+++ LEISTUNGSBESCHREIBUNG +++

1. Gegenstand der Beschaffung

1.1. Kurze Beschreibung der Leistung

Der Bereich Strategisches Marketing benötigt ab 1. Februar 2027 kompetente Dienstleister für das Echtzeitmonitoring/Social Listening im Web und Social Media sowie für die Auswertung ihrer Google Places Statistiken.

1.2. Angaben zur Losteilung

Die Leistung wird in zwei Losen ausgeschrieben:

Los 1: Social Listening

Los 2: Google Places

1.3. Laufzeit

Der Vertrag hat eine feste Laufzeit von 12 Monaten, beginnend mit Vertragsschluss am 01. Februar 2027. Der Vertrag verlängert sich automatisch um jeweils weitere 12 Monate, sofern die DAK-Gesundheit ihn nicht mit einer Frist von 3 Monaten zum Ende des jeweiligen Vertragsjahres kündigt. Eine automatische Verlängerung ist höchstens dreimal möglich. Die maximale Vertragslaufzeit beträgt damit 48 Monate. Der Vertrag endet spätestens mit Ablauf des 31.01.2031, ohne dass es einer Kündigung bedarf.

2. Anforderungen an die zu erbringende Leistung | Los 1: Social Listening

Die DAK-Gesundheit beabsichtigt, mit dem Tool Nennungen über sich selbst und relevante Leistungs- und Servicethemen im Web und in den Sozialen Netzwerken zu beobachten, auszuwerten und zu analysieren. Die Ergebnisse und Analysen dienen vor allem der Krisenprävention, dem Krisenmonitoring und der Reputationsanalyse. Das Tool soll daher einen umfangreichen Überblick darüber geben, was im Web und in den Sozialen Medien allgemein über die DAK-Gesundheit, relevante Wettbewerber und weitere, spezielle von der DAK-G definierten Themen veröffentlicht wird.

Dazu benötigt die DAK-Gesundheit:

- ein übersichtliches Onlinetool mit Zugriffsrechten für bis zu 10 Mitarbeiter
- eine Echtzeitüberwachung/Social Listening des Webs und der sozialen Netzwerke
- Suche und Trefferanzeige nach Schlagworten, Zeiträumen, Quellen
- exportierbare Auswertungen von Daten und Statistiken mit konfigurierbaren grafischen Darstellmöglichkeiten der Ergebnisse
- individuell konfigurierbare Allerts
- Support seitens des Anbieters beim Setup des Tools mit den relevanten Schlagwörtern und bei Bedarf bei der Erstellung von Analysen und Auswertungen

- Schulung aller beteiligten Mitarbeiter bei der DAK-Gesundheit zur Nutzung des Tools und zur eigenständigen Erstellung der Reporte

Folgende (soziale) Medien sollen mindestens überwacht werden

- soziale Netzwerke (Facebook, Instagram, X, YouTube, LinkedIn)
- Foren
- Blogs
- News-Seiten
- Websites
- Bewertungsplattformen
- Reddit
- TikTok

Als Mindestanforderung sollen zudem

- die Trefferergebnisse nach Anzahl, Schlagworten, Zeitraum, Quelle sortierbar mit direkter Verlinkung zur Quellseite angezeigt werden
- eigene Alerts durch den User eingerichtet werden können.

Technische Mindestanforderungen:

- Das Tool läuft auf allen Standardbrowsern (zum Beispiel Crome, Edge, Firefox) in der aktuellen Version sowie mindestens in den jeweils zwei vorherigen Versionen.
- Das Tool und alle Funktionen sind grundsätzlich 24/7 verfügbar.
- Tool-Ausfälle und Cyberangriffe werden umgehend an die DAK-G gemeldet.
- Über Versionsupdates wird mindestens zwei Wochen im Voraus informiert.

Weitere Qualitätsanforderungen:

- einfache, vom User selbst vornehmbare Einrichtung zusätzlicher Suchen zu Themen und Kampagnen
- einfaches Handling, übersichtliches Design
- durch den User anpassbare Suchen und Filter
- einfache, vom User konfigurierbare Erstellung und Export von grafisch dargestellten Trefferstatistiken als PDF und pptx
- Stimmungsanalyse der Treffer in positiv, neutral oder negativ
- Trend- und Stimmungsentwicklung
- Beschreibung des Tools (Bedienungsanleitung) als PDF

Außerdem sollten optional folgende Plattformen überwacht werden:

- Snapchat
- Pinterest
- Xing

Außerdem sollte stets die Möglichkeit zur technischen Weiterentwicklung gegeben sein, sodass zukünftig auch weitere/neue Kanäle ergänzt werden können.

