

Bewertungsmatrix Gästekarte / Gästebeitrag

Zuschlagskriterien	Gewichtung	max. Punkte	Bewertungspunkte	Bewertung	Auswertung
Leistungsportfolio gemäß Ausschreibung					
2.1 Funktionaler Umfang und Prozessqualität	25,0%	1000 Punkte	1000 Punkte	0 Punkte	0 Punkte
2.1.1 Projektsetup, Konzeption und Umsetzung bis Go-live	2,5%	100 Punkte	100 Punkte		0 Punkte
2.1.2 Aufbereitung Nutzergruppen, Rollen- und Rechtekonzept (inkl. Protokollierung)	2,5%	100 Punkte	100 Punkte		0 Punkte
2.1.3 Gästeregistrierung / Datenerfassung (betriebs- und/oder gastseitig)	5,0%	200 Punkte	200 Punkte		0 Punkte
2.1.4 Abrechnung, Nachweise, Exporte (Betriebe an die Stadt)	5,0%	200 Punkte	200 Punkte		0 Punkte
2.1.5 Schnittstellen & Integration	2,5%	100 Punkte	100 Punkte		0 Punkte
2.1.6 Reporting/Controlling (Pflichtreports und Erweiterungsoption Dashboard)	2,5%	100 Punkte	100 Punkte		0 Punkte
2.1.7 Betrieb, Support, Schulungen, Einführungssupport	2,5%	100 Punkte	100 Punkte		0 Punkte
2.1.8 Gästekarte – Ausgabe, Nachweis, Prüfung	2,5%	100 Punkte	100 Punkte		0 Punkte
2.2 Datenschutz und IT-Sicherheit	7,5%	134 Punkte	300 Punkte		0 Punkte
2.3 Technischen Anforderungen (Systemintegration und Umsetzung)	7,5%	270 Punkte	300 Punkte		0 Punkte
Preis	30,0%	1200 Punkte	1200 Punkte		0 Punkte
Bieterpräsentation	30,0%	1200 Punkte	1200 Punkte		0 Punkte
Summe	100%	3804 Punkte	4000 Punkte		0 Punkte

Hinweis: Zur Bieterpräsentation werden nur die Bieter eingeladen, die nach Auswertung der weiteren Kriterien noch rechnerische Chancen auf den Zuschlag haben.



2.2 Zuschlagskriterien & Bewertungsmatrix

Den Zuschlag erhält das wirtschaftlichste Angebot gemäß § 43 UVgO.

Die Bewertung erfolgt auf Grundlage der nachfolgenden Kriterien und Gewichtungen:

- **Leistungsportfolio gemäß Ausschreibung: 40 %**
 - **Funktionaler Umfang und Prozessqualität: 25 % (max. 1000 Punkte)**
Die Bepunktung entspricht der untenstehenden Bewertung. Näheres ist unten ersichtlich.
 - **Systemintegration und Umsetzung sowie Anforderungen an Datenschutz und IT-Sicherheit: 15 % (max. 600 Punkte)**
Die Bepunktung wird aus den Zusatz-Dokumenten übernommen, hochgerechnet und jeweils zur Hälfte gewichtet. Näheres kann der Beschreibung der Zusatz-Dokumente entnommen werden.
- **Preis: 30 % (max. 1200 Punkte)**
Das niedrigste Angebot erhält die volle Punktzahl (1200 Punkte). Das fiktiv doppelt-niedrigste Angebot erhält 0 Punkte, dazwischen wird linear interpoliert.
- **Bieterpräsentation: 30 % (max. 1200 Punkte)**
Die Bepunktung richtet sich nach dem Ergebnis der Bieterpräsentation. Näheres kann der Beschreibung zur Bieterpräsentation entnommen werden.

Das wirtschaftlichste Angebot ergibt sich aus der gewichteten Gesamtbewertung aller Kriterien.



3. Leistungsbeschreibung

Gegenstand der Vergabe ist die Bereitstellung eines digitalen Systems zur rechts- und revisions-sicheren Erhebung und Abrechnung des Gästebeitrags in der Stadt Koblenz inkl. Betrieb und Support. Das System soll die Betriebe bei der Umsetzung entlasten und zugleich dem Gast einen Mehrwert (digitale / analoge Gästekarte, optional digitaler Reisebegleiter) bieten.

Die Leistung umfasst insbesondere:

- Einrichtung/Umsetzung der Beitragslogik (gemäß Satzung/Regelwerk der Stadt Koblenz),
- digitale Gästeregistrierung (betriebsseitig mit der Option eines Pre-Check-Ins) inkl. druckfähige Vorlage analoge Gästeregistrierung
- Ausgabe einer (digitalen) Gästekarte,
- Abrechnung, Reporting, Exporte und (mindestens) standardisierte Übergaben an die städtische Finanzbuchhaltung,
- Schnittstellen zu gängigen Gastgeber-/PMS-Systemen,
- Betrieb (SaaS) inkl. Updates, Monitoring, Datensicherung sowie Support/Onboarding.

Der aufgeführte Pflichtumfang muss vollständig angeboten werden. Optionen sind anzugeben, aber nicht zu bepreisen, da sie von der Stadt Koblenz im Rahmen dieses Auftrags nicht beauftragt werden.

Hinweis zur Meldelogik: Das System muss die für den Gästebeitrag erforderlichen Daten unabhängig davon verarbeiten können, ob melderechtliche „Meldeschein“-Pflichten im Einzelfall bestehen oder nicht bestehen. Empfehlungen aus Erfahrungswerten sind bei der Angebotserstellung bitte zu begründen.

Die Antworten zur Lösung der geforderten Punkte 3.1 und 3.2 (Lösungskonzept) sind formfrei darzustellen. Für den Punkt 3.3 und 4 sind die Anlagen auszufüllen.

3.1 Pflichtumfang

Die untenstehenden Anforderungen sind mit einer maximalen Punktzahl versehen. Die Anforderungen des Pflichtumfangs werden wie folgt bewertet:

100% = Sehr gute, leicht verständliche, äußerst überzeugende Darstellung; sehr gute Benutzeroberfläche, Umsetzung aller gewünschten Punkte

75% = Überzeugende Darstellung, Gute Benutzeroberfläche, nur einige ergonomische und fachlich/technische Schwächen erkennbar.

50% = Darstellung der Leistungen überzeugte überwiegend, Benutzeroberfläche nicht sehr ergonomisch, fachlich/technische Schwächen.

25% = Darstellung der Leistungen überzeugte nur zum Teil, Benutzeroberfläche komplex und unübersichtlich, ungewohnte Bedienung, hohe fachlich/technische Schwächen.



0% = Darstellung überzeugte nicht; Benutzeroberfläche schwer verständlich, fachlich/technische Funktionen nicht umgesetzt bzw. fehlen.

3.1.1 Projektsetup, Konzeption und Umsetzung bis Go-live (**max. 100 Punkte**)

Das System muss bis zum Go-live Ende Q4/2026 (spätestens 01.01.2027) produktiv einsatzbereit sein. Eine saubere Projektstruktur (Meilensteine, Tests, Abnahmen) reduziert Einführungsrisiken und sichert, dass Betriebe und Verwaltung rechtzeitig arbeitsfähig sind.

Zu den angebotenen Leistungen müssen gehören:

- Projekt-Kick-off, Projektorganisation (Rollen, Verantwortlichkeiten)
- detaillierter Projektplan (inkl. Projektstart, Rollout, Schulung, Go-live, Support im Go-Live)
- Feinspezifikation/Workshopphase zur Parametrisierung des Koblenzer Regelwerks (Tarife, Befreiungen etc.)
- Testkonzept (System-, Schnittstellen- und Abnahmetests) inkl. Testfällen und Abnahmeprotokollen produktiver Systemstart inkl. Rückfall-/Notfallkonzept
- Verfahrensdokumentation, DSGVO-konformes Tracking nur mit Einwilligung

3.1.2 Aufbereitung Nutzergruppen, Rollen- und Rechtekonzept (inkl. Protokollierung) (**max. 100 Punkte**)

Das System verarbeitet beitragsrelevante und ggf. personenbezogene Daten. Ein Rollen- und Rechtekonzept stellt sicher, dass jede Stelle nur die Daten sieht/bearbeitet, die sie benötigt. Protokollierung ist wichtig für Nachvollziehbarkeit und Prüfungssicherheit.

