



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 Rechtekonzpts sind bewertungsrelevant. Die Qualitt des Rollen- und Rechtekonzpts 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