Zum Ende der Vertragslaufzeit stellt der Anbieter der DAK-Gesundheit alle zur Fortführung des Social Listenings erforderlichen und der DAK-Gesundheit zustehenden Daten, Informationen, Unterlagen und Konfigurationen vollständig zur Verfügung.

Dies umfasst insbesondere:

- Suchlogiken und Suchprofile,
- Keywords und Suchbegriffe,
- Themen- und Suchcluster,
- Quellen-, Filter- und sonstige Konfigurationen,
- relevante Datenbestände und Exporte sowie
- sonstige Informationen und Unterlagen, die für eine möglichst unterbrechungsfreie Fortführung des Monitorings erforderlich sind.

2.1. Team

Die DAK-Gesundheit benötigt bei Bedarf technische und inhaltliche Beratung und Unterstützung bei der Erstellung von Analysen und Auswertungen durch ein kompetentes Team seitens des Anbieters.

Es wird mindestens ein Research Analyst und mindestens ein Senior Analyst benötigt sowie jeweils mindestens eine entsprechende Vertretungsoption.

Research Analyst

Aufgaben:
- Beratung
- Reporting- und Analyseerstellung
- Kampagnenkonzeption
- Kampagnenmodellierung

Das vollständige Skillprofil finden Sie in den weiteren Ausschreibungsunterlagen.

Senior Analyst

Aufgaben:
- Beratung
- Reporting- und Analyseerstellung
- Kampagnenkonzeption
- Kampagnenmodellierung

Das vollständige Skillprofil finden Sie in den weiteren Ausschreibungsunterlagen.

2.2. Zugriff durch eine Agentur

Der Zugriff durch die DAK-Gesundheit muss auch durch eine von der DAK-Gesundheit ermächtigte Agentur erfolgen, die die gleichen Rechte wie die DAK-Gesundheit hat.

3. Anforderungen an die zu erbringende Leistung | Los 2: Google Places

Die DAK-Gesundheit beabsichtigt, mit dem Tool die Bewertungen ihrer Google Places Geschäftsstellen zu monitoren.

Das Tool soll für alle Unternehmensstandorte (ca. 300 Stück)

- die bisherigen sowie neue Rezensionen zentral erfassen.
- die Auswertung von Google Bewertungen ermöglichen.
- Veränderungen der Sternebewertungen dokumentieren.
- exportierbare Auswertungen von Daten und Statistiken erstellen

Dazu benötigt die DAK-Gesundheit

- ein übersichtliches Onlinetool mit Zugriffsrechten für bis zu fünf Mitarbeiter
- eine Echtzeit-Anzeige der Sternebewertungen für die zur DAK-Gesundheit gehörenden Googles Places
- konfigurierbare und exportierbare Auswertungen von Daten und Statistiken mit konfigurierbaren grafischen Darstellmöglichkeiten der Ergebnisse (als Excel sowie PDF) inkl. farbliches Scoring
- die Möglichkeit einen monatlichen Report für verschiedene Verteilergruppen anzulegen, die den Report monatlich via E-Mail erhalten
- Support seitens des Anbieters beim Setup des Tools mit den zur DAK-Gesundheit gehörenden Google Places Geschäftsstellen sowie beim Setup der Reporting-Struktur
- Schulung aller beteiligten Mitarbeiter bei der DAK-Gesundheit zur Nutzung des Tools und zur eigenständigen Erstellung der Reporte

Folgende Daten werden mindestens benötigt:

- Anzahl neuer Bewertungen
- Gesamtzahl der Bewertungen
- Anteil der 1, 2, 3, 4 und 5 Sterne-Bewertung
- Durchschnittliche Sternebewertung (auf Monats- und Jahresbasis)
- Entwicklung der Sternebewertung (auf Monats- und Jahresbasis)
- Ausgabe aller Dienststellen, auch wenn keine Bewertung abgegeben wurde

Folgende Daten je Google Places Standort werden mindestens benötigt:

- Anzahl neuer Bewertungen
- Gesamtzahl der Bewertungen
- Anteil der 1, 2, 3, 4 und 5 Sterne-Bewertung
- Durchschnittliche Sternebewertung (auf Monats- und Jahresbasis)
- Entwicklung der Sternebewertung (auf Monats- und Jahresbasis)

Technische Mindestanforderungen:

- Das Tool läuft auf allen Standardbrowsern (zum Beispiel Crome, Edge, Firefox) in der aktuellen Version sowie mindestens in den jeweils zwei vorherigen Versionen.
- Das Tool und alle Funktionen sind grundsätzlich 24/7 verfügbar.
- Tool-Ausfälle und Cyberangriffe werden umgehend an die DAK-Gesundheit gemeldet.
- Über Versionsupdates wird mindestens zwei Wochen im Voraus informiert.