Zu den angebotenen Leistungen müssen gehören:

- Rollen- und Rechtekonzept mindestens für: Beitragserhebende Mitarbeiter, Unterkunftsbetriebe, Gäste (Self-Service), Akzeptanzstellen (Prüfung)
- Administrationsoberfläche für Rechteverwaltung
- Protokollierung/Audit-Log für administrative Aktionen (z. B. Regelwerksänderungen, Rollenänderungen, manuelle Korrekturen)
- Berechtigungskonzept für Auswertungen/Exports (z. B. getrennte Rollen „Auswertung“ vs. „Administration“ seitens Beitragserhebende Mitarbeiter und der Koblenz Touristik)

3.1.3 Gästeregistrierung / Datenerfassung (betriebs- und/oder gastseitig) (**max. 200 Punkte**)

Die Datenerfassung ist der Startpunkt des End-to-End-Prozesses. Je einfacher und medienbruchfreier die Erfassung ist, desto höher ist die Akzeptanz bei Betrieben und Gästen und desto besser ist die Datenqualität für Abrechnung und Controlling.

Zu den angebotenen Leistungen müssen gehören:



- Erfassung der für den Gästebeitrag erforderlichen Daten (Pflichtfelder durch Stadt konfigurierbar)
- betriebsseitige Erfassung (Web-Client) inkl. Korrektur/Storno-Funktionen und Historie
- Möglichkeit einer gastseitigen Vorab-/Selbsterfassung (Pre-Check-in / Self-Service) innerhalb des Basissystems oder als im Basissystem vorhandene Funktion
- Import-/Massenupload (z. B. CSV/Excel/XML) als Alternative zu Schnittstellen
- Abbildung von Befreiungs-/Ermäßigungstatbeständen (konfigurierbar) inkl. Dokumentations-/Nachweismöglichkeit (ggf. Ergänzung Ergebnis aus Satzung / Benennung von Ausnahmen.)
- Plausibilitätsprüfungen (Pflichtfelder, Zeitraumlogik, Dubletten) und Fehlermeldungen für Anwender
- Die Software ist benutzerdefiniert anpassbar in der Schriftgröße, so dass sie auch von Menschen mit körperlicher Beeinträchtigung bedienbar ist.

Verarbeitet werden insbesondere

1. Vor- und Familienname,
2. Ggf. Anschrift,
3. An- und Abreisedatum sowie Dauer des Aufenthalts,
4. Anzahl der beitragspflichtigen Personen,
5. Art der Reise (Freizeit-/Geschäftsreise)
6. Angaben zu Befreiungs- oder Ermäßigungstatbeständen.

3.1.4 Abrechnung, Nachweise, Exporte (Betriebe an die Stadt) (max. 200 Punkte)

Eine stabile Abrechnung ist zentral für Einnahmesicherung und Prüf-/Revisionssicherheit. Betriebe brauchen klare Nachweise, die Stadt braucht konsistente Daten für Buchung und Kontrolle.

Zu den angebotenen Leistungen müssen gehören:

- Abrechnungsläufe je Betrieb (monatliche Abwicklung vorgesehen, aber Zeiträume frei definierbar)
- Online-Nachweise/Reports für Betriebe (Meldungen, Beitragssummen, Korrekturen)
- Korrekturmechanismus (Nachbuchung/Gutschrift/Storno) mit Historie
- Exportfunktionen (CSV/XLSX/PDF) für Verwaltung und Betriebe
- Offene-Posten-/Statusübersichten (gemeldet/abgerechnet/korrigiert)

3.1.5 Schnittstellen & Integration (max. 100 Punkte)

Die optimale PMS-Anbindung ist entscheidend für Betriebe; die FiBu-Übergabe ist entscheidend für den städtischen Prozess. Es muss zudem gesichert sein, dass auch Betriebe ohne Schnittstelle Meldungen vornehmen können.

Folgende Betriebsarten sind anzubinden:

- Hotels, Gasthöfe, Pensionen, Ferienwohnungen, Camping- und Wohnmobilstellplätze, Jugendherbergen und vergleichbare Einrichtungen,
- Sonstigen zur Beherbergung bestimmten Räumen (z. B. Privatzimmern, Ferienappartements, Plattform-Vermietungen) sowie



- Fahrgast- oder Flusskreuzfahrtschiffen, Sportboothäfen (Hausboote)

Zu den angebotenen Leistungen müssen gehören:

PMS / Gastgeber-IT :

- Darstellung der standardmäßig unterstützten PMS-Systeme
- mind. eine technische Importmöglichkeit (API oder strukturierter Import) zur Übernahme von Gast-/Aufenthaltsdaten
- Onboarding-Prozess für Betriebe ohne PMS-Schnittstelle (Massenupload/Manueller Prozess)

FiBu Stadt Koblenz

- standardisierter Export für Buchungs-/Abrechnungsdaten zur Weiterverarbeitung in der städtischen FiBu
- Software der Stadt Koblenz: Mach Finanzen ERP von der Mach GmbH
- Beschreibung: Formate, Beleglogik, Prüfnachweise

Option:

Export/Schnittstelle zur amtlichen Statistik (sofern möglich)
Schnittstelle zur Ticketerfassung des Verkehrsverbundes (Bewegtbild)

3.1.6 Reporting/Controlling (Pflichtreports und Erweiterungsoption Dashboard) (max. 100 Punkte)

Standardreports sind notwendig für Nachvollziehbarkeit und Steuerung. Optional kann ein Dashboard die politische/strategische Steuerung und das operative Controlling erleichtern.

Zu den angebotenen Leistungen müssen gehören:

Pflicht:

- Standardreports (Zeiträume, Betriebe, Herkunft, Beiträge, Befreiungen/Stornos)
- Filter, Export (PDF/Excel)
- Plausibilitäts-/Aufälligkeitsreports

Option:

- Dashboard (siehe 3.2 Optionen)

3.1.7 Betrieb, Support, Schulungen, Einführungssupport (max. 100 Punkte)

Betriebe benötigen in der Startphase schnelle Hilfe; die Verwaltung braucht verlässliche Betriebsprozesse. Gewünscht wird daher eine intensive Begleitung in der Startphase.

Zu den angebotenen Leistungen müssen gehören:

- Betrieb inkl. Updates/Release-Management
- Informationen zu Ticketsystem, Supportzeiten, definierte Reaktionszeiten
- Schulungs-/Onboardingkonzept für Stadt und Betriebe (Materialien, FAQ, ggf. Videos)
- Einführungssupport in der Startphase in Q1/2027 mit erweiterten Kapazitäten



- Monitoring/Verfügbarkeitskonzept und Störfallprozesse

3.1.8 Gästekarte – Ausgabe, Nachweis, Prüfung (max. 100 Punkte)

Die Gästekarte schafft Gastmehrwert und unterstützt die Akzeptanz des Gästebeitrags. Gleichzeitig muss die Karte zuverlässig ausgestellt und prüfbar sein, ohne den Betrieb zu belasten.

Zu den angebotenen Leistungen müssen gehören:

- Ausgabe einer digitalen Gästekarte mindestens als PDF/Print@Home und/oder QR-Code
- definierbare Gültigkeit (Aufenthaltszeitraum, Personenanzahl, ggf. Leistungsklassen)
- Bereitstellung einer Prüf-/Validierungsmöglichkeit (Web-Prüfseite oder App)
- optional: Wallet-Funktion (Apple/Google) als Option, sofern nicht Standard
- Dokumentation der Kartenlogik und Nachvollziehbarkeit (Zuordnung zum Aufenthalt)

Hinweis: es wird beabsichtigt, auch eine ÖPNV Nutzung anzubieten, hier soll der ÖPNV Nachweis getrennt von der Gästekarte ausgegeben werden. Ein Vorschlag zur Umsetzung ist bereits im Angebot zu benennen.

3.2 Optionale Leistungen

Zusätzlich zu den Pflichtleistungen können folgende optionale Leistungen angeboten werden. Die Inanspruchnahme erfolgt durch den Auftraggeber bedarfs-, haushalts- und budgetabhängig.

