbare und zuverlässige Cloud-Lösungen für Unternehmen zu entwickeln und zu optimieren.

Der Cloud Engineer unterstützt im Rahmen der Projekte beim Aufbau einer Cloud-Plattform mittels Infrastructure-as-Code (IaC), u. a. bei der Implementierung von Continuous Integration/Continuous Delivery (CI/CD) Pipelines. Zu seinen Aufgaben zählen ebenfalls die Implementierung von Sicherheitskonzepten, Umsetzung von Standards und Richtlinien (Cloud Governance) entlang der Prinzipien für DevSecOps sowie die Implementierung skalierbarer, performanter, sicherer und zuverlässiger Infrastruktur. Er stellt den kontinuierlichen Wissenstransfer durch Teilen seines Fachwissens mit NDR/ARD-Mitarbeitern, durch Schulungen, Workshops und Dokumentationen sicher und schärft das Bewusstsein für Dev-SecOp-Prinzipien. Der Cloud Engineer übernimmt Betriebsaufgaben wie Systemverwaltung, Konfigurationsaufgaben, Fehlersuche und Behebung.

⇒ *Anforderungen an den Cloud Engineer:*

⇒ Grundkenntnisse in Public-Cloud-Plattformen (AWS, Azure, GCP): Verständnis der Kernkonzepte von Public-Cloud-Anbietern, einschließlich Computer, Storage, Netzwerke und Datenbanken, Fähigkeit, um grundlegende Cloud-Ressourcen zu erstellen und zu konfigurieren.

⇒ Grundkenntnisse im Umgang mit Infrastructure-as-Code (IaC): Praktische Erfahrung mit IaC-Tools wie Terraform und OpenTofu, Verständnis von Versionskontrollsystemen wie Git

⇒ Grundkenntnisse im Aufbau von Landing Zones: Grundlegende Konzeption von Landing Zones (z. B. standardisierte Cloud-Umgebungen mit Governance und Sicherheitsrichtlinien), Fähigkeit, um Änderungen und Erweiterungen an bestehenden Landing Zones vorzunehmen.

⇒ Grundkenntnisse in Grundlagen der Cloud-Sicherheit: Verständnis für Sicherheitskonzepte wie IAM (Identity and Access Management), Firewalls, Verschlüsselung und Netzwerksicherheit, Fähigkeit, um Sicherheitsrichtlinien gemäß Vorgaben umzusetzen und Cloud-spezifische Sicherheitsdienste zu nutzen.

⇒ Grundkenntnisse in Monitoring und Fehlerbehebung: Grundkenntnisse in der Nutzung von Monitoring- und Logging-Tools, Fähigkeit, um einfache Probleme zu identifizieren und Fehler mit Unterstützung des Teams zu beheben.

⇒ Grundkenntnisse in Grundlagen der Netzwerkkonfiguration: Fähigkeit, um einfache Netzwerkkonfigurationen umzusetzen (z. B. Anlegen von Subnetzen oder Sicherheitsgruppen).

⇒ Grundkenntnisse in Zusammenarbeit mit Platform Engineering Teams: Fähigkeit, um einfache Aufgaben im Platform Engineering (z. B. Skripterstellung oder Konfigurationsanpassungen) umzusetzen.

- ⇒ Grundkenntnisse in der Automatisierung von Arbeitsabläufen: Automatisierung von Infrastruktur- und Plattformaufgaben mit Tools wie Bash, Python, PowerShell
- ⇒ Grundkenntnisse in der Dokumentation und technischen Kommunikation: Fähigkeit, um technische Dokumentationen zu erstellen und zu pflegen.
- ⇒ Nachweis in Projekten seiner Fähigkeit, sich schnell in neue Tools und Technologien einzuarbeiten.

2.4.3-(1) [A] Der AN verfügt mindestens über 1 Mitarbeiter, der die Anforderungen an einen Cloud Engineer erfüllt und für Projekte im Rahmen des Rahmenvertrages generell zur Verfügung steht.

2.4.3-(2) [I] Bitte geben Sie an, wie viele Mitarbeiter die Rolle „Cloud Engineer“ in Ihrem Unternehmen erfüllen und einnehmen.