Weitere Qualitätsanforderungen:

- einfaches Handling, übersichtliches Design
- durch den User anpassbare Suchen und Filter
- einfache vom User konfigurierbare Erstellung von Reports und Export von grafisch dargestellten Trefferstatistiken als PDF und pptx
- monatlicher automatischer Versand der Reports an definierbare E-Mail-Verteiler
- (Regionale) Zusammenfassung von Standorten
- Stimmungsanalyse der Treffer in positiv, neutral oder negativ
- Trend- und Stimmungsentwicklung
- Beschreibung des Tools (Bedienungsanleitung) als PDF

3.1. Team

Die DAK-Gesundheit benötigt bei Bedarf technische und inhaltliche Beratung und Unterstützung bei der Erstellung von Analysen und Auswertungen durch ein kompetentes Team seitens des Anbieters – zum Beispiel in Form von monatlichen und quartalsweisen Berichten.

Es wird mindestens ein Daten Analyst und mindestens ein Senior Analyst benötigt sowie jeweils mindestens eine entsprechende Vertretungsoption.

Daten Analyst

Aufgaben:
- Beratung
- Reporting- und Analyseerstellung

Das vollständige Skillprofil finden Sie in den weiteren Ausschreibungsunterlagen.

Senior Analyst

Aufgaben:
- Beratung
- Reporting- und Analyseerstellung

Das vollständige Skillprofil finden Sie in den weiteren Ausschreibungsunterlagen.

3.2. Zugriff durch eine Agentur

Der Zugriff durch die DAK-Gesundheit muss auch durch eine von der DAK-Gesundheit ermächtigte Agentur erfolgen, die die gleichen Rechte wie die DAK-Gesundheit hat.

4. +++ VERARBEITUNG PERSONENBEZOGENER DATEN +++

Bei beiden genannten Anforderung werden sehr wahrscheinlich folgende personenbezogene Sozialdaten verarbeitet:

Art der verwendeten Sozialdaten

Vor allem:

- Namen
- Adressen
- Geburtsdaten
- Versichertennummer
- Versichertenverhältnisse
- Versichertenanliegen

Grundsätzlich können personenbezogene Daten jeglicher Art verarbeitet werden, sofern diese proaktiv von den betroffenen Personen im Internet veröffentlicht werden.

Kategorien der betroffenen Personen

Vor allem:

- Versicherte der DAK-Gesundheit
- Versicherte anderer Krankenkassen, die sich für die DAK-Gesundheit interessieren
- Leistungserbringer und Stakeholder, die mit oder über die DAK-Gesundheit im Internet kommunizieren
- Personen, die sich im Zusammenhang mit DAK-relevanten Themen im Internet austauschen

Grundsätzlich können betroffene Personen jeglicher Kategorie involviert sein, sofern diese proaktiv öffentlich im Internet veröffentlichen.

Grundsätzlich gilt: Die Verarbeitung von personenbezogenen Daten und Sozialdaten ist auf das Minimum zu reduzieren.

Des Weiteren müssen alle gespeicherten Daten spätestens nach der Zusammenarbeit gelöscht werden. Die Löschung ist in einem Löschprotokoll zu protokollieren und das Löschprotokoll ist der DAK-Gesundheit zu übergeben.

5. Allgemeine Anforderungen an die IT-Sicherheit und Informationssicherheit

Der Bieter/Auftragnehmer hat angemessene und geeignete technische und organisatorische Maßnahmen zu ergreifen (bei sich und allen eingesetzten Unterauftragnehmern), die einen unbefugten und missbräuchlichen Zugriff auf die für die Leistung eingesetzten Systeme, Anwendungen, Komponenten sowie zugehörige Daten unterbinden. Die getroffenen Maßnahmen müssen dabei dem jeweils aktuell gültigen Stand der Technik entsprechen.