Die optionalen Leistungen sind im Angebot inhaltlich darzustellen. Soweit im Preisblatt vorgesehen, sind sie gesondert auszuweisen. Die optionalen Leistungen dürfen die Vergleichbarkeit der Pflichtleistungen nicht beeinträchtigen und sind technisch so auszugestalten, dass sie unabhängig vom Grundsystem oder in sinnvoller Erweiterung des Grundsystems realisiert werden können.

3.2.1 Erweitertes Monitoring/Controlling (Dashboard)

Über die Pflichtreports hinaus kann eine erweiterte Monitoring- und Controllinglösung angeboten werden. Ziel ist eine verbesserte operative und strategische Steuerung des Gästebeitrags, der Gästekartennutzung und – soweit umgesetzt – weiterer digitaler Module.

Zu den optionalen Leistungen gehören insbesondere:

- rollenbasierte Dashboards für Stadtverwaltung, Controlling und ggf. touristische Organisationen,
- frei definierbare Kennzahlen, Filter und Zeiträume,
- Visualisierung von Beitrags-, Übernachtungs- und Nutzungsdaten,
- Export- und Berichtsfunktionen,
- Dokumentation der Datenquellen, Aktualisierungslogik und Datenherkunft,
- anonymisierte und aggregierte Auswertungen zu Reisearten, Aufenthaltsmustern und Nutzungen in Koblenz, soweit diese datenschutzkonform erhoben werden können,



- anonymisierte und aggregierte Auswertungen zur Nutzung eines optionalen digitalen Reisebegleiters, insbesondere zu aufgerufenen Inhalten, Nutzungshäufigkeiten, Interessenclustern und digitalen Servicepfaden.

Personenbeziehbare Nutzungsanalysen sind nicht Bestandteil dieser Option, sofern hierfür keine gesonderte, wirksame Einwilligung vorliegt. Die Auswertungen sind grundsätzlich so zu gestalten, dass keine Rückschlüsse auf einzelne Personen möglich sind.

Der Bieter hat darzustellen, welche Dashboardfunktionen im Standard enthalten sind, welche anonymisierten bzw. aggregierten Analysen technisch möglich sind und welche datenschutzrechtlichen Voraussetzungen hierfür gelten.

3.2.2 Mobilitäts-/ÖPNV-Verknüpfung

Optional kann eine technische Verknüpfung des Systems mit Mobilitäts- und/oder ÖPNV-Angeboten angeboten werden. Diese Leistung ist nicht Bestandteil des verpflichtenden Grundsystems, kann jedoch als perspektivische Erweiterung vorgesehen werden.

Ziel dieser Option ist insbesondere die verbesserte Abbildung und Nachvollziehbarkeit der Nutzung von Mobilitätsangeboten im Zusammenhang mit dem Gästebeitrag und der Gästekarte.

Die Erstellung eines separaten Nachweises im Zusammenhang mit der Gästekarte (z. B. digitaler oder ausdrückbarer Nutzungsnachweis) ist Bestandteil der Pflichtleistungen und nicht Gegenstand dieser optionalen Erweiterung.

Der Bieter hat darzustellen, welche technischen Möglichkeiten zur Verknüpfung von Gästemeldung, Gästekarte und Mobilitätsnutzung bestehen und welche Voraussetzungen hierfür auf Seiten der Mobilitätspartner erforderlich sind.

Zu den optionalen Leistungen gehören insbesondere:

- Verarbeitung eines Mobilitätscodes bzw. vergleichbaren Identifikationsmerkmals, das einer Gästemeldung bzw. Gästekarte eindeutig zugeordnet werden kann,
- technische Unterstützung zur Erfassung und Auswertung von Ein- und Ausstiegspunkten oder vergleichbaren Nutzungsdaten im Mobilitätskontext, soweit diese durch die jeweiligen Mobilitätspartner bereitgestellt werden,
- Unterstützung der Nachweisführung gegenüber Verkehrsunternehmen (z. B. Nutzungshäufigkeiten, Gültigkeitszeiträume, Zuordnung zu Aufenthalten),
- Beschreibung der technischen Schnittstellen und Integrationslogik zu Mobilitäts- bzw. ÖPNV-Systemen,
- Darstellung der erforderlichen Partner- und Prozesslogik (z. B. Verkehrsverbünde, Akzeptanzstellen, Prüfmechanismen).



3.2.3 Digitaler Reisebegleiter (PWA/App) inkl. CMS

Es soll zur optimalen Gästelenkung und als Mehrwert für Gäste ein digitaler Reisebegleiter konzeptioniert werden, der die Akzeptanz für den Gästebeitrag erhöht, zusätzliche Serviceleistungen bietet und ein freiwilliges Empfehlungsmarketing / Monitoring ermöglicht (mit Einwilligung).

Zu den optionalen Leistungen gehören insbesondere:

- Konzeption & Umsetzung einer PWA/App, CMS oder CMS-Anbindung
- Schnittstelle zum Basissystem (Berechtigungs-/Kartenlogik)
- DSGVO-konformes Tracking nur mit Einwilligung

3.3 Datenschutz, IT-Sicherheit, technische Umsetzung (max. 600 Punkte)

Hinsichtlich des Datenschutzes, der IT-Sicherheit und der technischen Anforderungen (Systemintegration und Umsetzung) erfolgt die Bewertung anhand der bereitgestellten Zusatz-Dokumente. Die Zusatz-Dokumente enthalten auch KO-Kriterien. Siehe Anlagen.

4. Preisblatt/Preismodell (max. 1200 Punkte)

Das Preisblatt ist vollständig auszufüllen (siehe Anlage 03 – Preisblatt).

Neben den Preisen für die ausgeschriebenen Leistungen sind im Preisblatt zusätzlich Angaben zu Tagessätzen bzw. Stundenverrechnungssätzen für die im Projekt eingesetzten Rollen und Funktionen zu machen.

Diese Angaben dienen der Transparenz und Nachvollziehbarkeit der Kalkulation und sind unabhängig von der Preiswertung verpflichtend auszufüllen.

5. Bieterpräsentation (max. 1200 Punkte)

Die Bieterpräsentation wird in den Kalenderwochen 28 und 29 stattfinden. Das jeweilige Zeitfenster für eine Präsentation ist im Inhalt der Bieterpräsentation bereits angegeben. Zeitlich kann es sich allerdings nach gemeinsamer späterer Abstimmung auch um einen Nachmittagstermin handeln.



Anlage_SecMGMT_IDSMM-Anforderungen_CloudSaas_V0.2

Security-Management

STADTVERWALTUNG KOBLENZ

Cloud-/SaaS-Fachverfahren

Anforderungen der Informationssicherheit &
des Datenschutzes

- Leistungsbeschreibung / Lastenheft
- Zuschlagskriterien
- Gesamtbewertungsmatrix



Wichtige Informationen zu diesem Dokument

Dokumentenklasse:	Für den Dienstgebrauch
Dokumententitel:	IDSM Anforderungen Cloud-/SaaS-Fachverfahren
Verantwortliche/r Autor/in:	O. Philippsen
Dateiname:	20260226_SecMGMT_IDSM-Anforderungen_CloudSaas_V0.2
Fassung vom:	26.02.2026
Letzte Veröffentlichung:	---
Seitenzahl:	17
Versionsfreigabe:	0.2_Entwurf
Freigegeben durch:	O. Philippsen

Änderungsnachweis

Version	Datum	Status	Bearbeiter/in	Änderung/Bemerkung
0.1	25.02.2026	Entwurf	O. Philippsen	1. Entwurfsvorschlag
0.2	26.02.2026	Entwurf	O. Philippsen	Anpassungen „Drittlandübermittlung“

