ARD ZDF Deutschlandradio

BEITRAGSSERVICE

Beschaffung: Externer Sachverständiger

1. Kontaktadresse

Sollten Sie Interesse haben, an der Beschaffung „Externer Sachverständiger“ teilzunehmen, wenden Sie sich bitte mit Ihren Kontaktdaten (Name und Anschrift des Unternehmens, Ansprechpartner inkl. E-Mail-Adresse und Telefonnummer) bis spätestens zum

24.10.2024

an die nachfolgend angegebene Kontaktadresse.

Per E-Mail an:

beschaffungsportal@beitragsservice.de

Wir weisen darauf hin, dass kein Anspruch auf Beteiligung am späteren Wettbewerbsverfahren besteht. Sie erhalten lediglich im Falle einer Berücksichtigung eine Aufforderung zur Angebotsabgabe vom Beitragsservice von ARD, ZDF und Deutschlandradio (im Folgenden „Beitragsservice“).

Im vorliegenden Stadium geht es um eine I**nteressensbekundung** an einem späteren Wettbewerbsverfahren. **Es sind noch keine Angebote einzureichen**. **Auch Rückfragen zum Gegenstand der Beschaffung können erst im Rahmen der nachfolgenden Angebotsaufforderung gestellt werden.**

ARD ZDF Deutschlandradio

BEITRAGSSERVICE

Leistungsbeschreibung

Externer Sachverständiger

INTERNETAUFTRITT

1. Einleitung & Zielsetzung

Der Beitragsservice von ARD, ZDF und Deutschlandradio (nachfolgend Beitragsservice) führt als nicht rechtsfähige öffentlich-rechtliche Verwaltungsgemeinschaft für die in der Arbeitsgemeinschaft der öffentlich-rechtlichen Rundfunkanstalten der Bundesrepublik Deutschland (ARD) zusammengeschlossenen Landesrundfunkanstalten, das Zweite Deutsche Fernsehen (ZDF) und Deutschlandradio den Einzug des Rundfunkbeitrags durch.

In diesem Kontext werden rund 46,1 Millionen Beitragskonten (von natürlichen wie auch juristischen Personen) verwaltet. Der Beitragsservice steht dabei im Dialog mit den (potentiellen) Beitragskontoinhabern, um deren Daten und Anliegen entgegenzunehmen und eine effiziente Bearbeitung sicher zu stellen.

Der Beitragsservice ist aktuell dabei seinen kompletten Internetauftritt www.rundfunkbeitrag.de an den externen Dienstleister Queo auszulagern, welcher den Internetauftritt zukünftig sowohl betreiben als auch in Zusammenarbeit mit dem Beitragsservice weiterentwickeln wird.

Die Strategie des Beitragsservice sieht vor, die Kommunikation mit den Beitragszahlern und anderen Interessierten („Beitragszahlerkontakte“) in deutlich höherem Umfang digital (über den Internetauftritt) zu führen. Zukünftig soll der Internetauftritt rundfunkbeitrag.de den wichtigsten Kanal für den Beitragszahlerkontakt und damit die zentrale Schnittstelle zu den Beitragszahlern darstellen.

Die von Queo für den Managed Service Internetauftritt zu erbringende Leistung umfasst:

- Übernahme des gesamten Internetauftritts (Betriebsverantwortung) insbesondere
    - **Webprogrammierung von Online-Services**
    - CMS
    - Webanalyse
    - Suchfunktion
    - Betrieb
    - Sicherstellung von Informationssicherheit und Datenschutz
- sowie die Transformation zu einem modernen und zeitgemäßen Internetauftritt bezüglich
    - Entwicklung und Umsetzung einer neuen Architektur
    - Funktionale Weiterentwicklung des Internetauftritts
    - Nicht-funktionale und teils Funktionale Tests

Das bereitzustellende System muss insgesamt hohen Anforderungen an die Sicherheit, Verfügbarkeit und Compliance gerecht werden. Um die Verfügbarkeit des Internetauftritts auch im Falle eines Ausfalls von Queo sicherstellen zu können, erfolgt das Hosting nicht bei Queo selbst, sondern bei dessen Unterauftragnehmer (einem in Deutschland ansässigen Hostingdienstleister).