#### 2.4.4 Senior Cloud Engineer

Ein Senior Cloud Engineer ist ein IT-Spezialist, der Cloud-Infrastrukturen entwirft und implementiert. Dies beinhaltet die Migration von Anwendungen und Daten in die Cloud sowie die Gewährleistung von Sicherheit, Leistung und Kosteneffizienz. Er arbeitet eng mit anderen IT-Teams zusammen, um skalierbare und zuverlässige Cloud-Lösungen für Unternehmen zu entwickeln und zu optimieren.

Für den erfolgreichen Betrieb und die Weiterentwicklung einer Cloud-Plattform ist ein Senior Cloud Engineer mit unterschiedlichen Spezialisierungen unerlässlich. Es wird ein Experte in den Ausprägungen Network für die Konfiguration und Wartung der Cloud-Netzwerkinfrastruktur, Security für die Absicherung der gesamten Cloud-Umgebung und DevOps benötigt – letzteres sowohl mit Fokus auf Infrastruktur (Automatisierung und Bereitstellung) als auch auf Entwicklung (Anwendungsintegration und -bereitstellung). Abgerundet wird das Team durch einen Monitoring-Spezialisten, der die Leistungsfähigkeit und Verfügbarkeit der Cloud-Services kontinuierlich überwacht und optimiert. Diese Spezialisierungen werden über die Miniwettbewerbe genauer spezifiziert und abgerufen.

Der Senior Cloud Engineer unterstützt im Rahmen der Projekte bei der Planung und dem Aufbau der Cloud-Plattform mittels Infrastructure-as-Code (IaC), u. a. beim Entwurf und der Implementierung von Continuous Integration/Continuous Delivery (CI/CD) Pipelines. Zu seinen Aufgaben zählen ebenfalls die Entwicklung und Implementierung von Sicherheitskonzepten, Umsetzung von Standards und Richtlinien (Cloud Governance) entlang der Prinzipien für DevSecOps sowie Design und Implementierung skalierbarer, performanter, sicherer und zuverlässiger Infrastruktur. Er stellt den kontinuierlichen Wissenstransfer durch Teilen seines Fachwissens mit NDR/ARD-Mitarbeitern, durch Schulungen, Workshops und Dokumentationen sicher und schärft das Bewusstsein für DevSecOp-Prinzipien. Der Senior Cloud Engineer übernimmt Betriebsaufgaben wie Fehlersuche und Behebung bei komplexen Fehlerbildern.

⇒ *Anforderungen an den Senior Cloud Engineer:*

- ⇒ Vertiefte Kenntnisse und Expertise in Public-Cloud-Plattformen (AWS, Azure, GCP): Tiefes Wissen über die Kernkomponenten und Dienste der führenden Public-Cloud-Plattformen, Expertise in der effizienten Bereitstellung, Konfiguration und Optimierung von Cloud-Ressourcen in den Public-Cloud-Umgebungen
- ⇒ Vertiefte Kenntnisse und Expertise im Aufbau und Betrieb von Landing Zones: Erfahrung im Design und der Implementierung skalierbarer Landing Zones, einschließlich Automatisierung und Governance
- ⇒ Vertiefte Kenntnisse und Expertise in Infrastructure-as-Code (IaC) und Automatisierung: Tiefes Verständnis von IaC-Tools wie Terraform und OpenTofu, Erfahrung mit CI/CD-Pipelines und Automatisierung in Entwicklungs- und Betriebsprozessen