Sicherheitskonzepte und Nachweise
Folgende Unterlagen sind, soweit für den Ausschreibungsgegenstand relevant, mit dem Angebot einzureichen:

- Das ISMS des Bieters/Auftragnehmers muss über eine gültige Zertifizierung nach ISO/IEC 27001:2022 verfügen.
- Sicherheitskonzept des Bieters/Auftragnehmers (TOMs): Der Bericht über die letzte Überprüfung der TOMs ist ebenfalls einzureichen und darf zum Zeitpunkt der Angebotsabgabe nicht älter als 24 Monate sein.
- Verzeichnis zu Standorten der Geschäftsräume des Bieters/Auftragnehmers
- Übersicht der Unterauftragnehmer
- Ansprechpartner für die Informationssicherheit und den Datenschutz
- Löschkonzept

Wird in den TOMs auf weitere Konzepte oder ähnliche Dokumente verwiesen, sind diese ebenfalls mit dem Angebot einzureichen. Dazu gehören in der Regel:

- Rollen- und Rechte-Konzept
- Konzept zum Patch- und Update-Management
- Konzept zum Schwachstellenmanagement
- Notfall- und BCM-Konzept inklusive Incident Response und Angriffserkennung
- Backupkonzept
- Konzept zur sicheren Softwareentwicklung
- Architektur- und Datenflussdiagramme
- Angaben zur physischen Sicherheit

Die vorangegangene Auflistung ist nur als Beispiel zu verstehen. Die enthaltenen Themengebiete können auch direkt innerhalb des Sicherheitskonzeptes beschrieben sein. Richtlinien, z. B. zum Umgang mit Kennwörtern, Lieferanten oder Verschlüsselung, können bei Bedarf angefordert werden.
Die Architektur- und Datenflussdiagramme müssen eine Prüfung ermöglichen, ob die dargestellten Sicherheitsmaßnahmen zur technischen Ausgestaltung der Leistung passen.
Die Auftraggeberin wird im Rahmen der Angebotswertung die vom Bieter/Auftragnehmer eingereichten Unterlagen betreffend der Informationssicherheit prüfen. Bei Unklarheiten werden gegebenenfalls weitere Unterlagen nachgefordert oder es wird um ein klärendes Gespräch gebeten.
Die positive Feststellung der Erfüllung der für die Leistung geltenden Anforderungen an die Informationssicherheit ist Voraussetzung für die Zuschlagserteilung.

Hosting und Rechenzentren
Der Bieter/Auftragnehmer bestätigt gegenüber der Auftraggeberin, dass alle Server des Bieters/Auftragnehmers und aller für die Leistung eingesetzten Subdienstleister ausschließlich innerhalb der EU/EWR oder der Schweiz betrieben werden. Diese Anforderung gilt auch für Cloud-Dienste.
Der Zugriff durch Staaten außerhalb der EU/EWR oder der Schweiz ist der Auftraggeberin unverzüglich mitzuteilen und von ihr zu genehmigen.

Der Wechsel des Standortes aller für die Leistungserbringung eingesetzten Server des Bieters/Auftragnehmers und aller Unterauftragnehmer ist der Auftraggeberin unverzüglich mitzuteilen und von ihr zu genehmigen.
Die eingesetzten Rechenzentren müssen über eine gültige Zertifizierung nach ISO/IEC 27001:2022 verfügen. Der Bieter/Auftragnehmer hat die entsprechende Zertifizierung der Auftraggeberin nachzuweisen.
Administrative Zugriffsberechtigungen für den Betrieb der bereitgestellten Systeme sind regelmäßig durch den Bieter/Auftragnehmer zu überprüfen und auf das für die Aufgabenerfüllung erforderliche Maß zu beschränken.

Zugriffskontrolle
Zugangsdaten sind bei der Übertragung zu verschlüsseln und durch geeignete, dem Stand der Technik entsprechende kryptografische Verfahren zu schützen. Kennwörter dürfen nicht im Klartext oder in reversibel verschlüsselter Form gespeichert werden.
Der Bieter/Auftragnehmer hat geeignete technische Maßnahmen zur Durchsetzung einer angemessenen Kennwortgüte (Länge von mindestens 12 Zeichen, Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen) einzusetzen.
Falls das System den erzwungenen Passwortwechsel bei der Erstanmeldung unterstützt, muss dieser aktiviert werden. Besteht diese Möglichkeit nicht, muss der Anwender darauf hingewiesen werden, dass das Initialpasswort geändert werden muss. Initialpasswörter dürfen höchstens 14 Kalendertage gültig sein
Die Nutzung einer Mehr-Faktor-Authentisierung muss, soweit möglich, unterstützt werden. Abweichungen von dieser Vorgabe müssen technisch und organisatorisch von der Auftraggeberin geprüft werden.
Bei Abweichungen von diesen Vorgaben muss der Bieter/Auftragnehmer seine Passwortrichtlinie zur Verfügung stellen. Diese Passwortrichtlinie muss technisch und organisatorisch von der Auftraggeberin geprüft werden.