Im Rahmen des Relaunches wird Queo folgende Komponenten implementieren:

- **CMS: Neos**
- **Online Services: Symfony**
- **Suchfunktion: Elastic Search**
- **Webanalyse: Matomo**
- **Authentication Provider mit OIDC**
- **Anbindung der Open API Schnittstelle des Beitragsservice**

Um sicherzustellen, dass Queo die mit dem Beitragsservice vereinbarten wesentlichen Anforderungen erfüllt, beabsichtigt der Beitragsservice einen Dienstleister zu beauftragen, der die vorgenannten Anforderungen überprüft (nachfolgend Auftragnehmer bzw. externer Sachverständiger).

2. Gegenstand der Beschaffung

2.1 Rahmenbedingungen

Der Beitragsservice sucht einen externen Sachverständigen, der den Beitragsservice bei der Abnahme des Internetauftritts gegenüber Queo mit Prüfdienstleistungen unterstützt (Zeitfenster ca. 2 Wochen vor der Abnahme, zeitnahe Erstellung eines vorläufigen Prüfberichts) und mit bedarfsbezogenen Prüfdienstleistungen (mindestens einmal jährlich) die Arbeit des Generalunternehmers Queo evaluiert. Die Form der Überprüfung ist nachfolgend im Dokument Audit genannt.

Neben dem Audit im Rahmen der Abnahme des Internetauftritts und den bedarfsbezogenen Audits können konkrete Fragestellungen aufkommen, bei denen eine Beratung oder Beantwortung sinnvoll sein könnte. Dies kann beispielsweise die Bitte einer Einordnung sein, wie wichtig ein spezielles Sicherheitsupdate tatsächlich ist oder ob es Anregungen gibt, wie mit technischen oder organisatorischen Maßnahmen Risiken minimiert werden könnten.

2.2 Auditplanungen

Der Beitragsservice und Queo stellen Informationen über alle seit dem letzten Audit vorgenommenen Änderungen und Neuerungen des Internetauftritts zur Verfügung. Der Beitragsservice gibt darüber hinaus an, welchen Aufwand in PT der Auftragnehmer für die Durchführung der Prüfung kalkulieren darf.

Auf Grundlage dieser Vorgaben soll der Auftragnehmer einen fundierten Audit-Vorschlag unterbreiten, der die zu prüfenden Bereiche und deren Umfang umfasst. Der Beitragsservice behält sich dabei jederzeit das Recht vor, den Inhalt und Umfang des Audit-Vorschlags anzupassen.

2.3 Prüfungsleistung

Der Auftragnehmer hat im Rahmen des Audits zur Abnahme des Internetauftritts sowie der bedarfsbezogenen Audits, die folgenden Aspekte zu überprüfen und einen Ergebnisbericht zu erstellen:

- **Datenschutz,**
- **Informationssicherheit,**
- **Architektur.**

Die Auditsprache, die Ergebnisberichte sowie die Unterlagen sind in deutscher Sprache zu verfassen. Der Auftragnehmer ist verantwortlich für die Koordination der einzelnen Experten und die Überwachung der Einhaltung des vorher vereinbarten Budgets. Die zu prüfenden Themen werden je nach vorheriger Vereinbarung in unterschiedlicher Tiefe behandelt und umfassen beispielhaft:

<u>Architektur</u>

- **Skalierbarkeit,**
- **Portabilität,**
- **Nachvollziehbare Dokumentation,**

- **Nutzung marktgängiger Komponenten,**
- **Hosting durch externen Hosting-Anbieter,**
- **Austauschbarkeit von Komponenten,**
- **Integrierbarkeit neuer Technologien,**
- **Effiziente Weiterentwicklung.**