- ⇒ Vertiefte Kenntnisse in Platform-Engineering-Arbeiten: Erfahrung mit der Integration von Tools wie Kubernetes, Docker und serverlosen Technologien
- ⇒ Vertiefte Kenntnisse in Cloud-Sicherheitskonzepten: Kenntnisse in Sicherheits- und Compliance-Anforderungen (z. B. IAM, Zero Trust, Verschlüsselung), Zusammenarbeit mit Security Architects zur Sicherstellung eines sicheren Cloud-Betriebs
- ⇒ Vertiefte Kenntnisse in Netzwerkkonfiguration und -integration: Kenntnisse in der Konfiguration von Netzwerken in der Cloud (z. B. VPCs, Subnetze, Firewalls, VPNs, Peering)
- ⇒ Vertiefte Kenntnisse in Monitoring und Betrieb: Erfahrung mit Monitoring- und Logging-Tools
- ⇒ Vertiefte Kenntnisse in der Optimierung von Cloud-Kosten: Nutzung von Kostenmanagement-Tools der Public-Cloud-Anbieter
- ⇒ Vertiefte Kenntnisse in Fehlerbehebung und Incident Management: Fähigkeit, komplexe Probleme in Multicloud-Umgebungen zu identifizieren und zu beheben, Erfahrung in der Analyse von Logs, Systemmetriken und Netzwerkkonfigurationen zur Ursachenfindung
- ⇒ Vertiefte Kenntnisse in Technischer Dokumentation und Zusammenarbeit: Fähigkeit, technische Dokumentationen zu erstellen, z. B. für IaC-Skripte, Netzwerkkonfigurationen und Plattformarchitekturen
- ⇒ Die benötigten Kenntnisse und Fähigkeiten werden typischerweise nach einer Berufserfahrung in den einzelnen Bereichen von mindestens 4 Jahren erworben.

2.4.4-(1) [A] Der AN verfügt mindestens über 1 Mitarbeiter, der die Anforderungen an einen Senior Cloud Engineer erfüllt und für Projekte im Rahmen des Rahmenvertrag generell zur Verfügung steht.

2.4.4-(2) [I] Bitte geben Sie an, wie viele Mitarbeiter die Rolle „Senior Cloud Engineer“ in Ihrem Unternehmen erfüllen und einnehmen.

## 2.4.5 Cloud Security Architect

Ein Cloud Security Architect entwirft und implementiert Sicherheitsstrategien und -architekturen für Cloud-Umgebungen. Er stellt sicher, dass alle Cloud-Ressourcen, Daten und Anwendungen vor Bedrohungen geschützt sind und Compliance-Anforderungen erfüllt werden. Dies beinhaltet die Auswahl und Konfiguration geeigneter Sicherheitstools und -kontrollen sowie die Entwicklung von Best Practices für die Cloud-Sicherheit.

Die Aufgaben eines Cloud Security Architect im Rahmen der Projekte umfassen u. a. die strategische Planung, das Design und die Implementierung robuster Sicherheitsarchitekturen für Cloud-Umgebungen. Dies beinhaltet die Entwicklung umfassender Sicherheitskonzepte, die auf die spezifischen Anforderungen und Risikoprofile des Unternehmens zugeschnitten sind und Public, Private sowie Hybride Clouds berücksichtigen. Ein zentraler Aspekt ist die Definition und Implementierung von Sicherheitsrichtlinien und -verfahren sowie die Verwaltung von Zugriffskontrollen, um die Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Systemen zu gewährleisten. Des Weiteren ist der Cloud Security Architect für die kontinuierliche Überwachung und Analyse von Sicherheitsprotokollen zuständig, um Sicherheitsvorfälle frühzeitig zu erkennen und in Zusammenarbeit mit dem Security Operations Center (SOC) effektiv darauf zu reagieren. Er bewertet und führt neue Sicherheitstechnologien ein, implementiert und verwaltet Verschlüsselungslösungen und Key Management Systeme. Neben der technischen Umsetzung berät er Stakeholder und Führungskräfte in allen Fragen der Cloud-Sicherheit, arbeitet eng mit anderen Modulen der digitalen Erneuerung, Entwicklungs-, Betriebs- und DevOps-Teams zusammen und stellt die Einhaltung relevanter Sicherheitsstandards und gesetzlicher Bestimmungen wie der DSGVO sicher. Dazu gehört auch die

Koordination von Audits und Zertifizierungen. Schließlich verfolgt der Cloud Security Architect kontinuierlich aktuelle Trends und Best Practices im Cloud- und Cybersicherheitsbereich, um das Shared Responsibility Model zu verstehen und Zero-Trust-Modelle zu implementieren.