Impressum



Security-Management

STADTVERWALTUNG KOBLENZ

Der Oberbürgermeister

Datenschutzbeauftragter: Oliver Philippsen

Informationssicherheitsbeauftragter: Dominik Weber

Willi-Hörter-Platz 1

56068 Koblenz

☎ +49 (0)261 129-1017

✉ security.management@stadt.koblenz.de



Inhaltsverzeichnis

I.	Leistungsbeschreibung / Lastenheft.....	5
1.	Allgemeine datenschutzrechtliche Einordnung.....	5
2.	Auftragsverarbeitung gemäß Art. 28 DS-GVO.....	5
3.	Technische und organisatorische Maßnahmen (TOMs)	5
3.1.	Allgemeine Anforderungen	5
3.2.	Mindestanforderungen an die TOMs	5
3.3.	Berücksichtigung des Standes der Technik	6
4.	Zertifizierungen und Prüfungen.....	6
5.	Datenschutz- und Sicherheitsorganisation	6
6.	Unterauftragsverarbeiter	6
7.	Rollen- und Rechtekonzept.....	7
7.1.	Allgemeine Anforderungen	7
7.2.	Mindestanforderungen	7
7.3.	Administration und Kontrolle	7
8.	Löschkonzept und Speicherbegrenzung.....	7
8.1.	Allgemeine Anforderungen	7
8.2.	Mindestinhalte des Löschkonzepts.....	7
8.3.	Technische Umsetzung und Nachweisbarkeit.....	8
8.4.	Löschung bei Vertragsende	8
9.	Datenverarbeitung und Datenübermittlung in Drittländer	8
9.1.	Transparenzpflicht	8
9.2.	Zulässigkeit der Drittlandübermittlung	8
9.3.	Besondere Anforderungen bei Datenübermittlungen in die USA	9
9.4.	Einsatz von Garantien nach Art. 46 DS-GVO.....	9
10.	Kontroll-, Informations- und Kündigungsrechte	9
11.	Bewertungsrelevanz	10
II.	Zuschlagskriterien – Datenschutz (Cloud-/SaaS-Fachverfahren)	11
1.	Technische und organisatorische Maßnahmen (TOMs)	11
1.1.	Qualität und Nachvollziehbarkeit der TOM-Dokumentation	11
1.2.	Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit	11
1.3.	Berücksichtigung des Standes der Technik	11
2.	Zertifizierungen und Prüfungen.....	12
2.1.	Informationssicherheits-Zertifizierungen.....	12
3.	Datenschutz- und Sicherheitsorganisation	12
3.1.	Organisation und Verantwortlichkeiten	12
4.	Unterauftragsverarbeiter	12
4.1.	Transparenz und Steuerbarkeit von Unterauftragsverarbeitern	12



5.	Rollen- und Rechtekonzept	13
5.1.	Granularität und Struktur des Rollen-/Rechtekonzepts	13
5.2.	Berechtigungsverwaltung und Lifecycle	13
5.3.	Protokollierung und Kontrolle.....	13
6.	Löschkonzept und Speicherbegrenzung	14
6.1.	Vollständigkeit und Verständlichkeit des Löschkonzepts	14
6.2.	Technische Umsetzung und Automatisierungsgrad	14
6.3.	Backups, Test- und Entwicklungsumgebungen.....	14
6.4.	Löschung bei Vertragsende.....	14
7.	Drittlandübermittlungen	15
7.1.	Transparenz zu Drittlandverarbeitungen	15
7.2.	Rechtliche Grundlage und Garantien	15
8.	Kontroll- und Kündigungsrechte	15
8.1.	Steuerbarkeit durch die Auftraggeberin	15
9.	Gesamtsystematik.....	15
III.	Gesamtbewertungsmatrix	16
1.	Technische und organisatorische Maßnahmen (TOMs)	16
2.	Zertifizierungen und Prüfungen.....	16
3.	Datenschutz- und Sicherheitsorganisation	16
4.	Unterauftragsverarbeiter	16
5.	Rollen- und Rechtekonzept.....	17
6.	Löschkonzept und Speicherbegrenzung.....	17
7.	Drittlandübermittlungen	17
8.	Kontroll-, Informations- und Kündigungsrechte.....	17
	Gesamtübersicht.....	18



I. Leistungsbeschreibung / Lastenheft

1. Allgemeine datenschutzrechtliche Einordnung

Der Auftragnehmer verarbeitet im Rahmen der Leistungserbringung personenbezogene Daten als **Auftragsverarbeiter** im Sinne des Art. 4 Abs. 1 Nr. 8 der Datenschutz-Grundverordnung (DS-GVO).

Auftraggeberin ist die Stadt Koblenz und **Verantwortliche** im Sinne des Art. 4 Abs. 1 Nr. 7 DS-GVO.

Die Verarbeitung personenbezogener Daten erfolgt ausschließlich auf dokumentierte Weisung der Auftraggeberin/Verantwortlichen „Stadt Koblenz“ und unter Einhaltung der einschlägigen datenschutzrechtlichen Bestimmungen, insbesondere der Art. 5, 28 und 32 DS-GVO.

2. Auftragsverarbeitung gemäß Art. 28 DS-GVO

Der Auftragnehmer/Auftragsverarbeiter verpflichtet sich, alle Anforderungen an die Auftragsverarbeitung gemäß Art. 28 DS-GVO zu erfüllen.

Mit Angebotsabgabe ist eine Eigenerklärung vorzulegen, aus der hervorgeht, dass geeignete technische und organisatorische Maßnahmen (TOMs) implementiert wurden.

Die Eigenerklärung gilt uneingeschränkt auch für alle eingesetzten Unterauftragsverarbeiter, sofern diese im Rahmen der Leistungserbringung personenbezogene Daten verarbeiten oder die Möglichkeit der Kenntnisnahme dieser Daten besteht.

3. Technische und organisatorische Maßnahmen (TOMs)

3.1. Allgemeine Anforderungen

Der Auftragnehmer/Auftragsverarbeiter hat geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau gemäß Art. 32 DS-GVO sicherzustellen.

Dabei sind insbesondere zu berücksichtigen:

- der Stand der Technik,
- die Implementierungskosten,
- die Art, der Umfang und die Zwecke der Verarbeitung,
- die Risiken für die Rechte und Freiheiten natürlicher Personen.

3.2. Mindestanforderungen an die TOMs

Die TOMs müssen insbesondere Maßnahmen zur Sicherstellung der folgenden Schutzziele enthalten:

- **Vertraulichkeit,**
- **Integrität,**
- **Verfügbarkeit,**
- **Belastbarkeit** der Systeme und Dienste.



Hierzu zählen unter anderem:

- Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags- und Verfügbarkeitskontrollen,
- Maßnahmen zur Mandantentrennung im Cloud-/SaaS-Betrieb,
- Verschlüsselung personenbezogener Daten bei Übertragung und Speicherung,
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOMs.

Die Qualität und Nachvollziehbarkeit der Darstellung ist bewertungsrelevant.

3.3. Berücksichtigung des Standes der Technik

Der Auftragnehmer/Auftragsverarbeiter hat darzulegen, welche technischen Standards, Sicherheitskonzepte und organisatorischen Verfahren zur Umsetzung der TOMs eingesetzt werden und wie diese regelmäßig aktualisiert werden.

Der Auftragnehmer/Auftragsverarbeiter hat darzulegen:

- welche Sicherheitsstandards angewendet werden,
- wie Sicherheitsmaßnahmen fortlaufend aktualisiert werden,
- wie Änderungen am Sicherheitsniveau dokumentiert und kommuniziert werden.

4. Zertifizierungen und Prüfungen

Sofern vorhanden, sind mit Angebotsabgabe einschlägige Zertifizierungen oder Prüfberichte (z. B. ISO/IEC 27001, SOC 2, ISAE 3000 oder vergleichbare Standards) vorzulegen.

Zertifizierungen sind nur dann bewertungsrelevant, wenn ihr Geltungsbereich das angebotene Fachverfahren und die zugrunde liegende Betriebsumgebung umfasst.

5. Datenschutz- und Sicherheitsorganisation

Der Auftragnehmer/Auftragsverarbeiter hat darzulegen:

- ob ein Datenschutzbeauftragter gemäß Art. 37 DS-GVO benannt ist,
- welche organisatorischen Regelungen zur Informationssicherheit bestehen,
- wie Mitarbeitende regelmäßig zu Datenschutz und Informationssicherheit geschult werden,
- welche Prozesse zur Behandlung von Datenschutz- und Sicherheitsvorfällen eingerichtet sind.

6. Unterauftragsverarbeiter

Der Auftragnehmer/Auftragsverarbeiter hat alle Unterauftragsverarbeiter vollständig zu benennen, die im Rahmen der Leistungserbringung personenbezogene Daten verarbeiten oder die Möglichkeit der Kenntnisnahme haben.