Anwendungssicherheit
Der Bieter/Auftragnehmer hat geeignete Maßnahmen zum Schutz der Anwendungen vor möglichen Bedrohungen zu treffen, die deren Vertraulichkeit, Integrität oder Verfügbarkeit beeinträchtigen können. Hierbei sind anerkannte Standards (z. B. OWASP Top 10) und Sicherheitsempfehlungen, insbesondere des BSI, angemessen zu berücksichtigen.

Systemtrennung
Produktions-, Test- und Entwicklungsumgebungen müssen, falls vorhanden, angemessen voneinander getrennt werden. Für die jeweiligen Umgebungen sind getrennte Benutzer- und Administrationskonten zu verwenden. Produktivdaten sollten nicht in Test- oder Entwicklungsumgebungen verwendet werden.

Mandantentrennung
Der Bieter/Auftragnehmer muss eine wirksame Trennung der Daten und Berechtigungen der Auftraggeberin von denen anderer Mandanten sicherstellen. Ein Zugriff anderer Mandanten auf Daten oder Funktionen der Auftraggeberin ist auszuschließen.

Angriffserkennung und Schutz vor Schadsoftware
Sicherheitsrelevante Ereignisse müssen protokolliert und überwacht werden. Der Bieter/Auftragnehmer betreibt Angriffserkennungssysteme nach dem Stand der Technik, um Sicherheitsvorfälle so früh wie möglich erkennen zu können und dann entsprechend zu handeln. Auf Anforderung muss der Bieter/Auftragnehmer Logdateien mit Alarmen für Entitäten der Auftraggeberin an einer definierten Schnittstelle zur Verfügung stellen.
Der Bieter/Auftragnehmer gewährleistet, dass alle für die Leistung eingesetzten Systeme und Anwendungen durch geeignete technische und organisatorische Maßnahmen vor Schadsoftware geschützt werden.

Patch- und Schwachstellen-Management

Der Bieter/Auftragnehmer muss über einen Patch-Management-Prozess gewährleisten, dass alle von ihm eingesetzten Systeme, Systemkomponenten und Entwicklungswerkzeuge auf einem stabilen und sicheren Versionsstand sind.
Insbesondere stellt der Bieter/Auftragnehmer das Einspielen empfohlener Patches je nach Risiko für die Anwendung sicher. Es dürfen nur IT-Systeme und Komponenten eingesetzt werden, für die Sicherheitsupdates vom Hersteller bereitgestellt werden.
Schwachstellen, die als kritisch eingestuft sind (CVSS-Score ≥ 9,0) oder bereits aktiv ausgenutzt werden, müssen unverzüglich, spätestens jedoch innerhalb von 72 Stunden, geschlossen werden.
Schwachstellen mit einem CVSS-Score von mindestens 7,0 und unter 9,0 müssen spätestens innerhalb von 30 Tagen geschlossen werden.
Zusätzlich sind die eingesetzten IT-Systeme und Komponenten regelmäßig und anlassbezogen auf Schwachstellen zu überprüfen. Der Bieter/Auftragnehmer informiert die Auftraggeberin über eventuelle Risiken.

Verschlüsselung / sichere Kommunikationskanäle
Sämtliche Datenübertragungen im Zusammenhang mit der bereitgestellten Leistung sind durch nach dem Stand der Technik als sicher anerkannte kryptographische Verschlüsselungsverfahren (z. B. TLS) zu verschlüsseln.
Das Server-Zertifikat muss vom Bieter/Auftragnehmer beschafft werden. Das Zertifikat muss von einer vertrauenswürdigen Zertifizierungsstelle stammen. Der Bieter/Auftragnehmer stellt die sichere Speicherung und rechtzeitige Erneuerung der zugehörigen Zertifikate und privaten Schlüssel sicher.
Daten sollten auch bei der Speicherung und bei Datensicherungen durch nach dem Stand der Technik als sicher anerkannte kryptografische Verschlüsselungsverfahren verschlüsselt werden. Sollte hiervon abgewichen werden, muss die Auftraggeberin diesem zustimmen.