Informationssicherheit

- **Maßnahmen zur Gewährleistung der Vertraulichkeit (z.B. Kryptografie),**
- **Maßnahmen zur Gewährleistung eines störungsfreien Betriebs (z.B. Backup/Recovery-Verfahren),**
- **Umsetzung der implementierten Maßnahmen zur Behandlung identifizierter Risiken,**
- **Identifizierung unbekannter Schwachstellen (z.B. Penetrationstests),**
- **Behandlung bekannter Schwachstellen (z.B. Schwachstellenmanagement).**

Datenschutz

- **AVV-Vereinbarungen mit Unterauftragnehmern von Queo,**
- **Ort der Verarbeitung (EU-Staaten, sichere EU-Drittstaaten),**
- **Meldewege bei Datenschutzverletzungen,**
- **Webanalyse-Tool,**
- **Prüfung von technischen und organisatorischen Maßnahmen (TOM),**
- **Prüfung des Datenschutzkonzepts oder einzelner Komponenten.**

Aufgrund der Komplexität und des zur Verfügung stehenden Tageskontingents sind risikobasiert in Abstimmung mit dem Beitragsservice Prüfungsschwerpunkte festzulegen. Hierbei sind insbesondere Risiken für den Beitragsservice sowie für die Daten der Beitragszahlenden zu berücksichtigen.

Der Prüfungsplan wird hierzu vorab vom Auftragnehmer inkl. des geplanten Aufwands pro Prüfungsgebiet erstellt und muss vom Beitragsservice bestätigt werden.

Die Prüfungen sollen - nach vorheriger Abstimmung mit dem Beitragsservice - grundsätzlich erfolgen z.B. in Form von

- **Interviews,**
- **Dokumentenreviews,**
- **Code- bzw. Datenanalysen.**

Die Leistung ist remote zu erbringen. Prüfungen vor Ort sind nicht vorgesehen.

Der Auftragnehmer erhält auf Anforderung Einblick und Zugang zu allen in diesem Zusammenhang erforderlichen Informationen, die er benötigt, um ihn bei der Prüfung zu unterstützen. Dazu gehören zum Beispiel:

- **Dokumentationen der Architektur, Sicherheitsmechanismen, datenschutzrelevante Dokumentationen und Prozessbeschreibungen,**
- **Einblick in die relevanten Vertragsabschnitte mit Unterauftragnehmern bezüglich Datenschutz, Informationssicherheit, technische und organisatorische Maßnahmen (TOM) und deren Standorte bzw. Orte der Datenverarbeitung,**
- **Sourcecode, Konfigurationen und Software-Versionen,**
- **Betriebsverfahren wie beispielsweise Changemanagement, Schwachstellenmanagement, Malwareschutz, Backup und Restore, Protokollierung, Monitoring, usw.**

2.4 Prüfbericht

Nach jeder durchgeführten Prüfung erstellt der Auftragnehmer einen Prüfbericht. Zunächst wird ein kurzfristig zu erstellender Vorabbericht mit den wichtigsten Ergebnissen erstellt. Anschließend folgt ein ausführlicher Abschlussbericht, der alle Feststellungen detailliert dokumentiert.

Beide Prüfberichte müssen dabei die folgenden Inhalte enthalten:

- **Kurze Erläuterung zum Vorgehen der Prüfung,**
- **Ergebnisse**
  - **Nachvollziehbare Beschreibung,**
  - **Einordnung in Schweregrad bzw. damit verbundenes Problem/Risiko,**
  - **Praktikabler Lösungsansatz zur Behebung,**
- **Ggf. Empfehlungen für zukünftige Prüfungen,**
- **Fazit.**

Der externe Sachverständige wird den Prüfbericht gemeinsam mit Queo und dem Beitragsservice besprechen. Der Beitragsservice behält die Entscheidungskompetenz darüber, welche Maßnahmen von Queo umgesetzt werden und welche nicht.

3. Bewertungskriterien

3.1 Qualifizierungsanforderungen / Muss-Anforderungen

Die nachstehend aufgeführten Qualifizierungsanforderungen müssen vollständig erfüllt werden. Diese Anforderungen sind Muss-Kriterien, deren Einhaltung der Auftragnehmer im Fall einer Auftragserteilung jederzeit gegenüber dem Beitragsservice sicherstellen muss.