Der Einsatz von Unterauftragsverarbeitern ist nur zulässig, wenn:

- diese auf mindestens gleichwertige TOMs verpflichtet sind,
- die Auftraggeberin/Verantwortliche vorab informiert wird,
- die datenschutzrechtlichen Verpflichtungen uneingeschränkt weitergegeben werden.



7. Rollen- und Rechtekonzept

7.1. Allgemeine Anforderungen

Das Fachverfahren muss ein rollenbasiertes Berechtigungs- und Zugriffskonzept unterstützen, das dem Prinzip der **minimalen Rechtevergabe** sowie dem **Need-to-know-Prinzip** entspricht.

7.2. Mindestanforderungen

Das Rollen- und Rechtekonzept muss mindestens folgende Funktionen umfassen:

- vordefinierte Rollen mit klar abgegrenzten Berechtigungen,
- Möglichkeit zur Anpassung und Erweiterung von Rollen,
- Steuerung des Zugriffs auf Funktionen, Datenkategorien und – soweit fachlich vorgesehen – einzelne Datensätze,
- Protokollierung von An- und Abmeldungen sowie von Änderungen an Berechtigungen.

7.3. Administration und Kontrolle

Das Fachverfahren muss Funktionen zur zentralen Verwaltung von Benutzerkonten und Berechtigungen bereitstellen, insbesondere:

- Anlage, Änderung und Deaktivierung von Benutzerkonten,
- zeitlich befristete Berechtigungen,
- Auswertungsmöglichkeiten für Zugriffs- und Berechtigungsprotokolle.

Der Umfang und die Ausgestaltung des Rollen- und Rechtekonzepts sind bewertungsrelevant. Die Qualität des Rollen- und Rechtekonzepts wird insbesondere anhand folgender Kriterien bewertet:

- Granularität der Rechtevergabe,
- Nachvollziehbarkeit und Prüfbarkeit der Berechtigungssteuerung,
- Unterstützung organisatorischer Anforderungen einer kommunalen Verwaltung.

8. Löschkonzept und Speicherbegrenzung

8.1. Allgemeine Anforderungen

Der Auftragnehmer/Auftragsverarbeiter hat ein datenschutzkonformes Löschkonzept gemäß Art. 5 Abs. 1 lit. e) DS-GVO (Speicherbegrenzung) bereitzustellen.

Das Löschkonzept muss sicherstellen, dass personenbezogene Daten nur so lange gespeichert werden, wie es für die festgelegten Zwecke erforderlich ist.

8.2. Mindestinhalte des Löschkonzepts

Das Löschkonzept muss mindestens folgende Aspekte enthalten:

- Beschreibung der löschbaren Datenkategorien,
- Unterstützung von konfigurierbaren Aufbewahrungs- und Löschfristen,
- Darstellung der eingesetzten Löschmechanismen,
- Regelungen zum Umgang mit Daten in Produktiv-, Test- und Entwicklungsumgebungen sowie in Backups.



8.3. Technische Umsetzung und Nachweisbarkeit

Der Auftragnehmer/Auftragsverarbeiter hat darzulegen:

- ob Löschungen automatisiert unterstützt werden,
- wie Löschvorgänge protokolliert und dokumentiert werden,
- wie die Umsetzung bei Unterauftragsverarbeitern sichergestellt wird.

Die Ausgestaltung der technischen Umsetzung ist bewertungsrelevant.

8.4. Löschung bei Vertragsende

Nach Beendigung des Vertragsverhältnisses sind personenbezogene Daten nach Weisung der Auftraggeberin/Verantwortlichen zu löschen oder zurückzugeben.

Der Auftragnehmer/Auftragsverarbeiter hat darzustellen:

- innerhalb welcher Fristen die Löschung erfolgt,
- in welcher Form eine Löschbestätigung erbracht wird,
- wie mit Sicherungskopien verfahren wird.

9. Datenverarbeitung und Datenübermittlung in Drittländer

9.1. Transparenzpflicht

Der Auftragnehmer/Auftragsverarbeiter hat vollständig offenzulegen, ob und in welche Drittländer personenbezogene Daten übermittelt oder dort verarbeitet werden.

Hierbei sind anzugeben:

- das jeweilige Drittland,
- der Zweck der Übermittlung,
- die betroffenen Datenkategorien,
- die eingesetzten (Unter-)Auftragsverarbeiter.

Das Löschkonzept wird insbesondere bewertet nach:

- Vollständigkeit und Verständlichkeit,
- Grad der Automatisierung,
- Nachweisbarkeit der Löschvorgänge,
- Umsetzbarkeit in der kommunalen Praxis.

9.2. Zulässigkeit der Drittlandübermittlung

Sofern eine Drittlandübermittlung erfolgt, hat der Auftragnehmer/Auftragsverarbeiter darzulegen, auf welcher Rechtsgrundlage diese erfolgt.

Zulässige Rechtsgrundlagen sind insbesondere:

- Angemessenheitsbeschlüsse gemäß Art. 45 DS-GVO,
- geeignete Garantien gemäß Art. 46 DS-GVO
 - BCR – Binding Corporate Rules „verbindliche interne Datenschutzvorschriften“
 - SCC – Standard Contractual Clauses „Standardvertragsklauseln“
 - SCC + TIA – Transfer Impact Assessment



- *SCC + TIA bedeutet die Anwendung der EU-Standardvertragsklauseln gemäß Art. 46 DS-GVO in Verbindung mit einer dokumentierten Transfer Impact Assessment zur Bewertung der Risiken der Drittlandübermittlung.*
- *Werden EU-Standarddatenschutzklauseln gemäß Art. 46 Abs. 2 DS-GVO eingesetzt, sind bewertungsrelevant ergänzend die zusätzlich implementierten technischen Maßnahmen darzulegen, die geeignet sind, den Zugriff auf personenbezogene Daten durch unbefugte Dritte im Drittland zu verhindern. Hierzu zählen insbesondere Maßnahmen wie Verschlüsselung mit ausschließlicher Schlüsselhoheit der Auftraggeberin/Verantwortlichen bzw. EU-Schlüsselhoheit, Pseudonymisierung vor Drittland-übermittlung oder vergleichbare technische Schutzmechanismen.*
- *Sofern der Auftragnehmer/Auftragsverarbeiter Binding Corporate Rules (BCR) gemäß Art. 46 Abs. 2 lit. b, Art. 47 DS-GVO einsetzt, sind diese mit Angebotsabgabe bewertungsrelevant konkret zu benennen und in geeigneter Form nachzuweisen.*
- *Der Auftragnehmer/Auftragsverarbeiter hat darzulegen, für welche Konzerngesellschaften und Verarbeitungsvorgänge die BCR gelten und ob ergänzende technische oder organisatorische Maßnahmen implementiert wurden.*

9.3. Besondere Anforderungen bei Datenübermittlungen in die USA

Sofern personenbezogene Daten in die Vereinigten Staaten von Amerika übermittelt werden, ist nachzuweisen, dass der jeweilige Empfänger am **EU-U.S. Data Privacy Framework (DPF)** teilnimmt. Der Auftragnehmer/Auftragsverarbeiter verpflichtet sich, die Auftraggeberin/Verantwortliche unverzüglich über Änderungen der Zertifizierung zu informieren.

9.4. Einsatz von Garantien nach Art. 46 DS-GVO

Werden geeignete Garantien gemäß Art. 46 DS-GVO eingesetzt, hat der Auftragnehmer/Auftragsverarbeiter ergänzend darzulegen:

- welche Garantien konkret verwendet werden,
- ob zusätzliche technische oder organisatorische Maßnahmen implementiert wurden,
- ob eine risikobasierte Bewertung der Drittlandübermittlung (z. B. Transfer Impact Assessment) durchgeführt wurde.

10. Kontroll-, Informations- und Kündigungsrechte

Der Auftragnehmer/Auftragsverarbeiter räumt der Auftraggeberin/Verantwortlichen folgende Rechte ein:

- Auskunft über alle datenschutzrelevanten Aspekte der Leistungserbringung,
- Information über wesentliche Änderungen der Datenverarbeitung,
- Audit- und Kontrollrechte,
- Sonderkündigungsrecht bei Wegfall der datenschutzrechtlichen Zulässigkeit der Datenverarbeitung.