⇒ *Anforderungen an den Cloud Security Architect:*

- ⇒ Vertiefte Kenntnisse in Strategischer Cloud Security Architektur und Design: Fähigkeit, eine ganzheitliche Sicherheitsstrategie und Architektur für eine Multicloud-Plattform zu entwerfen, Auswahl geeigneter Sicherheitskontrollen und deren Integration in die Plattform
- ⇒ Vertiefte Kenntnisse in Multicloud-Sicherheitsmodellen und -Services: Tiefe Kenntnisse der Sicherheitsangebote und -modelle der großen Cloud-Anbieter (z. B. AWS, Azure, GCP)
- ⇒ Vertiefte Kenntnisse in DevSecOps und Infrastructure-as-Code (IaC) Security: Kenntnisse der Integration von Sicherheitsmechanismen in den CI/CD-Pipeline-Prozess
- ⇒ Vertiefte Kenntnisse in Policy-Design und Governance: Erstellung von Sicherheitsrichtlinien (Policies) und Governance-Modellen für Cloud-Plattformen und Übersetzung abstrakter Sicherheitsanforderungen in konkrete Vorgaben.
- ⇒ Vertiefte Kenntnisse in Cloud-Netzwerksicherheit: Expertise in der Konzeption und Absicherung der Netzwerkinfrastruktur in einer Multicloud-Umgebung, insbesondere Virtual Private Clouds (VPC), Subnetzen, Firewalls, VPNs und hybriden Netzwerklösungen
- ⇒ Vertiefte Kenntnisse in Risikomanagement und Bedrohungsmodellierung: Fähigkeit, um Bedrohungen und Risiken in einer Multicloud-Umgebung zu identifizieren und zu bewerten sowie die Entwicklung geeigneter Gegenmaßnahmen.
- ⇒ Vertiefte Kenntnisse in Compliance und regulatorischen Anforderungen: Kenntnis der regulatorischen und branchenspezifischen Standards wie ISO 27001, DSGVO, NIST sowie deren Umsetzung in Cloud-Umgebungen. Sicherstellung, dass die Security-Kontrollen nachweisbar implementiert und wirksam sind.
- ⇒ Vertiefte Kenntnisse in sicherheitsrelevantes Logging, Monitoring und Incident Response: Erfahrung in der Etablierung von robusten Monitoring- und Alerting-Systemen und Incident Response
- ⇒ Vertiefte Kenntnisse in Daten- und Anwendungssicherheit in der Cloud: Konzeptionierung von Verschlüsselung, Key Management (KMS), Secrets Management (Secrets Manager, Vault) sowie die Unterstützung der Entwicklerteams
- ⇒ Vertiefte Kenntnisse in Kommunikation, Beratung und Stakeholdermanagement: Exzellente Kommunikationsfähigkeit, um komplexe Sicherheitsthemen an technische und nicht-technische Stakeholder zu vermitteln. Fähigkeit, andere Teams (Cloud Architects, Engineers) bei der Umsetzung zu unterstützen und zu befähigen.
- ⇒ Die benötigten Kenntnisse und Fähigkeiten werden typischerweise nach einer Berufserfahrung in den einzelnen Bereichen von mindestens 4 Jahren erworben.

2.4.5-(1) [B-J/N] Der AN verfügt über mindestens einen Mitarbeiter, der die Anforderungen eines Cloud Security Architect erfüllt und für Projekte im Rahmen des Rahmenvertrages generell zur Verfügung steht.

Ja = 10 Pkt., nein = 0 Pkt.

2.4.5-(2) [I] Bitte geben Sie an, wie viele Mitarbeiter die Rolle „Cloud Security Architect“ in Ihrem Unternehmen erfüllen und einnehmen.

## 2.4.6 Cloud FinOps Expert

Ein Cloud FinOps Expert ist ein Spezialist, der Finanzmanagement-Prinzipien mit Cloud-Operationen verbindet, um die Kosten für Cloud-Ressourcen transparent zu machen und zu optimieren. Er analysiert Cloud-Ausgaben, identifiziert Einsparpotenziale und implementiert Strategien zur Kostenkontrolle, wie z. B. die Nutzung von Reserved Instances oder Spot-Instanzen. Sein Ziel ist es, die finanzielle Effizienz von Cloud-Investitionen zu maximieren und die Zusammenarbeit zwischen Finanz-, Technik- und Geschäftsteams zu fördern.