Der Auftragnehmer verfügt oder hat Zugriff auf Profile (zum Beispiel auch über Unterauftragnehmer), mit folgender Qualifikation:

- **Volljurist/in, Diplom-Jurist/in oder Wirtschaftsjurist/in, welche/r im Schwerpunkt im Bereich Datenschutz tätig ist und über mindestens 3 Jahre Berufserfahrung in diesem Rechtsgebiet verfügt,**
- **Penetrationstester/in mit dem Schwerpunkt Internet und mit mindestens 3 Jahren einschlägiger Berufserfahrung,**
- **Mitarbeiter/in mit dem Schwerpunkt Informationssicherheit und mit mindestens 3 Jahren einschlägiger Berufserfahrung.**

Bei einer Bewerbung ist in jeder Qualifikation ein entsprechendes Profil abzugeben, das die zuvor genannten Muss-Anforderungen abdeckt. Die Profile sind dabei wie folgt aufzubauen:

- **Aktuelle Berufsbezeichnung und Schwerpunkt,**
- **Erläuterungen zur einschlägigen Qualifizierung (Datenschutz, Penetrationtests und Informationssicherheit) inklusive entsprechender einschlägiger Ausbildungsnachweise und Zertifizierungen,**

- **Darstellung der einschlägigen Projekterfahrung in den letzten 5 bis 10 Jahren und insbesondere nachvollziehbarer Angaben dazu, in welchem Zeitraum der jeweilige Mitarbeiter bzw. die jeweilige Mitarbeiterin das Projekt unterstützt hat und mit welchen Aufgaben bzw. Tätigkeit.**

Die angegebenen Profile müssen immer vergleichbar zu den später eingesetzten Mitarbeiter(n)/innen sein (gleichwertiges Qualifikationsniveau). Eine niedrigere Qualifikation darf nicht eingesetzt werden.

Referenzen

Der Auftragnehmer stellt drei Referenzen zu Kunden-Projekten bereit, deren Geschäftsbeziehung mit dem Auftragnehmer nicht älter als fünf Jahre ist. Die folgenden Kriterien müssen durch diese Referenzen abgedeckt werden:

- **Mindestens ein Kunde war eine öffentlich-rechtliche Institution,**
- **Jedes Kunden-Projekt betraf eine Prüfungsleistung im Zusammenhang mit Anwendungen in öffentlichen Netzen,**
- **Die drei Referenzen müssen insgesamt mindestens folgende Prüfungen abdecken:**
  - **Einmal die Prüfung im Kontext Datenschutz,**
  - **Einmal die Prüfung im Kontext Penetrationstest,**
  - **Einmal die Prüfung im Kontext Informationssicherheit.**

  Nicht jede Referenz muss alle drei Prüfungsgebiete umfassen. Es ist ausreichend, wenn die drei Referenzen gemeinsam alle Prüfungsgebiete abdecken.

Zu den Referenzen sind - sofern möglich - noch die folgenden Angaben zur Verfügung zu stellen:

- **Kontaktangaben zu einem Ansprechpartner, der ggf. bei Bedarf kontaktiert werden könnte,**
- **Beschreibung des Prüfauftrags,**
- **Umfang des Prüfungsauftrags, insbes.**
  - **Zeitumfang,**
  - **Abgedeckte Themen,**
  - **Prüftiefe.**

3. 2 Qualifizierungsanforderungen / KANN-Anforderungen

Die nachstehend aufgeführten Anforderungen sollen erfüllt werden. Es handelt sich um Kann-Kriterien, deren Einhaltung im Rahmen einer vergleichenden Bewertung berücksichtigt wird.