11. Bewertungsrelevanz

Die Erfüllung der vorgenannten Anforderungen ist Bestandteil der Angebotswertung. Die Qualität, Vollständigkeit und Nachvollziehbarkeit der Angaben sowie der vorgelegten Nachweise fließen in die Bewertung ein.

Die maximale Punktzahl wird nur vergeben, wenn die Anforderungen vollständig, konkret und nachvollziehbar beschrieben und durch geeignete Unterlagen belegt sind.



II. Zuschlagskriterien – Datenschutz (Cloud-/SaaS-Fachverfahren)

1. Technische und organisatorische Maßnahmen (TOMs)

1.1. Qualität und Nachvollziehbarkeit der TOM-Dokumentation

Gewichtung: **7 %**

Max. Punkte: **10**

Punkte	Bewertbare Ausprägung
0	Keine oder rein pauschale Angaben
3	TOMs entlang Art. 32 DS-GVO benannt
6	Strukturierte TOMs inkl. Schutzbedarfsbezug
8	Zusätzlich: konkrete technische Maßnahmen
10	Zusätzlich: externe Prüfberichte / Auditnachweise

1.2. Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit

Gewichtung: **9 %**

Max. Punkte: **12**

Punkte	Bewertbare Ausprägung
0	Keine konkrete Darstellung
4	Grundlegende Maßnahmen je Schutzziel
8	Maßnahmen + SLAs (z. B. Verfügbarkeit)
12	Zusätzlich: Redundanzen, Notfall- & Wiederanlaufkonzepte

1.3. Berücksichtigung des Standes der Technik

Gewichtung: **4 %**

Max. Punkte: **6**

Punkte	Bewertbare Ausprägung
0	Keine Aussagen
2	Allgemeiner Verweis auf Standards
4	Konkrete Standards benannt
6	Zusätzlich: Update- und Reviewprozesse



2. Zertifizierungen und Prüfungen

2.1. Informationssicherheits-Zertifizierungen

Gewichtung: 6 %

Max. Punkte: 8

Punkte	Bewertbare Ausprägung
0	Keine Zertifizierung
3	Teilzertifizierung
6	ISO/IEC 27001 (voller Geltungsbereich)
8	Zusätzlich: SOC 2 / ISAE 3000

3. Datenschutz- und Sicherheitsorganisation

3.1. Organisation und Verantwortlichkeiten

Gewichtung: 4 %

Max. Punkte: 6

Punkte	Bewertbare Ausprägung
0	Keine Angaben
2	Datenschutzbeauftragter benannt
4	Schulungen & Richtlinien
6	Zusätzlich: Incident-Response-Prozess

4. Unterauftragsverarbeiter

4.1. Transparenz und Steuerbarkeit von Unterauftragsverarbeitern

Gewichtung: 6 %

Max. Punkte: 8

Punkte	Bewertbare Ausprägung
0	Keine Angaben
3	Unterauftragsverarbeiter benannt
6	TOM-Gleichwertigkeit sichergestellt
8	Zusätzlich: Audit- & Genehmigungsrechte



5. Rollen- und Rechtekonzept

5.1. Granularität und Struktur des Rollen-/Rechtekonzepts

Gewichtung: 7 %

Max. Punkte: 10

Punkte	Bewertbare Ausprägung
0	Kein Rollenmodell
3	Statisches Rollenmodell
6	Mehrstufige Rollen
8	Fein granulare Rechte
10	Zusätzlich: Datensatz-/Funktionsrechte

5.2. Berechtigungsverwaltung und Lifecycle

Gewichtung: 5 %

Max. Punkte: 8

Punkte	Bewertbare Ausprägung
0	Manuell / keine Angaben
3	Zentrale Verwaltung
6	Zeitlich befristete Rechte
8	Automatisierte Deaktivierung / Rezertifizierung

5.3. Protokollierung und Kontrolle

Gewichtung: 4 %

Max. Punkte: 6

Punkte	Bewertbare Ausprägung
0	Keine Protokolle
2	Login-Protokolle
4	Rechteänderungen
6	Auswertbare Reports



6. Löschkonzept und Speicherbegrenzung

6.1. Vollständigkeit und Verständlichkeit des Löschkonzepts

Gewichtung: 6 %

Max. Punkte: 10

Punkte	Bewertbare Ausprägung
0	Kein Löschkonzept
3	Allgemeine Beschreibung
6	Datenkategorien & Fristen
8	Technische Umsetzung
10	Zusätzlich: Verantwortlichkeiten & Nachweise

6.2. Technische Umsetzung und Automatisierungsgrad

Gewichtung: 8 %

Max. Punkte: 12

Punkte	Bewertbare Ausprägung
0	Nur manuelle Löschung
4	Teilautomatisiert
8	Vollautomatisiert
10	Konfigurierbare Fristen
12	Protokollierte Löschläufe

6.3. Backups, Test- und Entwicklungsumgebungen

Gewichtung: 5 %

Max. Punkte: 8

Punkte	Bewertbare Ausprägung
0	Keine Angaben
3	Backup-Löschung beschrieben
6	Fristen & Verfahren
8	Einheitliches Gesamtkonzept

6.4. Löschung bei Vertragsende

Gewichtung: 3 %

Max. Punkte: 6

Punkte	Bewertbare Ausprägung
0	Keine Regelung
2	Löschzusage
4	Fristen & Verfahren
6	Löschbestätigung



7. Drittlandübermittlungen

7.1. Transparenz zu Drittlandverarbeitungen

Gewichtung: 4 %

Max. Punkte: 6

Punkte	Bewertbare Ausprägung
0	Keine oder unklare Angaben = unzulässig
2	Drittland benannt
4	Drittland, Zweck und Datenarten benannt
6	Zusätzlich: strukturierte Datenflussdarstellung inkl. Unterauftragnehmer

7.2. Rechtliche Grundlage und Garantien

Gewichtung: 16 %

Max. Punkte: 12

Punkte	Bewertbare Ausprägung
0	Keine Zulässigkeitslegitimation = unzulässig
4	<ul style="list-style-type: none"> ➤ SCC (Standardvertragsklauseln) ➤ BCR (Binding Corporate Rules) <u>ohne</u> TIA (Transfer Impact Assessment)
8	<ul style="list-style-type: none"> ➤ Angemessenheitsbeschluss <u>ohne</u> Informations- & Exitregelungen ➤ SCC + TIA „allgemein“ (abstrakt / generisch) ➤ BCR + TIA „allgemein“ (abstrakt / generisch)
12	<ul style="list-style-type: none"> ➤ Angemessenheitsbeschluss + Informations- & Exitregelungen ➤ SCC + TIA „konkret“ (verfahrens- / angebotsbezogen) + zusätzliche technische Maßnahmen (TOMs) ➤ BCR + TIA „konkret“ (verfahrens- / angebotsbezogen) + TOMs

8. Kontroll- und Kündigungsrechte

8.1. Steuerbarkeit durch die Auftraggeberin

Gewichtung: 6 %

Max. Punkte: 6

Punkte	Bewertbare Ausprägung
0	Keine Regelungen
3	Informationsrechte
6	Zusätzlich: Audit- & Sonderkündigungsrechte

9. Gesamtsystematik

Bereich	Max. Punkte	Gewicht
Datenschutz & Informationssicherheit	134	100 %



III. Gesamtbewertungsmatrix

1. Technische und organisatorische Maßnahmen (TOMs)

Nr.	Zuschlagskriterium	Max. Punkte	Gewicht
1.1	Qualität und Nachvollziehbarkeit der TOM-Dokumentation	10	7 %
1.2	Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit	12	9 %
1.3	Berücksichtigung des Standes der Technik	6	4 %
Summe Bereich 1		28	20 %

2. Zertifizierungen und Prüfungen

Nr.	Zuschlagskriterium	Max. Punkte	Gewicht
2.1	Informationssicherheits-Zertifizierungen und Prüfberichte	8	6 %
Summe Bereich 2		8	6 %

3. Datenschutz- und Sicherheitsorganisation

Nr.	Zuschlagskriterium	Max. Punkte	Gewicht
3.1	Organisation, Verantwortlichkeiten, Incident-Response	6	4 %
Summe Bereich 3		6	4 %