Der Cloud FinOps Expert fungiert im Rahmen der Projekte als zentrale Schaltstelle zwischen Finanz-, Technik- und Geschäftsteams, um die finanzielle Effizienz von Cloud-Investitionen zu maximieren. Seine Kernaufgaben umfassen die kontinuierliche Überwachung, Analyse und Optimierung der Cloud-Kosten über verschiedene Cloud-Anbieter hinweg. Hierfür implementiert er robuste Kostenmanagement- und Reporting-Systeme, identifiziert Verschwendungsquellen und erarbeitet Strategien zur Kostenreduzierung, wie beispielsweise die effektive Nutzung von Reserved Instances, Savings Plans oder Spot-Instanzen. Darüber hinaus fördert er eine Kultur der Kostenverantwortung und des Bewusstseins innerhalb des Unternehmens, indem er Best Practices etabliert, Schulungen anbietet und die Zusammenarbeit zwischen Entwicklungsteams und der Finanzabteilung stärkt. Er berät bei der Budgetplanung für Cloud-Ressourcen, erstellt Prognosen und stellt sicher, dass die Ausgaben im Einklang mit den Geschäftszielen und dem ROI stehen. Kurz gesagt, der Cloud FinOps Expert ist der Katalysator, der Unternehmen dabei hilft, das volle Potenzial ihrer Cloud-Investitionen auszuschöpfen, indem er Transparenz schafft, Effizienz steigert und eine kostenbewusste Entscheidungsfindung ermöglicht.

⇒ *Anforderungen an den Cloud FinOps Expert:*

- ⇒ Vertiefte Kenntnisse in strategischem Kostenmanagement, z. B. FinOps: Fähigkeit, ein ganzheitliches Kostenmanagement für eine Multicloud-Plattform zu konzipieren und durch die Unterstützung der Engineers zu implementieren, Integration des Frameworks in die bestehenden Platform-Engineering-Prozesse
- ⇒ Vertiefte Kenntnisse in Multicloud-Kostenmodellen und Reporting: Erfahrung mit mindestens zwei großen Public-Cloud-Plattformen und deren Kostenstrukturen, tiefe Kenntnisse der Kostenmodelle und Reporting-Tools der Public-Cloud-Anbieter
- ⇒ Vertiefte Kenntnisse in Tagging- und Naming-Konzept-Design und Governance: Erfahrung in der Implementierung und Überwachung von Tagging-Strategien
- ⇒ Vertiefte Kenntnisse in Kostenverrechnung und Showback/Chargeback-Modelle: Erfahrung in der Entwicklung und Umsetzung von transparenten Verrechnungskonzepten (Chargeback oder Showback), um die verursachungsgerechte Kostenverteilung zwischen Teams oder Organisationseinheiten zu gewährleisten.
- ⇒ Vertiefte Kenntnisse in der Konzeption und der Zusammenarbeit mit Engineering Teams zur Automatisierung von Kostenmanagement-Prozessen
- ⇒ Vertiefte Kenntnisse in Kostenoptimierung durch Ressourcenmanagement: Expertise in der Identifizierung und Umsetzung von Kosteneinsparpotenzialen durch Optimierung der Ressourcen, Nutzung von Rabattprogrammen (z. B. Reserved Instances, Savings Plans)
- ⇒ Vertiefte Kenntnisse in finanzieller Budgetierung und Prognose: Fähigkeit, Budgets für Cloud-Umgebungen zu planen und zu überwachen.
- ⇒ Die benötigten Kenntnisse und Fähigkeiten werden typischerweise nach einer Berufserfahrung in den einzelnen Bereichen von mindestens 4 Jahren erworben.

- 2.4.6-(1) [B-J/N] Der AN verfügt über mindestens einen Mitarbeiter, der die Anforderungen an einen Cloud FinOps Expert erfüllt und für Projekte im Rahmen des Rahmenvertrag generell zur Verfügung steht.

Ja = 10 Pkt., nein = 0 Pkt.

- 2.4.6-(2) [I] Bitte geben Sie an, wie viele Mitarbeiter die Rolle „Cloud FinOps Expert“ in Ihrem Unternehmen erfüllen und einnehmen.