Dabei werden zur Bewertung der Qualifizierung insgesamt 260 Punkte vergeben. Jedes Kriterium erhält eine Gewichtungspunktzahl. Die Gewichtungspunktzahl drückt aus, wie wichtig das Kriterium für den Beitragsservice ist (0 = absolut unwichtig; 10 = absolut wichtig). Für jedes Kriterium können maximal 10 Punkte vergeben werden. Dabei sieht die Gewichtung wie folgt aus:

- **Gewichtung 8 bei dem Kriterium „Qualifikation der eingereichten Profile“**
- **Gewichtung 10 bei dem Kriterium „Prüfauftragsähnlichkeit bzgl. der eingereichten Referenzen“**
- **Gewichtung 4 bei Kriterium „anonymisierten Auditplan als Arbeitsprobe“**
- **Gewichtung 4 bei Kriterium „vom Auftragnehmer genutztes Template für Prüfergebnisse oder einen anonymisierten Audit-Bericht“**

Kriterium Qualifikation der erforderlichen Profile

Für dieses Kriterium können maximal 80 Punkte erreicht werden (10 Punkte x Gewichtung 8 = 80 Punkte).

- **wenn der Schwerpunkt der Tätigkeit eindeutig in der Prüfung der Spezialisierung (Datenschutz, Informationssicherheit, Penetrationtest) liegt**
- **einschlägige und als hochwertig anzusehende Zertifikate oder Ausbildungsnachweise in der jeweiligen Spezialisierung vorliegen. Ein Zertifikat oder Ausbildungsnachweis wird dann als hochwertig angesehen, wenn es eine Fortbildung/Ausbildung von mindestens fünf PT beinhaltet sowie einen bestandenen Abschlusstest**

Kriterium Referenzenähnlichkeit

Für dieses Kriterium können maximal 100 Punkte erzielt werden (10 Punkte x Gewichtung 10 = 100 Punkte), sofern

- **der Prüfauftrag vergleichbar ist**
- **und die Prüftiefe und der Umfang vergleichbar sind**

Kritierium Auditplan

Für die Vorlage eines anonymisierten Audit-Plans, der Aufschluss darüber gibt, wie der Auftragnehmer Audits plant, durchführt und koordiniert können maximal 40 Punkte (10 Punkte x Gewichtung 4 = 40 Punkte) erzielt werden.

Kriterium Audit-Bericht/Template

Für die Vorlage eines anonymisierten Audit-Berichts oder entsprechenden Templates, welches Aufschluss darüber gibt, wie der Auftragnehmer Prüfergebnisse für den Kunden dokumentiert bzw. aufbereitet, können 40 Punkte (10 Punkte x Gewichtung 4 = 40 Punkte) erzielt werden.

3.3 Einsatz von Unterauftragnehmern zur Erfüllung der Qualifizierungsanforderungen

Sofern und soweit der Auftragnehmer nicht über eigene Mitarbeiter/innen mit den geforderten Qualifizierungen verfügt, kann er zur Leistungserbringung auch Unterauftragnehmer einbinden, sofern deren Mitarbeiter/innen die geforderten Qualifikationen besitzen.

4. Auftragsvolumen

Der Beitragsservice beabsichtigt einen Abrufauftrag ohne Abnahmeverpflichtung mit einem maximalen Auftragsvolumen von 150 Personentage (PT) zu vergeben.

Bei der Kalkulation des Tagessatzes ist ein Mischpreis anzugeben, der sich auf alle eingesetzten Rollen und Skills bezieht. Unterschiedliche Tagessätze je Rolle sind nicht vorgesehen.

Die Leistung ist remote zu erbringen.

Im ersten Vertragsjahr soll aufgrund der Betriebsübernahme durch Queo eine initiale Prüfung durchgeführt werden (voraussichtlich im ersten Halbjahr 2025). In den Folgejahren ist mit bedarfsbezogenen Prüfungen (mindestens einmal jährlich) zu rechnen. Die Vorlaufzeit beträgt mindestens sechs Wochen.

5. VERTRAGSLAUFZEIT/VERLÄNGERUNGSOPTION

Es ist beabsichtigt, mit dem wirtschaftlichsten Bieter einen Vertrag mit einer Laufzeit von 3 Jahren ab dem 01.01.2025 abzuschließen. Darüber hinaus behält sich der Beitragsservice die Option vor, den Auftrag einmalig um ein Jahr zu gleichen Konditionen zu verlängern. Es handelt sich um eine reine Laufzeitverlängerung ohne Erhöhung der PT.