4. Unterauftragsverarbeiter

Nr.	Zuschlagskriterium	Max. Punkte	Gewicht
4.1	Transparenz, Steuerbarkeit, Audit- und Genehmigungsrechte	8	6 %
Summe Bereich 4		8	6 %



5. Rollen- und Rechtekonzept

Nr.	Zuschlagskriterium	Max. Punkte	Gewicht
5.1	Granularität und Struktur des Rollen-/Rechtekonzepts	10	7 %
5.2	Berechtigungsverwaltung und Lifecycle-Management	8	5 %
5.3	Protokollierung und Kontrollmöglichkeiten	6	4 %
Summe Bereich 5		24	16 %

6. Löschkonzept und Speicherbegrenzung

Nr.	Zuschlagskriterium	Max. Punkte	Gewicht
6.1	Vollständigkeit und Verständlichkeit des Löschkonzepts	10	6 %
6.2	Technische Umsetzung und Automatisierungsgrad	12	8 %
6.3	Backups sowie Test- und Entwicklungsumgebungen	8	5 %
6.4	Löschung bei Vertragsende	6	3 %
Summe Bereich 6		36	22 %

7. Drittlandübermittlungen

Nr.	Zuschlagskriterium	Max. Punkte	Gewicht
7.1	Transparenz zu Drittlandverarbeitungen	6	4 %
7.2	Rechtliche Grundlage (Art. 45 DS-GVO / Garantien)	12	16 %
Summe Bereich 7		18	20 %

8. Kontroll-, Informations- und Kündigungsrechte

Nr.	Zuschlagskriterium	Max. Punkte	Gewicht
8.1	Audit-, Informations- und Sonderkündigungsrechte	6	6 %
Summe Bereich 8		6	6 %



Gesamtübersicht

Bereich	Max. Punkte	Gewicht
1. TOMs	28	20 %
2. Zertifizierungen	8	6 %
3. Organisation	6	4 %
4. Unterauftragsverarbeiter	8	6 %
5. Rollen-/Rechtekonzept	24	16 %
6. Löschkonzept	36	22 %
7. Drittlandübermittlungen	18	20 %
8. Kontrollrechte	6	6 %
Gesamt	134 Punkte	100 %

Die maximale Punktzahl wird nur vergeben, wenn die Anforderungen vollständig, konkret und nachvollziehbar beschrieben und durch geeignete Unterlagen belegt sind.

Koblenz, den 26.02.2026

X

Oliver Philippsen
Datenschutzbeauftragter

Nr.	Kriterium Bei Cloud / SaaS Nutzung	Bemerkung	Erfüllt (Ja/Nein) Nachweis
1	TLS Unterstützung (BSI TR-02102) mind. 1.2 empfohlen 1.3	Die Anwendung unterstützt Transportverschlüsselung gemäß BSI TR-02102. Mindestens TLS 1.2 ist zulässig, TLS 1.3 wird empfohlen. Es dürfen nur sichere Cipher-Suites verwendet werden.	
2	Keine hartkodierten Zugangsdaten	Zugangsdaten, Schlüssel oder Tokens sind nicht im Quellcode oder in Konfigurationsdateien fest hinterlegt, sondern sicher parametrisiert und geschützt gespeichert.	
3	Mandantentrennungskonzept vorhanden	Es liegt ein dokumentiertes Konzept zur logischen und/oder physikalischen Trennung von Mandantendaten vor. Mandantenübergreifende Zugriffe sind technisch ausgeschlossen.	
4	Der Service wurde bereits einem White-Box-Pentest bei externer Erreichbarkeit (Internet) unterzogen	Bei Internet-exponierten Anwendungen ist vor Produktivsetzung ein White-Box-Penetrationstest durchzuführen. Festgestellte Schwachstellen sind nachweislich behoben.	
5	Parametrisierbare Netzverbindungen (Firewall/Routing/Proxy)	IP-Adressen, Ports und Kommunikationsziele sind konfigurierbar und nicht fest im System verankert. Dies ermöglicht kontrollierte Firewall-Freigaben.	
6	Bereitstellung als Cloud-/Webbasierte Anwendung (Browserzugriff) für Betriebe und Verwaltung	IP-Adressen, Ports und Kommunikationsziele sind konfigurierbar und nicht fest im System verankert. Dies ermöglicht kontrollierte Firewall-Freigaben.	
7	Wartung der Systeme	Eine lokale Client-Installation auf städtischen Computern bzw. Servern darf nicht erforderlich sein. Zur Wartung des Systems zählen insbesondere die Bereitstellung von Sicherheitsupdates, die Behebung von Fehlern, die Pflege der Systemkomponenten sowie die Weiterentwicklung im Rahmen vereinbarter Releases, u. a. bei Änderungen von rechtlichen und organisatorischen Rahmenbedingungen (z. B. Satzungs-/Regelwerksanpassungen).	

Nr.	Kriterium Technik	Bemerkung	Gewichtung (1-2)	Bewertung (0-10)	Gewichtete Punkte	Bewertungsvorgabe
						jede nicht Beantwortung ergibt 0 Punkte
1	SAML / OIDC Unterstützung	Die Anwendung unterstützt moderne föderierte Authentifizierungsverfahren (SAML 2.0 und/oder OpenID Connect) zur Integration in zentrale Identity-Provider.	1,2			0= keine Angabe oder Nein 6= mind ein Auth.Verf. Wird unterstützt 10= vollständig möglich 0
2	LDAPS Anbindung (RODC)	Eine verschlüsselte Authentifizierung gegen Verzeichnisdienste (LDAPS) ist möglich, auch über Read Only Domain Controller.	1,2			0= keine Angabe oder Nein 6= Ja grds. möglich 10= Ja auf RODC 0
3	API dokumentiert (OpenAPI)	Schnittstellen sind formal dokumentiert (z. B. OpenAPI/Swagger) und ermöglichen eine standardisierte Systemintegration.	1,2			0= keine Angabe oder Nein 4= Schnittstellen sind benannt 8= Schnittstellen sind benannt und formal dokumentiert 0 10= vollständig erfüllt
4	Structured Data (XML/JSON)	Daten werden in standardisierten, maschinenlesbaren Formaten (XML oder JSON) übertragen und exportiert.	1,2			0= keine Angabe oder Nein 0 10= vollständig erfüllt
5	Protokolle vollständig benannt	Alle verwendeten Netzwerkprotokolle inkl. Ports, Richtung der Verbindungen und Zweck sind vollständig dokumentiert.	1,2			0= keine Angabe oder Nein 6 = Angaben liegen teilweise vor 0 10= vollständig erfüllt
6	Firewall-Freigaben vollständig dokumentiert	Es liegt eine Kommunikationsmatrix vor, aus der alle erforderlichen Firewall-Regeln eindeutig hervorgehen.	1,2			0= keine Angabe oder Nein 6= Angaben liegen teilweise vor 0 10= vollständig erfüllt
7	WEB-Browser	Soweit WEB-Browser genutzt werden sind die aktuellen Versionen von MS EDGE und Firefox zu unterstützen	1,2			0= keine Angabe oder Nein 6= mind einer der beiden Browser wird in der aktuellen Version unterstützt 0 10= vollständig erfüllt
8	Keine Datenverarbeitung in DMZ-Gateway	Die DMZ dient ausschließlich als Gateway-/Proxy-Schicht. Fachliche Datenverarbeitung erfolgt nicht in der DMZ.	1,2			0= keine Angabe oder Nein 6= Teilweise erfüllt 8= überwiegend erfüllt 0 10= vollständig erfüllt