## 2.4.7 Cloud GreenOps Expert

Ein Cloud GreenOps Expert ist ein Spezialist, der sich darauf konzentriert, die Umweltauswirkungen von Cloud-Infrastrukturen zu minimieren, indem er Energieeffizienz und Nachhaltigkeit in den Mittelpunkt rückt. Er analysiert den Energieverbrauch von Cloud-Ressourcen und identifiziert Optimierungspotenziale, um den CO<sub>2</sub>-Fußabdruck zu reduzieren. Sein Ziel ist es, nachhaltige Cloud-Praktiken zu implementieren, die sowohl ökologische als auch ökonomische Vorteile bieten.

Der Cloud GreenOps Expert konzentriert sich im Rahmen der Projekte auf die Minimierung des ökologischen Fußabdrucks von Cloud-Infrastrukturen und treibt die Nachhaltigkeit in Cloud-Operationen voran. Seine Hauptaufgaben umfassen die Analyse und Optimierung des Energieverbrauchs von Cloud-Ressourcen, um Emissionen zu reduzieren und die Effizienz zu steigern. Dies beinhaltet die Identifizierung von inaktiven oder überdimensionierten Ressourcen, die Implementierung von „Right-Sizing“-Strategien für virtuelle Maschinen und Container sowie die Nutzung von energieeffizienten Services und Regionen der Cloud-Anbieter. Der Cloud GreenOps Expert berät Teams bei der Auswahl nachhaltiger Architekturen und Praktiken, fördert den Einsatz von erneuerbaren Energien durch die Cloud-Anbieter und entwickelt Metriken und Reporting-Systeme zur Messung und Berichterstattung der Umweltauswirkungen. Er arbeitet eng mit FinOps- und Entwicklungsteams zusammen, um Kostenoptimierung mit Nachhaltigkeitszielen zu vereinen und eine Kultur der „grünen“ Cloud-Nutzung im gesamten Unternehmen zu etablieren.

⇒ *Anforderungen an den Cloud GreenOps Expert:*

- ⇒ Vertiefte Kenntnisse in strategischem Nachhaltigkeits-Framework-Design, z. B. GreenOps: Erfahrung in der Konzipierung eines ganzheitlichen Nachhaltigkeit-Frameworks für eine Multicloud-Plattform und der Integration von z. B. GreenOps in die Platform-Engineering-Prozesse
- ⇒ Vertiefte Kenntnisse in Messung und Reporting von Nachhaltigkeitsmetriken: Tiefe Kenntnisse der Tools und Ansätze der Public-Cloud-Anbieter zur Messung des Energieverbrauchs und der CO<sub>2</sub>-Emissionen der Cloud-Ressourcen
- ⇒ Vertiefte Kenntnisse in Workload-Optimierung für Energieeffizienz: Erfahrung in der Optimierung von IT-Ressourcen mit Schwerpunkt auf Energieeffizienz
- ⇒ Vertiefte Kenntnisse in der Konzeption von GreenOps-Prozessen: Expertise in der Automatisierung von GreenOps-Aktivitäten mithilfe von Skripten (z. B. Python, PowerShell) oder IaC-Tools (z. B. Terraform) und der Implementierung in Zusammenarbeit mit Engineering Teams
- ⇒ Vertiefte Kenntnisse in der Kollaboration mit Platform-Engineering-Teams: Erfahrung in der Zusammenarbeit mit Platform-Engineering-Teams, um nachhaltige Cloud-Architekturen und Betriebsmodelle zu entwickeln und sicherzustellen, dass Nachhaltigkeitsziele in technischen Entscheidungen berücksichtigt werden.
- ⇒ Vertiefte Kenntnisse im Lebenszyklus-Management von Cloud-Ressourcen: Implementierung von Prozessen zur Identifizierung und zum Abbau von ungenutzten oder überdimensionierten Ressourcen

- ⇒ Vertiefte Kenntnisse in Nachhaltigkeitsstandards und Compliance: Vertrautheit mit internationalen Nachhaltigkeitsstandards (Green IT), Erfahrung in der Umsetzung von Nachhaltigkeits- und Compliance-Standards, vorzugsweise im IT- oder Cloud-Bereich
- ⇒ Vertiefte Kenntnisse in Governance und Policy-as-Code für GreenOps: Fähigkeit, Richtlinien zur Förderung von Nachhaltigkeit in der Plattform zu definieren und diese in Zusammenarbeit mit Engineering Teams umzusetzen.
- ⇒ Vertiefte Kenntnisse in Kommunikation, Schulung und Befähigung der Kunden der Plattform: Fähigkeit, Nachhaltigkeitsziele und -maßnahmen sowohl technischen als auch nicht-technischen Stakeholdern zu vermitteln und Veränderungen im Betrieb voranzutreiben, Erfahrung in der Erstellung von Best-Practice-Leitfäden, Workshops oder Schulungen.