Datensicherung und Wiederherstellung
Der Bieter/Auftragnehmer muss durch dem Stand der Technik entsprechende Datensicherungs- und Wiederherstellungsverfahren (3-2-1 Regel für Backups) sicherstellen, dass die für die Leistung erforderlichen Daten und Systeme nach Störungen, Ausfällen und Informationssicherheitsvorfällen wiederhergestellt werden können.
Datensicherungen von geänderten Daten sind mindestens täglich durchzuführen. Die letzte Vollsicherung darf nicht länger als 30 Tage zurückliegen. Die Sicherungskopien sind angemessen von den Produktivsystemen zu trennen und vor unberechtigtem Zugriff, Veränderung und Löschung zu schützen.
Die Wiederherstellbarkeit der Daten, Programme und Systeme muss regelmäßig, mindestens einmal jährlich, durch geeignete Wiederherstellungstests überprüft werden. Die Durchführung und die Ergebnisse der Wiederherstellungstests müssen dokumentiert und auf Anforderung der Auftraggeberin bereitgestellt werden.

Penetrationstests
Der Bieter/Auftragnehmer stellt die Sicherheit der für die Leistung bereitgestellten Anwendungen durch jährliche Penetrationstests sicher.
Die Durchführung und Berichte der Penetrationstests sind der Auftraggeberin auf Anforderung nachzuweisen.

Informationssicherheitsvorfälle
Informationssicherheitsvorfälle, die direkt oder indirekt den vom Bieter/Auftragnehmer für die Auftraggeberin bereitgestellten Leistung betreffen, meldet der Bieter/Auftragnehmer der Auftraggeberin unverzüglich. Reaktionen auf diese Vorfälle werden der Auftraggeberin unverzüglich mitgeteilt und ggf. abgestimmt.

Unterauftragnehmer

Finden wesentliche Teile der Leistungserbringung bei weiteren Unterauftragnehmer statt, sind auch dort die für die Leistung geltenden Anforderungen an die Informationssicherheit zu beachten.
Die relevanten Dokumente der weiteren Unterauftragnehmer sind mit einzureichen oder es ist anderweitig, z. B. durch relevante Zertifikate, zu belegen, dass dort ein ausreichendes Sicherheitsniveau vorliegt.

Audit
Die Auftraggeberin behält sich das Recht vor, die Umsetzung und Einhaltung der Maßnahmen und Prozesse zur Gewährleistung der Informationssicherheit im Rahmen eines Audits zu überprüfen.
Im Rahmen des Audits kann die Auftraggeberin insbesondere Folgendes prüfen:

- die eingereichten Sicherheitskonzepte und Nachweise
- die Einhaltung der vereinbarten Sicherheitsmaßnahmen, z. B. durch ein Vor-Ort-Audit
- die Architektur von technischen Bestandteilen hinsichtlich erforderlicher und vorhandener Schutzmechanismen (Threat Modeling)

Die Auftraggeberin weist darauf hin, dass sich das Audit auch auf alle Unterauftragnehmer des Bieters/Auftragnehmers erstreckt, die er für den Einsatz für datenschutz- und informationssicherheitskritische Bereiche vorsieht, z. B. Rechenzentrumsbetreiber. Der Bieter/Auftragnehmer hat dafür Sorge zu tragen, dass die Auftraggeberin auch bei diesen Unterauftragnehmern ein Audit durchführen kann.
Alternativ zu Vor-Ort-Prüfungen bei Unterauftragnehmern können auch Zertifikate von Zertifizierungsstellen gewertet werden, die vom Bundesamt für Sicherheit der Informationstechnik anerkannt sind, sofern der Geltungsbereich des Zertifikats die Systeme, Technologien und Prozesse des Auftragsgegenstandes einschließt. Die bei der Zertifizierung verwendete Prüfnorm muss sich am BSI-Grundschutz oder ähnlichen Normen orientieren.
Die Auftraggeberin behält sich vor, ein entsprechendes Audit jährlich durchzuführen.
Durch das Audit entstehende Aufwände beim Bieter/Auftragnehmer werden durch die Auftraggeberin nicht vergütet.