Nr.	Kriterium Strategisch	Bemerkung	Gewichtung (1-2)	Bewertung (0-10)	Gewichtete Punkte	Bewertungsvorgabe
9	Exit-Strategie inkl. Datenexport	Es existiert ein dokumentiertes Verfahren zur Vertragsbeendigung inkl. vollständigem und strukturiertem Datenexport.	1,2			0= keine Angabe oder Nein 6= Verfahren ist beschrieben 0 10= vollständige Beschreibung inkl. strukt. Datenexport
10	Datenexport strukturiert (XML)	Daten können vollständig in offenen, strukturierten Formaten exportiert werden, um Systemwechsel zu ermöglichen.	1,2			0= keine Angabe oder Nein 0 10= vollständig erfüllt
11	Kein Vendor-Lock-in	Die Lösung vermeidet proprietäre Abhängigkeiten, die einen Anbieterwechsel technisch oder wirtschaftlich erschweren.	1,2			0= keine Angabe oder Nein 6= Teilweise erfüllt 8= überwiegend erfüllt 0 10= vollständig erfüllt
12	Kommunale Referenzen	Der Anbieter kann vergleichbare produktive Installationen bei öffentlichen Verwaltungen nachweisen mit einer Größe von > 50.000 Einwohner und/oder 1.500 Beschäftigten nachweisen.	1,2			0=trifft nicht zu 4=mindestens 1 6= mindestens 3 0 10= mehr als 3
13	Release-Management transparent	Updates, Wartungszyklen und Versionsstrategien sind dokumentiert und nachvollziehbar kommuniziert.	1,2			0= keine Angabe oder Nein 6= nur grob beschrieben 0 10= vollständig erfüllt

14	Major Updates abstimmbar	Größere Versionssprünge erfolgen nicht unangekündigt, sondern werden mit dem Auftraggeber abgestimmt.	1,2		0= keine Angabe oder Nein 6= Innerhalb einer zeitl.Range < 2 Wochen abstimmbar 8= Innerhalb einer zeitl.Range < 4 Wochen abstimmbar 10= Innerhalb einer zeitl.Range > 4 Wochen abstimmbar
15	Backup- und Restore-Konzept	Ein dokumentiertes Konzept zur Datensicherung und Wiederherstellung inkl. Testverfahren ist vorhanden.	1,2		0= keine Angabe oder Nein 6= Konzept ist vorhanden 10= Konzept inkl. Dokumentierten Testverf. Ist vorhanden

Nr.	Kriterium	Bemerkung	Gewichtung (1-2)	Bewertung (0-10)	Gewichtete Punkte
Sicherer Betrieb					
16	EU/DE Rechenzentrumsstandort	Die Datenverarbeitung erfolgt ausschließlich in Rechenzentren innerhalb der EU.	1,5		0= keine Angabe oder Nein 10= ja
20	Mandantentrennung technisch erklärt	Die technische Umsetzung der Mandantentrennung (z. B. Datenbank, Applikation, Storage) ist nachvollziehbar beschrieben.	1,5		0= keine Angabe oder Nein 6= Mandantentrennung ist möglich 8= Mandantentrennung ist möglich und rudimentär beschrieben 10= Mandantentrennung ist möglich und vollumfänglich beschrieben
21	Penetrationstestbericht vorgelegt	Aktueller Bericht eines unabhängigen Penetrationstests wird zur Verfügung gestellt.	1,5		0= keine Angabe oder Nein 5= Angabe ja - ist erfolgt, wird aber nicht zur Verfügung gestellt 10= vollständig erfüllt
23	Verschlüsselte Storage-Systeme	Daten werden im Ruhezustand (at rest) verschlüsselt gespeichert.	1,5		0= keine Angabe oder Nein 10= vollständig erfüllt
26	Schlüsselmanagement dokumentiert	Verfahren zur Generierung, Speicherung, Rotation und Löschung kryptographischer Schlüssel sind dokumentiert.	1,5		0= keine Angabe oder Nein 6= teilweise erfüllt 10= vollständig erfüllt
28	SLA ≥ 99,5 %	Die vertraglich zugesicherte jährliche Verfügbarkeit beträgt mindestens 99,5 %.	1,5		0= keine Angabe oder Nein oder unter 95 % 4= > 95 % 6= > 98 % 8= > 99 % 10 ≥ 99,5 %
				Gesamtsumme:	0

Bieterpräsentation

Agenda



Bieterpräsentation

I. Bewertung

Die einzelnen Unterpunkte der Bieterpräsentationen werden wie folgt bewertet:

100% = Sehr gute, leicht verständliche, äußerst überzeugende Darstellung; sehr gute Benutzeroberfläche, Umsetzung aller gewünschten Punkte

75% = Überzeugende Darstellung, Gute Benutzeroberfläche, nur einige ergonomische und fachlich/technische Schwächen erkennbar.

50% = Darstellung der Leistungen überzeugte überwiegend, Benutzeroberfläche nicht sehr ergonomisch, fachlich/technische Schwächen.

25% = Darstellung der Leistungen überzeugte nur zum Teil, Benutzeroberfläche komplex und unübersichtlich, ungewohnte Bedienung, hohe fachlich/technische Schwächen.

0% = Darstellung überzeugte nicht; Benutzeroberfläche schwer verständlich, fachlich/technische Funktionen nicht umgesetzt bzw. fehlen.

II. Agenda für die Bieterpräsentation (Start: 8:30 Uhr – Ende: 11:30 Uhr)

Kategorie	Nr.	Thema	Punkte	Notizen
Begrüßung	1	Begrüßung, kurze Vorstellung der Teilnehmenden der Stadt Koblenz 1. Vorstellung der teilnehmenden Personen seitens der Stadt Koblenz.		Nicht bewertungsrelevant

Projekt	2 a)	Vorstellung des Anbieters Präsentationsteams und zukünftige Ansprechpartner (Vertrieb/Produkt) Vorstellung der vorgesehenen Projektumsetzungsmitglieder des Anbieters	200 50	
Projekt	b)	Vorstellung der Erfahrungen mit ähnlichen Projekten Plausibilität der Umsetzungsfähigkeit der angebotenen Leistungen Komptabilität mit anderen regionalen Systemen	50	
Projekt	c)	Vorstellung des Projektablaufs und des Zeitplans Klare Darstellung der zeitlichen Umsetzbarkeit und notwendiger Schritte Realisierbarkeit innerhalb des vorgegebenen Zeitrahmens Unterstützung bei der Einführung (Support) & darüber hinaus 1) bis 2c) 8:30 – 9:00 (30 Min.)	100	
	d)	Eingehen auf Fragen (max. 10 Min.)		Nicht bewertungsrelevant
Software	3 a)	Vorstellung der Software Grundsätzliche Vorstellung der Software inkl. Bildschirmaufbau, Mgl. der Individualisierungen, Begriffsdefinitionen, Strukturierungselemente, Initiale Datenimportmöglichkeiten (Max. 10 Min. bis 09:20)	700 100	

Softwar eproz s	b)	Darstellung der Gästeregistrierung an 4 Beispielen (nicht beitragspflichtig, voll beitragspflichtig, beitragsbegünstigt und befreit auf Datenbasis unseres Satzungsentwurfs), an 1 Beispiel inkl. Storno und Korrekturen. Umgang mit Nachweisdokumenten.	200	
Gästek arte	c)	Darstellung der Ausgabe der Gästekarte (digital und in Print) unter der Berücksichtigung eines möglichen getrennten ÖPNV-Nachweises.	200	
Softwareproze ss	d)	Beschreibung der Übermittlung der Daten von den Betrieben an die Stadt Koblenz (am Bsp. Eines PMS-Systems) und Darstellung des Empfangs in der Software bei den Mitarbeitern der Beitragserhebung. Ermittlung der Beitragssummen, Abrechnungslauf in der Stadt. Abgabemöglichkeit an die kommunale Finanzsoftware 3b) bis d) 9:20 – 10:30 (80 Min.)	200	
		Eingehen auf Fragen und kurze Pause (Max. 15 Min.)		Nicht bewertungsrelevant
Reporti ng	4 a)	Vorstellung Rechte und Reporting Darstellung der Standardauswertungen und Kontrollfunktionen. Darstellung der Supportmöglichkeiten	300 200	

Rechte und Rollen &	b)	Darstellung des Berechtigungskonzept und Rechtevergabe. Welchen Daten können die Mitarbeiter der beitragshebenden Stelle sehen und auswerten und welche Daten können die Mitarbeiter der Touristik im Rahmen touristischer Marketingplanung sehen und auswerten. 4a) und b) 10:45 – 11:15	100	
Optionen	c)	Darstellung des erweiterten Dashboards, der Mobilitätsverknüpfung und des digitalen Gästeführers (Max.5 Min.)		Nicht bewertungsrelevant
		Eingehen auf Fragen (Max. 10 Min.)		Nicht bewertungsrelevant
Summe			1.200	