2.4.7-(1) [B-J/N] Der AN verfügt über mindestens einen Mitarbeiter, der die Anforderungen eines Cloud GreenOps Expert erfüllt und für Projekte im Rahmen des Rahmenvertrages generell zur Verfügung steht.

Ja = 10 Pkt., nein = 0 Pkt.

2.4.7-(2) [I] Bitte geben Sie an, wie viele Mitarbeiter die Rolle „Cloud GreenOps Expert“ in Ihrem Unternehmen erfüllen und einnehmen.

### 3 Serviceanforderungen im Rahmen der Projekte

#### 3.1 Servicelevel/Servicezeiten

Generell gibt es im Rahmen von Projekten verschiedene Anforderungen an den AN:

⇒ Bronze:

- 08:00-16:30 Uhr, Mo-Do (Werktag im Bundesland Hamburg) und
- 08:00-15:00 Uhr, freitags (Werktag im Bundesland Hamburg)
- keine Bereitschaften abends/nachts oder Wochenende/feiertags

⇒ Silber:

- 8-18 Uhr (an allen Werktagen außer Samstag im Bundesland Hamburg)
- keine Bereitschaften abends/nachts oder Wochenende/feiertags

⇒ Gold:

- 8-18 Uhr (an allen Werktagen außer Samstag im Bundesland Hamburg)
- Bereitschaften Wochenende/feiertags 9-23 Uhr

⇒ Platin:

- 8-18 Uhr (an allen Werktagen außer Samstag im Bundesland Hamburg)
- 24/7 Bereitschaften abends/nachts oder Wochenende/feiertags

⇒ Anforderungen:

- 3.1-(1) [A] Der AN sichert zu, dass Servicelevel „Bronze“ im Rahmen von Projekten abgedeckt werden kann.
- 3.1-(2) [B-J/N] Der AN kann zusichern, dass Servicelevel „Silber“ im Rahmen von Projekten abgedeckt wird.  
Ja = 10 Pkt., nein = 0 Pkt.
- 3.1-(3) [B-J/N] Der AN kann zusichern, dass die Zeitenrahmen von Gold im Rahmen von Projekten abgedeckt werden.  
Ja = 10 Pkt., nein = 0 Pkt.
- 3.1-(4) [B-J/N] Der AN kann zusichern, dass die Zeitenrahmen von Platin im Rahmen von Projekten abgedeckt werden.  
Ja = 10 Pkt., nein = 0 Pkt.
- 3.1-(5) [A] In seltenen Ausnahmefällen muss ein Bereitschaftsdienst übernommen werden, auch wenn Servicelevel „Platin/Gold“ als nicht erfüllt beantwortet wurde.

## **4 Organisatorische Regeln**

### **4.1 Allgemein**

Im Rahmen der Miniwettbewerbe werden die Organisatorischen Regelungen für die entsprechenden Projekte vorgegeben/vereinbart.

### **4.2 Preisblatt**

Im Preisblatt (PB) auf der Seite „Titelblatt“ ist der Bietername einzutragen.

Auf der Seite „Stunden“ sind die Stundensätze und die prozentualen Zuschläge für Arbeiten außerhalb der Regelarbeitszeit einzutragen.

Es wird ein Stundensatz für Remote-Arbeiten und ein Stundensatz für Vor-Ort-Tätigkeiten abgefragt.

Es werden keine weiteren Nebenkosten oder Reisekosten vergütet.

Es sind für die folgenden Rollen entsprechende Stundensätze und Zuschläge einzutragen:

- ⇒ Senior Cloud Consultant/Cloud FinOps Expert/Cloud GreenOps Expert
- ⇒ Senior Cloud Architect/Cloud Security Architect
- ⇒ Cloud Engineer
- ⇒ Senior Cloud Engineer

Die angegebenen Preise gelten als maximale Stundensätze für die späteren Projekte.